MICROSEC

e-Szignó Certification Authority

Unified
Certification Practice Statement

ver. 3.20

Date of effect: 2026-05-13

OID	1.3.6.1.4.1.21528.2.1.1.230
Version	3.20
First version date of effect	2023-08-30
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	2026-05-08
Date of effect	2026-05-13

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.

Version	Effect date	Description
3.7	2023-08-30	- New document.
3.8	2023-08-31	- Further requirements for S/MIME.
3.9	2023-09-15	- Revocation of CodeSigning Certificates.
3.10	2023-10-30	- Identity validation of natural persons. - CA hierarchies. **[[QUA:** **<ALA:** **- S/MIME certificates for qualified signature. >** **<BEL:** **- S/MIME certificates for qualified seal. >** **]]**
3.11	2023-12-19	- Revision. <ALA: - Natural person identity validation based on electronic signature. > **[[QUA:** **<not TLS:** **- EKU in S/MIME certificates.** **- S/MIME revocation rules.** **- Adding MD940C to QSCD list.** > **]]** <UNI: - S/MIME revocation rules. - EKU in S/MIME certificates. >
3.12	2024-04-03	- Removing SerialNumber extension.

Version	Effect date	Description
3.14	2024-09-01	- Revision. - Change in Hungarian and EU legal requirements. - Self Audit. - Appropriate certificate use. - Router and firewall logging. - Termination preliminary notification 3 months. - Initial identity validation. - New dedicated CA hierarchies. - Reuse of validation materials. - Revocation reasons and deadlines. - Move Certificate fields from 7.1.1 to 7.1.2 - OCSP Responder Certificate. - producedAt field in OCSP response. <not TLS: - CAA check for S/MIME. **[[QUA:** **- Distributed QSCD devices.** **]]** >

Version	Effect date	Description
3.15	2025-03-12	- Global revision. - 2024/2690 Committee order. - Cryptographic requirements. - Adding new CA units. - Pre-issuance linting. - Post-linting on random sample. - Introducing MPIC. <TLS: - Introducing ACME. - Restructuring sections 3.2.2.x to fit CABF BR. - Introducing 3.2.2.4.19 DV method. - Removing 3.2.2.4.9 and 3.2.2.4.15 DV methods. *[[ADV:* *- Removing IV certificates.* *]]* **[[QUA:** **- PSD2 QWAC not EV.** **]]** > <UNI: - Offline CA for CodeSigning TimeStamping. >
3.16	2025-05-20	<UNI: - National Wallet Relying Party Access Certificate. >

Version	Effect date	Description
3.17	2025-09-15	- Revision. - Post incident review. - Key management. <TLS: - Changes in CA hierarchies. - Mass revocation plan and test. - Retire some domain validation methods. - Announced changes in certificate validities. **[[QUA:** **- Increased validity for PSD2 certificates.** **]]** - DNSSEC validation. >
3.18	2025-12-22	- Revision. - New multipurpose RSA-based hierarchy. - Improve validation rules for email address. <not TLS: - DNSSEC validation of CAA records. > - Improve rules for using revocation reasons. - Correct OCSP nocheck OID. **[[QUA:** **<not TLS:** **- Update supported QSCD list. >** **]]** **[[QUA:** **- Conformance to EN 301 549.** **]]**

Version	Effect date	Description
3.19	2026-04-02	- Revision. - Phasing out RSA-2048. - RFC 8954 > RFC 9654. **[[QUA:** **<not TLS:** **- Extent of responsibility information in the certificate. >** **]]** <TLS: - Changes in domain validation methods. - Chrome and CCADB compliance disclosure. - Reuse period for domain validation data. - Certificate validity period. >
3.20	2026-05-13	- Revision. - Certificate modification or re-key initiated by the Service Provider. <TLS: - New subordinate CA units. >

Table of Contents

1 Introduction

This document is the Certification Practice Statement concerning the issuance of several type of certificates service of e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or Certification Service Provider).

- **Purpose of creating the Unified Certification Practice Statement**

  The Certification Service Provider uses a common source to create each Certificate Policy and Certification Practice Statements documents by using appropriate filter settings. The purpose of issuing this document is to summarize the regulations that appear independently in individual public regulations, but are the same in many places, in a common document, thereby helping to compare the specific rules for each type of certificate. Another main purpose of issuing the consolidated regulation is to help the work of the organizations performing conformity assessment and the supervisory authority. In addition to this explanation, these regulations contain exactly the descriptions that can be found independently in the following independent public regulations:

  - eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement
  - eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement
  - eIDAS conform Qualified Certificate for Website Authentication Certification Practice Statement
  - eIDAS conform Non-Qualified Certificate for Electronic Signature Certification Practice Statement
  - eIDAS conform Non-Qualified Certificate for Electronic Seal Certification Practice Statement
  - eIDAS conform Certificate for Website Authentication Certification Practice Statement
  - Non eIDAS covered Certificates Certification Practice Statement

  The individual regulations that come into effect at the same time always have the same version number, but not all regulations are issued every time. In the event of a change in any of the regulations, the consolidated regulations will also be issued, so the provisions of the consolidated regulations always correspond to the provisions of the separate regulations in force, the version number of which can never be higher than the version number of the consolidated regulations.

- **The notations used**

  A significant part of the text of each regulation is the same in all regulations, they are displayed in normal black letters.

  - The following parts can be distinguished based on qualification:
    - parts can be found only in qualified regulations

* parts can be found only in not qualified regulations

The two types of qualification are mutually exclusive, their meaning cannot be combined.

Qualified policies

The sections of the text that apply only to qualified policies

* is denoted by a bold font and
* the full text is located between the opening and closing brackets as indicated below:
  [[QUA: ... text relating to qualified ...]]

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a **[[QUA: qualified]]** sample in a flowing text ...

or

[[QUA:
This is an arbitrary length section found only in qualified policies
....
until this
]]

Not qualified policies

The sections of the text that apply only to non-qualified policies

* is denoted by an italic font and
* the full text is located between the opening and closing brackets as indicated below:
  [[ADV: ... text relating to non-qualified ...]]

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a *[[ADV: not qualified]]* sample in a flowing text ...

or

[[ADV:
This is an arbitrary length section found only in not qualified policies
....
until this
]]

– According to the purpose of certificate use, we distinguish the following types:
  * the parts found only in the website authentication certificate policies
  * the parts found only in the regulations for electronic signature certificates
  * the parts found only in the regulations for electronic seal certificates
  * other parts found in the regulations of certificates not covered by eIDAS

Website authentication certificate policies

Sections regarding the website authentication certificates

* are denoted by red font and
* the full text is located between the opening and closing brackets as indicated below:
  <TLS: ... text related to website authentication certificates ... >

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a <TLS: website authentication certificate> sample in a flowing text ...

or

<TLS:
This is an arbitrary length section found only in the website authentication certificate policies
....
until this
>

Electronic signature certificate policies

Sections regarding the electronic signature certificates

* are denoted by dark blue font and
* the full text is located between the opening and closing brackets as indicated below:
  <SIG: ... text related to electronic signature certificates ... >

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a <ALA: electronic signature certificate> sample in a flowing text ...

or

<ALA:
This is an arbitrary length section found only in the electronic signature certificate policies
....
until this
>

Electronic seal certificate policies

Sections regarding the electronic seal certificates

* are denoted by green font and

* the full text is located between the opening and closing brackets as indicated below:
  <SEA: ... text related to electronic seal certificates ... >

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a <BEL: electronic seal certificate> sample in a flowing text ...

or

<BEL:
This is an arbitrary length section found only in the electronic seal certificate policies
....
until this >

Certificate policies not according to the eIDAS Regulation

Sections regarding the not eIDAS covered certificates

* are denoted by purple font and
* the full text is located between the opening and closing brackets as indicated below:
  <UNI: ... text related to not eIDAS covered certificates ... >

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a <UNI: not eIDAS covered certificate> sample in a flowing text ...

or

<UNI:
This is an arbitrary length section found only in the not eIDAS covered certificate policies
....
until this
>

Exclusion

In the case of certificate types, the exclusion of individual types can be interpreted if a part of the text can be interpreted for all certificate types except for a specific type (e.g. everything that is not a website authentication). This option is indicated in the policy as follows:

* in all cases it is indicated by a uniformly light blue font, and
* the full text is located between the opening and closing brackets as indicated below:
  <not TLS: ... text for all certificates except website authentication ... >

The highlighted part can be a short part within the current text, or a longer part, the separation of which is also helped by the segmentation of the text, such as

... this is a <not TLS: all certificates except website authentication> sample in a flowing text ...

or

<not TLS:
This is an arbitrary length section found in each policies except the website authentication
....
until this
>

Multiple exclusions can also be interpreted here, such as e.g.

<not TLS:
<not UNI:
This is an arbitrary length section found only in signature and seal policies
....
until this
>>

- **Combining marks**

  The described markings - where this can be interpreted - can be found in the regulations in combination with each other, or more precisely, embedded in each other, in which case combinations of the described markings must be used according to their meaning.

  If there is an interpretation problem regarding the markings in the regulations, it is worth comparing the specific parts with the corresponding parts of the separately published regulations.

The Certification Service Provider provides its services for its Clients with whom it has contractual relationship.

The present Certification Practice Statement describes the framework of the provision of the aforementioned services and includes the detailed procedures and miscellaneous operating rules. It makes recommendations for the Relying Parties for the verification of the <ALA: electronic signatures and> <BEL: electronic seals and> Certificates created by using the services.

<TLS:
The Certification Practice Statement complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU **[[QUA: qualified]]** Trust Service.
>
<ALA:

The Certification Practice Statement complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU **[[QUA: qualified]]** Trust Service.

>

<BEL:

The Certification Practice Statement complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU **[[QUA: qualified]]** Trust Service.

>

<TLS:

[[QUA:

The Website Authentication Certificate issued for legal persons under the service can fulfil the requirements of CA/Browser Forum EV (Extended Validation) Certificates [65].

]]

>

<TLS:

[[ADV:

The Certification Service Provider announced the provision of the trust service to the National Media and Infocommunications Authority on the 1st of July 2016.

]]

>

<ALA:

The Certification Service Provider announced the provision of the trust service to the National Media and Infocommunications Authority on the 1st of July 2016.

>

<BEL:

The Certification Service Provider announced the provision of the trust service to the National Media and Infocommunications Authority on the 1st of July 2016.

>

[[QUA:

The conformity assessment audit of the qualified trust services was carried out by the independent auditor TÜV Informationstechnik GmbH (hereinafter: TÜViT).

<TLS:

Based on the successful conformity assessment audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the Hungarian Trusted List [75] on the 1st of January 2019.

>

<ALA:

Based on the successful conformity assessment audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the Hungarian Trusted List [75] on the 20th of December 2016.

>

<**BEL:**

Based on the successful conformity assessment audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the Hungarian Trusted List [75] on the 20th of December 2016.

>

The conformity assessment of the qualified trust service will be performed by Hunguard Kft. (hereinafter: Hunguard) as an independent auditor from October 2020.

]]

[[QUA:

The Certification Service Provider provides the most important information to the Clients also in the form of a Disclosure Statement. The Disclosure Statement will be published as described in Section 2.1.

]]

[[ADV:

<TLS:

The Certification Service Provider provides the most important information to the Clients also in the form of a Disclosure Statement. The Disclosure Statement will be published as described in Section 2.1.

>

<ALA:

The Certification Service Provider provides the most important information to the Clients also in the form of a Disclosure Statement. The Disclosure Statement will be published as described in Section 2.1.

>

<BEL:

The Certification Service Provider provides the most important information to the Clients also in the form of a Disclosure Statement. The Disclosure Statement will be published as described in Section 2.1.

>

]]

1.1 Overview

The aim of the present Certification Practice Statement is to summarize all the information that the Clients coming into contact with the Certification Service Provider should know. This aims to foster that its Clients and future Clients:

- get better acquainted with the details and requirements of the services provided by the Certification Service Provider, and the practical background of the service provision
- be able to see through the operation of the Certification Service Provider, and thus more easily decide whether the services comply or which type of services meet their individual needs and expectations.

Furthermore, the aim of this document is to support the users and relying parties of Certificates, Certificate Revocation Lists and Online Certificate Status Responses issued by the Certification Service Provider to clearly understand the ways of their management, the level of security guaranteed by them as well as the relevant technical, commercial and financial guarantees with legal responsibility related to them.

The content and format of the present document complies with the requirements of the IETF RFC 3647 [40] framework. It consists of 9 sections that contain the security requirements, processes defined by the Certification Service Provider and the practices to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, section headings where the document does not impose a requirement have the statement "No stipulation".

Considering the end user activity related to the services used, besides the present Certification Practice Statement further requirements may be found in <not TLS: the Time Stamping Policy [78], > the General Terms and Conditions and the service agreement concluded with the provider, the Certificate Policies applied by the Certification Service Provider (see section 1.2.1) and other regulation or document independent from the Certification Service Provider as well.

Section 1.6 of this document specifies several terms which are not or not fully used in this sense in other areas. Terms used in this sense are indicated in capital letters and italics throughout the document.

<TLS:

- The Certification Service Provider conforms to the current version of the "Chrome Root Program Policy" [68] published at

  `https://googlechrome.github.io/chromerootprogram/`

  URL.

- The Certification Service Provider conforms to the current version of the "Common CA Database Policy" [67] published at

  `https://www.ccadb.org/policy`

  URL.

>

1.2 Document Name and Identification

Issuer	e-Szignó Certification Authority
Document name	Unified Certification Practice Statement
Document version	3.20
Date of effect	2026-05-13

The list and identification information of the Certificate Policies that can be used according to the present Certification Practice Statement can be found in section 1.2.1.

1.2.1 Certificate Policies

All Certificates issued by the Certification Service Provider refer to that Certificate Policy on the basis of which they were issued.

The first seven numbers of the OID identifying the Certificate Policies are the unique identifier of Microsec, as follows:

(1)	International Organization for Standardization (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2
(6)	United States Department of Defense (DoD)
(1)	Internet
(4)	Private projects
(1)	Private enterprises
(21528)	MICROSEC Ltd.

The system of the further numbers was allocated within Microsec's own scope of authority, the interpretation of it is as follows:

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	e-Szignó Certification Authority
(1)	documents
(1)	public documents
(x)	unique identifier number of the document

In accordance with this Certification Practice Statement the Certification Service Provider issues Certificates based on the following Certificate Policies:

OID	DENOMINATION	SHORT NAME
<TLS:		
[[QUA:		
1.3.6.1.4.1.21528.2.1.1.170	**Certificate Policy for Qualified certificates for website authentication, prohibiting the use of pseudonyms.**	**MWJSN**
1.3.6.1.4.1.21528.2.1.1.235	**Certificate Policy for Qualified certificates for other than website authentication, prohibiting the use of pseudonyms.**	**MPJSN**
]]		
[[ADV:		
1.3.6.1.4.1.21528.2.1.1.159	*Certificate Policy for certification class III. certificates for website authentication, issued for legal persons, prohibiting the use of pseudonyms.*	*HWJSN*

1.3.6.1.4.1.21528.2.1.1.161	*Certificate Policy for certification class II. certificates for website authentication, prohibiting the use of pseudonyms.*	*KWJSN*
1.3.6.1.4.1.21528.2.1.1.162	*Certificate Policy for certificates for website authentication certificates, issued during automatic issuance, prohibiting the use of pseudonyms.*	*AWxSN*

]]

>

<ALA:

[[QUA:

1.3.6.1.4.1.21528.2.1.1.142	**Certificate Policy for Qualified certificates, for the generation and verification of electronic signatures, issued on Qualified Electronic Signature or Seal Creation Device for natural persons, prohibiting the use of pseudonyms.**	**MATBN**
1.3.6.1.4.1.21528.2.1.1.143	**Certificate Policy for Qualified certificates, for the generation and verification of electronic signatures, issued on Cryptographic Hardware Device for natural persons, prohibiting the use of pseudonyms.**	**MATHN**
1.3.6.1.4.1.21528.2.1.1.144	**Certificate Policy for Qualified certificates, for the generation and verification of electronic signatures, issued as a software token for natural persons, prohibiting the use of pseudonyms.**	**MATSN**
1.3.6.1.4.1.21528.2.1.1.232	**Certificate Policy for Qualified S/MIME certificates, which can be used also for the generation and verification of electronic signatures, issued for natural persons, prohibiting the use of pseudonyms.**	**MSxxN**

]]

[[ADV:

1.3.6.1.4.1.21528.2.1.1.149	*Certificate Policy for Not qualified, certification class III. certificates, for the generation and verification of electronic signatures, issued on Cryptographic Hardware Device for natural persons, prohibiting the use of pseudonyms.*	*HATHN*
1.3.6.1.4.1.21528.2.1.1.150	*Certificate Policy for Not qualified, certification class III. certificates, for the generation and verification of electronic signatures, issued as a software token for natural persons, prohibiting the use of pseudonyms.*	*HATSN*

1.3.6.1.4.1.21528.2.1.1.153	*Certificate Policy for Not qualified, certification class II. certificates, for the generation and verification of electronic signatures, issued for for natural persons, prohibiting the use of pseudonyms.*	*KATxN*

]]

>

<BEL:

[[QUA:

1.3.6.1.4.1.21528.2.1.1.181	**Certificate Policy for Qualified certificates, for the generation and verification of electronic seals, issued on Qualified Electronic Signature or Seal Creation Device for legal persons, prohibiting the use of pseudonyms.**	**MBJBN**
1.3.6.1.4.1.21528.2.1.1.182	**Certificate Policy for Qualified certificates, for the generation and verification of electronic seals, issued on Cryptographic Hardware Device for legal persons, prohibiting the use of pseudonyms.**	**MBJHN**
1.3.6.1.4.1.21528.2.1.1.183	**Certificate Policy for Qualified certificates, for the generation and verification of electronic seals, issued as a software token for legal persons, prohibiting the use of pseudonyms.**	**MBJSN**
1.3.6.1.4.1.21528.2.1.1.232	**Certificate Policy for Qualified S/MIME certificates, which can be used also for the generation and verification of electronic seals, issued for legal persons, prohibiting the use of pseudonyms.**	**MSxxN**

]]

[[ADV:

1.3.6.1.4.1.21528.2.1.1.184	*Certificate Policy for Not qualified, certification class III. certificates, for the generation and verification of electronic seals, issued on Cryptographic Hardware Device for legal persons, prohibiting the use of pseudonyms.*	*HBJHN*
1.3.6.1.4.1.21528.2.1.1.185	*Certificate Policy for Not qualified, certification class III. certificates, for the generation and verification of electronic seals, issued as a software token for legal persons, prohibiting the use of pseudonyms.*	*HBJSN*
1.3.6.1.4.1.21528.2.1.1.174	*Certificate Policy for Not qualified, certification class II. certificates, for the generation and verification of electronic seals, issued for legal persons, prohibiting the use of pseudonyms.*	*KBJxN*

]]

>
<UNI:

1.3.6.1.4.1.21528.2.1.1.155	Certificate Policy for Non eIDAS covered, certification class III. certificates, issued on Cryptographic Hardware Device for natural persons, prohibiting the use of pseudonyms.	HETHN
1.3.6.1.4.1.21528.2.1.1.156	Certificate Policy for Non eIDAS covered, certification class III. certificates, issued as a software token for natural persons, prohibiting the use of pseudonyms.	HETSN
1.3.6.1.4.1.21528.2.1.1.158	Certificate Policy for Non eIDAS covered, certification class III. certificates, issued as a software token for legal persons, prohibiting the use of pseudonyms.	HEJSN
1.3.6.1.4.1.21528.2.1.1.223	Certificate Policy for Non eIDAS covered, certification class III. certificates, prohibiting the use of pseudonyms.	HExxN
1.3.6.1.4.1.21528.2.1.1.227	Certificate Policy for Non eIDAS covered, certification class III. code signing certificates, issued on Cryptographic Hardware Device, prohibiting the use of pseudonyms.	HKxHN
1.3.6.1.4.1.21528.2.1.1.237	Certificate Policy for Non eIDAS covered, certification class III. WRPAC certificates, issued as a software token for legal persons, prohibiting the use of pseudonyms.	HZJSN
1.3.6.1.4.1.21528.2.1.1.226	Certificate Policy for Non eIDAS covered, certification class II. certificates, issued for legal persons, prohibiting the use of pseudonyms.	KEJxN
1.3.6.1.4.1.21528.2.1.1.225	Certificate Policy for Non eIDAS covered, certification class II. certificates, issued for natural persons, prohibiting the use of pseudonyms.	KETxN
1.3.6.1.4.1.21528.2.1.1.221	Certificate Policy for Non eIDAS covered, certification class II. certificates, issued on Cryptographic Hardware Device, prohibiting the use of pseudonyms.	KExHN
1.3.6.1.4.1.21528.2.1.1.160	Certificate Policy for Non eIDAS covered, certification class II. certificates, prohibiting the use of pseudonyms.	KExxN
1.3.6.1.4.1.21528.2.1.1.228	Certificate Policy for Non eIDAS covered, certification class II. code signing certificates, issued on Cryptographic Hardware Device, prohibiting the use of pseudonyms.	KKxHN
1.3.6.1.4.1.21528.2.1.1.231	Certificate Policy for S/MIME certificates, prohibiting the use of pseudonyms.	xSxxN

>

The rules of the formation and interpretation of the Certificate Policy short names can be found in the Appendix of this document.

<ALA: The Certification Service Provider doesn't issue Certificates with pseudonym. >

<UNI: The Certification Service Provider doesn't issue Certificates with pseudonym. >

The detailed requirements of the listed Certificate Policy(s) can be found in " e-Szignó Certification Authority – Unified Certificate Policies ver.3.20." [77].

[[ADV:

<ALA:

Based on these Certificate Policies the Certification Service Provider issues Certificates that are appropriate for eIDAS Regulation [1] advanced electronic signature or seal creation. The documents with advanced with electronic signature or seal meets the requirements for phrasing.

>

The issuance of Certificate belonging to the III. certification class is bound to preliminary personal identification done by the Certification Service Provider, at class II. Certificate issuance, remote registration is permitted as well.

]]

<not TLS:

<not SEA:

In case of Certificate Policies concerning Certificates issued to natural persons, the Subject is always a natural person.

>

<not SIG:

In case of Certificate Policies concerning Certificates issued to non-natural persons, the Subject is a legal person.

>

The denomination of the IT systems, applications and automatism by the help of the Certificate can be used, can be indicated within the Certificates (Certificate for Automatism).

>

<TLS:

In case of Website Authentication Certificates at the name of the Subject the domain name *[[ADV: or IP address]]* is indicated.

The Website Authentication Certificate cannot be pseudonymous.

>

<BEL:

All of the present Certificate Policies prohibit the use of pseudonyms, the real name of the Subject is indicated on the Certificate in all cases.

>

[[QUA:

<not TLS:

In case of Certificate Policies ([xxxBx]) requiring the usage of a Qualified Electronic Signature or Seal Creation Device, the Certification Service Provider shall make sure that the private key associated with the Certificate is located in a Qualified Electronic Signature or Seal Creation Device, verified by a certification body registered in a member state of the European Union.

>

]]

<not TLS:

[[QUA:

In case of a Certificate Policy ([xxxHx]) that requires the usage of Cryptographic Hardware Device, the Certification Service Provider guarantees that the private key belonging to the Certificate is stored only on such Cryptographic Hardware Device that has at least one of the following certifications:

- **Certificate issued in any of the member states of the European Union certifying that the equipment is a Qualified Electronic Signature or Seal Creation Device**
- **Common Criteria [72] certification according to CEN SSCD PP [73], at least at level EAL-4**
- **an EAL-4 or higher level Common Criteria [72] certificate according to CEN 419 221-5 [35]**
- **FIPS 140-2, Level 2 (or higher) certification [69]**
- **FIPS 140-3, Level 2 (or higher) certification [70].**

]]

>

<UNI:

In case of a Certificate Policy ([xxxHx]) that requires the usage of Cryptographic Hardware Device, the Certification Service Provider guarantees that the private key belonging to the Certificate is stored only on such Cryptographic Hardware Device that has at least one of the following certificates:

- certificate issued in any of the member states of the European Union certifying that the equipment is a Qualified Electronic Signature or Seal Creation Device
- an EAL-4 or higher level Common Criteria [72] certificate according to CEN SSCD PP [73], at least at level EAL-4
- an EAL-4 or higher level Common Criteria [72] certificate according to CEN 419 221-5 [35]
- FIPS 140-2, Level 2 (or higher) certificate [69]
- FIPS 140-3, Level 2 (or higher) certificate [70].

>

[[QUA:

<not TLS: <not UNI:

Qualified Certificate based advanced electronic signature or seals can be created automatically, and without direct supervision with an IT equipment specified in the legislation.

>>

<not TLS:

Certificates that comply with Certificate Policies that require the usage of a Qualified Electronic Signature or Seal Creation Device or Cryptographic Hardware Device may be issued for usage in a remote key management service, if

- **the remote key management service is provided by a Qualified Trust Service Provider,**
- **the private keys of the users are managed in Qualified Electronic Signature or Seal Creation Device or Cryptographic Hardware Device devices having the proper certificates,**
- **a conformity assessment report, created by an independent accredited auditor, proofs that the remote key management service fulfils the relevant requirements,**
- **the Qualified Trust Service Provider declares in writing that it manages the private key belonging to the public key to be indicated in the Certificate in Qualified Electronic Signature or Seal Creation Device or Cryptographic Hardware Device, respectively, in accordance with the device certification.**

The private key belonging to a Certificate issued based on Certificate Policies ([xxxBx]) that require the usage of a Qualified Electronic Signature or Seal Creation Device, is protected by a Qualified Electronic Signature or Seal Creation Device. Qualified electronic signature or seal can be created only on the basis of such Certificate.

If a qualified Certificate Policy doesn't require the usage of a Qualified Electronic Signature or Seal Creation Device, an advanced electronic signature or seal can be created based on that qualified Certificate issued according to that policy.

A document, with a qualified electronic signature or seal or with advanced electronic signature or seal based on a qualified Certificate under paragraph 325 of Act CXXX of 2016 on Civil Procedure [12] is representing conclusive evidence (in Hungary).

>

]]

<TLS:

[[QUA:

When the Certificate is issued for website authentication:

]]

- The Certification Service Provider conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates [63] published at

https://cabforum.org/baseline-requirements-documents/

URL.

In case of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

[[QUA:

- **The Certification Service Provider conforms to the current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates [65] published at**

  https://cabforum.org/extended-validation/

  URL.

  In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

]]

>

<not TLS:

<not UNI:

The **[[QUA: qualified]]** signing Certificates issued in accordance with the <ALA: **[[QUA: [MATBN], [MATHN], [MATSN] Certificate Policies]]** *[[ADV: [HATHN], [HATSN] Certificate Policy]]* > <BEL: **[[QUA: [MBJBN], [MBJHN], [MBJSN] Certificate Policies]]** *[[ADV: [HBJHN], [HBJSN] Certificate Policy]]* > fully comply with the requirements of the related legislation, like the (Hungarian) Government Decree 137/2016. (VI. 13.) on the requirements for the use of electronic signatures and stamps related to the provision of electronic administration services (later E-Signature Government Decree) [16] and the private keys belonging to them can be used for creating electronic signature or seals for public administration use.

In case of the Email (S/MIME) Certificate the Certification Service Provider conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates" [62] published at

https://cabforum.org/smime-br/

URL.

If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

> >

<UNI:

In case of the Code Signing Certificate the Certification Service Provider conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" [64] published at

https://cabforum.org/baseline-requirements-code-signing/

URL.

If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

In case of the Email (S/MIME) Certificate the Certification Service Provider conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates" [62] published at

`https://cabforum.org/smime-br/`

URL.

If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

>

Among the present Certificate Policies:

<TLS:

[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard*
- *each Certificate Policy complies with the [DVCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard, if the organization name is not indicated in the Certificate*
- *each Certificate Policy complies with the [OVCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard, if the organization name is indicated in the Certificate*

]]

[[QUA:

- **each Certificate Policy complies with the [NCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard**
- **Differentiated according to the area of use of Certificate:**
  - **When the issued Certificate can also be used to authenticate websites:**
    - **each Certificate complies with the [QEVCP-w] Certificate Policy defined in the ETSI EN 319 411-2 [24] standard**
    - **each Certificate issued for PSD2 purposes complies also with the [QCP-w-psd2] Certificate Policy defined in the ETSI TS 119 495 [34] specification.**
  - **When the issued Certificate cannot be used to authenticate websites:**
    - **each Certificate complies with the [QNCP-w-gen] Certificate Policy defined in the ETSI EN 319 411-2 [24] standard**
    - **each Certificate issued for PSD2 purposes complies also with the [QCP-w-psd2] Certificate Policy defined in the ETSI TS 119 495 [34] specification.**

]]

>

<ALA:

[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard*
- *except the [KATxN] and [KKTxN] Certificate Policy each Certificate Policy complies with the [NCP] Certificate Policy*

]]
[[QUA:

- **each Certificate Policy complies with the [QCP-n] Certificate Policy defined in the ETSI EN 319 411-2 [24] standard**
- **the [MATBN] Certificate Policy complies with the [QCP-n-qscd] Certificate Policy**
- **the [MSxxN] Certificate Policy complies with the [QCP-n-qscd] Certificate Policy, when the Certificate issued on Qualified Electronic Signature or Seal Creation Device**
- **the [MATHN] Certificate Policy complies with the [NCP+] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard.**

]]
>
<BEL:
[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard*
- *except the [KBJxN] and [KKJxN] Certificate Policy each Certificate Policy complies with the [NCP] Certificate Policy.*

]]
[[QUA:

- **each Certificate Policy complies with the [QCP-l] Certificate Policy defined in the ETSI EN 319 411-2 [24] standard**
- **the [MBJBN] Certificate Policy complies with the [QCP-l-qscd] Certificate Policy**
- **the [MSxxN] Certificate Policy complies with the [QCP-l-qscd] Certificate Policy, when the Certificate issued on Qualified Electronic Signature or Seal Creation Device**
- **the [MBJHN] Certificate Policy complies with the [NCP+] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard.**

]]
>
<UNI:

- each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [23] standard
- the [HETHN], [HETSN] és [HEJSN], [HExxN], [HKxHN] and [HZJSN] Certificate Policys comply also with the [NCP] Certificate Policy
- the [HETHN] Certificate Policy complies also with the [NCP+] Certificate Policy
- the private key belonging to the Certificates issued according to the [KExHN] Certificate Policy are issued on Cryptographic Hardware Device

>

Compliance with the ETSI Certificate Policies

In cases when an ETSI Certificate Policy is based on another ETSI Certificate Policy and this way contains all the requirements of it, only the Identifier of the Higher Level Certificate Policy is referenced in the issued Certificates.

<TLS:

[[QUA:

When the issued Certificate can also be used to authenticate websites:

	[NCP]	[EVCP]	[QEVCP-w]	[QCP-w-psd2]
MWJSN (website)	(x)	(x)	X	
MWJSN (Open Banking)	(x)	(x)	X	
MWJSN (PSD2)	(x)	(x)	X	X

When the issued Certificate cannot be used to authenticate websites:

	[NCP]	[QNCP-w-gen]	[QCP-w-psd2]
MPJSN (Open Banking)	(x)	X	
MPJSN (PSD2)	(x)	X	X

]]

[[ADV:

	[LCP]	*[DVCP]*	*[OVCP]*
HWJSN	*(x)*		*X*
KWJSN	*(x)*		*X*
AWxSN	*(x)*	*X*	

]]

>

<ALA:

[[QUA:

	[QCP-n]	[QCP-n-qscd]	[NCP+]
MATBN	(x)	X	
MATHN	X		X
MATSN	X		
MSxxN	X		
MSxxN (on QSCD)	(x)	X	

]]
[[ADV:

	[LCP]	*[NCP]*	*[NCP+]*
HATHN	*(x)*	*(x)*	*X*
HATSN	*(x)*	*X*	
KATxN	*X*		

]]
>
<BEL:
[[QUA:

	[QCP-l]	[QCP-l-qscd]	[NCP+]
MBJBN	(x)	X	
MBJHN	X		X
MBJSN	X		
MSxxN	X		
MSxxN (on QSCD)	(x)	X	

]]
[[ADV:

	[LCP]	*[NCP]*	*[NCP+]*
HBJHN	*(x)*	*(x)*	*X*
HBJSN	*(x)*	*X*	
KBJxN	*X*		

]]
>
<UNI:

	[LCP]	[NCP]	[NCP+]
HETHN	(x)	(x)	X
HETSN	(x)	X	
HEJSN	(x)	X	
HExxN	(x)	X	
HKxHN	(x)	X	
HZJSN	(x)	X	
KEJxN	X		
KETxN	X		
KExHN	X		
KExxN	X		
KKxHN	X		
xSxxN	X		

>

1.2.2 Effect

Subject Scope

The Certification Practice Statement is related to the provision and usage of the services described in section 1.3.1.

Temporal Scope

The present version of the Certification Practice Statement is effective from the 2026-05-13 date of effect, until withdrawal. The effect automatically terminates at the cessation of the services or at the issuance of the newer version of the Certification Practice Statement.

Personal Scope

The effect of the Certification Practice Statement extends each of the participants mentioned in section 1.3.

The Certification Service Provider provides trust services primarily to citizens of the European Union and organizations registered in the European Union, but does not exclude natural or legal persons from other countries as long as they accept the system of rules followed by the Certification Service Provider and the controls necessary to provide the services can be done safely and economically.

People with disabilities

The Certification Service Provider strives to ensure equal opportunity access to the services provided by the company to the highest possible standards.

In order to establish equal opportunities regarding the service, the Certification Service Provider applies every possible and reasonable measure to make its services available without obstructions

to disabled people as well. It is especially important them to ensure that the disabled clients receive services, which are adapted to their special needs, of the same quality as those for the other clients.

The Certification Service Provider cooperates with clients in order to guarantee them an administrative process which is the most suitable for their personal needs within the framework determined by the Certification Practice Statement.

Geographical Scope

The present Certification Practice Statement based on the European Union requirements includes Hungarian specific requirements for services operating under the Hungarian law in Hungary.

The Certification Service Provider may extend the geographical scope of the service, in this case it shall use not less stringent requirements than those applicable in the Certification Practice Statement. At services provided to foreign Clients, detailed conditions that differ from the Certification Practice Statement may be regulated in a specific service agreement.

The service provided according to the present Certification Practice Statement is available worldwide. The validity of the Certificates, Certificate Revocation Status Lists and OCSP responses issued according to the present Certification Practice Statement is independent of the geographical location where they were requested from, and where they will be used.

The service provided according to the present Certification Practice Statement can be only used as described in the present Certification Practice Statement and in the Certificate Policy.

1.2.3 Security Levels

The Certification Service Provider defined security levels by taking into account the relevant requirements as follows.

The authentication strength of the Certificate Subject in descending order:

- [M****] qualified Certificates
- [H****] non-qualified III. certification class Certificates issued by e-Szignó Certification Authority
- [K****] non-qualified II. certification class Certificates issued by e-Szignó Certification Authority
- non-qualified Certificates issued not by the e-Szignó Certification Authority.

Based on the used container in descending order by security:

- [***B*] Certificates issued on Qualified Electronic Signature or Seal Creation Device
- [***H*] Certificates issued on Cryptographic Hardware Device
- [***S*] otherwise, for example Certificates issued by software

By taking into account the two points of view the Certification Service Provider established the following aggregated order in descending order of security:

- [M**B*] qualified Certificates issued on Qualified Electronic Signature or Seal Creation Device
- [M**H*] qualified Certificates issued on Cryptographic Hardware Device
- [M**S*] qualified otherwise, for example Certificates issued by software
- [H**S*] non-qualified, III. certification class Certificates issued by e-Szignó Certification Authority
- [K**S*] non-qualified, II. certification class Certificates issued by e-Szignó Certification Authority
- non-qualified Certificates issued by other CA than e-Szignó Certification Authority

During the communication with the Clients the Certification Service Provider supports the use of electronic channels and enables the use of electronic signature or seal during the administration in most cases possible.

It is a general rule, that during the administration related to the Certificates, the Client can use its own signing Certificate to verify the electronic documents, if its level of security according to the aforementioned list is not lower than the relevant Certificate.

On an individual basis in special cases, the Certification Service Provider can deviate from the strict application of the above list with regard to particular tasks (for example the personal identification for III. certification class Certificates in case of new qualified Certificate Application or the modification of an existing one as a result of the same procedural identification rules it accepts the identification required for qualified Certificate).

1.3 PKI Participants

The participants applying the services provided within the framework of present Certification Practice Statement consist of the following:

- the Microsec e-Szignó Certification Authority
- the Clients of Microsec e-Szignó Certification Authority (Subscribers and Subjects)
- Relying Parties
- other participants.

1.3.1 Certification Authorities

Data of the Certification Service Provider

Name:	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number:	01-10-047218 Company Registry Court of Budapest
Head office:	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number:	+36-1 505-4444
Fax number:	+36-1 505-4445
Internet address:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

Customer Service Office

The name of the provider unit:	e-Szignó Certification Authority
Customer service:	
	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building SP3
Office hours of the customer service:	on workdays between 8:30-16:30 by prior arrangement
Telephone number of the customer service:	+36-1 505-4444
Email address of the customer service:	`info@e-szigno.hu`
Send revocation request to:	`revocation@e-szigno.hu`
Service related information access:	`https://www.e-szigno.hu`
Place for registering complaints:	Microsec ltd. Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building SP3
Relevant Consumer Protection Inspectorate:	Budapest Capital Authority for Consumer Protection 1052 Budapest, Városház str. 7. 1364 Budapest, Pf. 144.
Relevant Arbitration Board:	Arbitration Board of Budapest 1016 Budapest, Krisztina krt. 99. III. em. 310. Mailing address: 1253 Budapest, Pf.: 10.

Introduction of the Certification Service Provider

Microsec ltd. is an EU qualified trust service provider according to the 910/2014/EU Regulation [1] (hereinafter: eIDAS).

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [7] (hereinafter: Eat.):

- provides non-qualified electronic signature certification services, time stamping, and placement of signature-creation data on signature creation devices services according to Eat. since May 30, 2002 (registration number: MH 6834 1/2002.)
- provides qualified electronic signature certification services, time stamping, and device services according to Eat. since May 15, 2005
- provides qualified long term preservation service according to Eat. since February 1, 2007. (reference number of the decision on the registration: HL-3549-2/2007).

On the 1st of July, 2016. the whole system of services related to electronic signatures changed uniformly on a European basis with eIDAS and its complement Act CCXXII of 2015. [11] coming into force.

Microsec provides its non-qualified trust services conformant to eIDAS furthermore started the issuance of eIDAS qualified signing certificates for natural persons from the 1st of July 2016.

Microsec provides the following qualified trust services conformant to eIDAS form the 20th of December 2016:

- qualified certificates for electronic seals
- qualified time stamping
- qualified archiving (preservation of electronic signatures and seals).

Microsec provides the following qualified trust service conformant to eIDAS form the 2nd of January 2019:

- qualified certificates for website authentication.

Microsec provides the following qualified trust service component conformant to eIDAS form the 29th of May 2020:

- remote key management service suitable for creating qualified electronic signatures and seals.

Quality and Information Security

Microsec highlights the importance of Client experience. In order to maintain a high level of services, Microsec has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002.

Microsec assigns high priority to the security of the systems it operates and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003.

The scope of both the quality control system and the information security management system covers the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly.

Based on the results of the risk assessment the Certification Service Provider

- sets up new measures to eliminate the vulnerabilities, or/and
- accepts the identified residual risks by stating the reason of the decision.

See:

`https://www.microsec.hu/en/quality-assurance-and-audit`

The Certification Service Provider makes available for all interested parties its Information Security Policy on its web page on the following link:

`https://www.microsec.hu/en/quality-assurance-and-audit`

Any change to the Information Security Policy is communicated to third parties via this web page.

Changes to the information security policy is communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

Due to their confidential nature the Certification Service Provider doesn't disclose its internal Security Rules. The Certification Service Provider informs its subcontractors, contractors and other interested parties concerned of the security rules applicable to them when concluding the contract.

Business Providing Certification Services

Operating as an independent business unit within the organization of Microsec, e-Szignó Certification Authority is responsible for creation and management of Certificates, publication of Certificate repository and Certificate revocation status information, management and delivery of Electronic Signature or Seal Creation Devices, provision of the online certificate status service, and tasks related to the management of policies and practices.

The e-Szignó Certification Authority has its own Registration Authority.

Services

The Certification Service Provider provides the following <not UNI: trust> services <not UNI: defined by the eIDAS Regulation [1] > to the Subscriber within the framework of the present Certification Practice Statement:

<TLS:

[[ADV:

- *Issuance of non-Qualified Certificates for Website Authentication*

]]

[[QUA:

- **Issuance of Qualified Certificates for Website Authentication**

]]

> <ALA:

- Issuance of

  [[QUA:

  Qualified

  ]]

  Certificates for Electronic Signatures

> <BEL:

- Issuance of

  [[QUA:

  Qualified

  ]]

  Certificates for Electronic Seals

> <UNI:

- Issuance of Non-eIDAS Certificates

>

[[QUA:

The Certification Service Provider provides its services within the framework of the present Certification Practice Statement as a qualified trust service provider.

]]

The Certification Service Provider to provide the service signs a service agreement with the Subscriber, within the confines of it issues **[[QUA: qualified]]** Certificate(s) to the Subjects specified by the Subscriber. The Certificate provides a certified connection between the data of the identified Subject and the public key belonging to the private key that the Subject holds. Within the framework of a service agreement, multiple Certificates can be issued to multiple Subjects.

<TLS:

In case of a Website Authentication Certificate, the Subject is a webserver which is identified by the domain name *[[ADV: or IP address]]* indicated in the Certificate. The Applicant is that natural person, who acts during Certificate Application.

>

<not TLS: <not UNI:

[[QUA:

In case of using a qualified Certificate issued based on present Certification Practice Statement, if the electronic signature or seal was created by a Qualified Electronic Signature or Seal Creation Device, the electronic signature or seal is a qualified electronic signature or seal. If the electronic signature or seal was not created by a Qualified Electronic Signature or Seal Creation Device then the electronic signature or seal is an advanced electronic signature or seal based on qualified certificate. A document verified by a qualified electronic signature or seal or an advanced electronic signature or seal based on a qualified certificate under the paragraph 325 of Act CXXX of 2016 on Civil Procedure [12] considered as a private document providing a full probative value.

]]

>>

In case of a valid a subscription, the Subject or Applicant may initiate the following actions:

- Subject or Applicant may apply for a Certificate <not TLS: <not UNI: (and a Electronic Signature or Seal Creation Device in addition) >> from the Certification Service Provider, the Certificate issuance is performed according to a Certificate Policy or policies

- the Subject or Applicant may request the revocation of its Certificate

<not TLS:

- the Subject or Applicant may request the suspension and reinstation of its Certificate.

> The Subscriber may also request the <TLS: revocation> <not TLS: revocation, suspension or reinstation> of the belonging Subject's Certificate.

These actions may also be requested by the Organizational Administrator authorized by the Subscriber and registered by the Certification Service Provider.

The Certification Service Provider makes the Certificate Revocation Lists publicly available, containing the revocation status of the issued Certificates. The Certification Service Provider also makes the Certificate public, based on the Subject or Applicant's consent. The <not TLS: suspended, > revoked or expired Certificate is invalid.

<ALA:

Signatures created with an invalid Certificates do not have any legal effect.

>

<BEL:

Seals created with an invalid Certificates do not have any legal effect.

>

The Certification Service Provider also issues test certificates with the purpose of testing its system. The test certificates do not have any legal effect.

Upon requests the Certification Service Provider may issue free Certificates for testing purposes on an individual bases. The Certificates issued this way need to be managed prudently because they have the same legal effect as the normal Certificates.

Certificate Types

The Certificate Policies supported by the present Certification Practice Statement are presented in section 1.2.1.

The ID of the applied Certificate Policy is always indicated in the "Certificate Policies" field of the Certificate.

The e-Szignó Certification Authority provides various certificate types for its Clients, which mainly differ concerning their properties and data authentically bound to the Subject.

<TLS:

- Organizational Certificate means a Certificate wherein the Certificate attests the relationship of an Organization with the domain name *[[ADV: or IP address]]* included in it. In this case the name of the Organization is included in the "O" field of the Certificate.

  The name of an Organization can be indicated in a Website Authentication Certificate only if the Organization is the legal user, owner of the domain *[[ADV: or IP address]]* or has the authorisation of them.

>

<not TLS:

- Organizational Certificate means a Certificate wherein the Subject is an Organization, a device under the control of the Organization or the Certificate attests the relationship of a natural person Subject with the Organization. In this case, the name of the Organization is indicated in the "O" field of the Certificate.

>
<not TLS: <not SEA:

- Certificate for Profession means a Certificate issued to a natural person which is not an Organizational Certificate and which contains the title or profession of the Subject in the "Title" field.

>>
<not TLS:

- Certificate for Automatism means a Certificate wherein the denomination of the IT device (application, system) is indicated amongst the Subject data in the Certificate, by the help of the Subject uses the Certificate.
- Pseudonymous Certificate means a Certificate wherein not the official – verified by the Certification Service Provider – denomination of the Subject is in the Certificate. In the pseudonymous Certificates the requested name is indicated in the "Pseudonym" field, and it is stated in the "CN" field that the Certificate contains a pseudonym.

>
<not TLS: <not UNI:
[[QUA:

- **Certificates requiring Qualified Electronic Signature or Seal Creation Device usage: In that case the Certificate was issued to a public key for which the corresponding private key was generated on a Qualified Electronic Signature or Seal Creation Device – so it is guaranteed that the private key can not be extracted and copied –, then that information is indicated on the Certificate in the "QCStatements" field. Qualified electronic signature or seal can be created only based on a Certificate this type.**

]]
>>
<not TLS:

- Personal Certificate means a Certificate that does not contain either an "O" or a "Title" field. This type can only be issued to natural persons.

>
The e-Szignó Certification Authority issues Certificates for natural persons and legal persons. In case of Certificates issued to legal persons the authorized representative natural person or a trustee authorized by the representative need to act on behalf of the legal person.

Test Certificates

The Certification Service Provider issues test Certificates – firstly to test their system, on the other hand, to third parties in order to test the services. No legal effect belongs to the test Certificates, and the Certification Service Provider does not take any responsibility for their issuance, usage and service availability.

The Certification Service Provider does not issue test Certificates under the top level service provider (root) Certification Unit.

The issuance of the test Certificates is done under the "Microsec e-Szigno Test Root CA 2008" and the "Test e-Szigno Root CA 2017" roots exclusively created and operated for this task.

The Certification Service Provider indicates the test Certificates in the "Certificate Policies" field according to the following (see section 7.1.2):

- the 1.3.6.1.4.1.21528.2.1.1.9 OID is indicated as a Certificate Policy in the Certificate, or
- the 1.3.6.1.4.1.21528.2.1.1.100 OID is indicated as a Certificate Policy in the Certificate, or
- no Certificate Policy is indicated in the Certificate.

<not TLS: <not UNI:

Device Service

Within the confines of the device service Certification Service Provider

[[QUA:

puts the Certificate related signature- or seal-creation data of the Subject on an Electronic Signature or Seal Creation Device which complies with the Qualified Electronic Signature or Seal Creation Device requirements defined in eIDAS Regulation [1]. The usage of these Qualified Electronic Signature or Seal Creation Devices is prerequisite for the creation of qualified electronic signature or seals.

]]

[[ADV:

puts the Certificate related signature- or seal-creation data of the Subject on a Electronic Signature or Seal Creation Device.

]]

>>

Certification Units

Below we present the Certification Units appearing in the e-Szignó Certification Authority system and falling under the scope of this Certification Practice Statement. Further information about the Certification Service Provider's certificate hierarchy can be found via the website

`https://e-szigno.hu/ca-certificates`

RSA-based multipurpose eIDAS hierarchy - 2025

RSA-based multipurpose hierarchy independent of the Root Programs.
Each Certification Unit in this hierarchy uses 4096-bit RSA keys.

- "e-Szigno RSA Root CA 2025" – Root certification unit,
  issues subordinate Certificates for the Certification Units.
  This Certification Unit has a self-signed Certificate, based on 4096-bit RSA key.

[[QUA:
<not TLS:

- **"e-Szigno RSA Qualified CA 2025"**
  This Certification Unit issues qualified Certificates on Qualified Electronic Signature or Seal Creation Device in the "e-Szigno RSA Root CA 2025" hierarchy, to create qualified electronic signatures and qualified electronic seals.

>

- **"e-Szigno RSA Qualified QCP CA 2025"**
  This Certification Unit issues qualified Certificates for keys residing not on Qualified Electronic Signature or Seal Creation Devices in the "e-Szigno RSA Root CA 2025" hierarchy.
  This Certification Unit issues can issue also such qualified Website Authentication Certificates, which are not intended to be used for website authentication (like PSD2 QWAC).

]]
[[ADV:

- *"e-Szigno RSA CA 2025"*
  This Certification Unit issues not-qualified Certificates in the "e-Szigno RSA Root CA 2025" hierarchy.

]]
In this hierarchy, all the issued end-user Certificates use at least 3072-bit RSA or 256-bit ECC keys.
<TLS:

RSA-based hierarchy dedicated to TLS - 2025

RSA-based dedicated hierarchy exclusively for issuing Website Authentication Certificates, in line with the new requirements of the Root Programs. The issued Certificates contain only "serverAuth" EKU.
Each of the Certification Units in this hierarchy uses at least a 3072-bit RSA key-based Certificate.
In accordance with the requirements of the "Chrome Root Program Policy" [68]:

- The certificates of the intermediate Certification Unit entities used in the hierarchy have a short validity period (3 years)
- Certification Authority uses a Certification Unit to issue new end-user Certificates for a maximum of one year; issuance is then regularly transferred to newly created Certification Units.
- "e-Szigno RSA TLS Root CA 2025" – Root certification unit

  issues subordinate Certificates for the Certification Units.

  This Certification Unit has a self-signed, 4096-bit RSA key-based Certificate.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

[[QUA:

- **"e-Szigno RSA Qualified TLS CA 2026"**

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170 Certificate Policy in the "e-Szigno TLS Root CA 2023" hierarchy.

]]
[[ADV:

- *"e-Szigno RSA DV TLS CA 2025"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno RSA TLS Root CA 2025" hierarchy.
- *"e-Szigno RSA OV TLS CA 2025"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno RSA TLS Root CA 2025" hierarchy.
- *"e-Szigno RSA DV TLS CA 2026"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno RSA TLS Root CA 2025" hierarchy.
- *"e-Szigno RSA OV TLS CA 2026"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno RSA TLS Root CA 2025" hierarchy.

]]
In this hierarchy, all issued end-user Certificates use at least a 2048-bit RSA key.
>
<TLS:
[[QUA:

ECC-based multipurpose eIDAS hierarchy - 2024

ECC-based multipurpose hierarchy independent of the Root Programs for issuing special purpose Certificates.
Each Certification Unit in this hierarchy uses at least 384-bit ECC keys.

- **"e-Szigno Root CA 2024" – Root certification unit,**
  issues subordinate Certificates for the Certification Units.
  This Certification Unit has a self-signed Certificate, based on 384-bit ECC key.

- **"e-Szigno Qualified TLS CA 2024"**
  This Certification Unit issues such qualified Website Authentication Certificates in the "e-Szigno Root CA 2024" hierarchy, which are not intended to be used for website authentication (like PSD2 QWAC)

- **"e-Szigno Qualified TLS CA 2025 EU"**
  This Certification Unit issues such qualified Website Authentication Certificates in the "e-Szigno Root CA 2024" hierarchy, which are not intended to be used for website authentication (like PSD2 QWAC)

In this hierarchy, all the issued end-user Certificates use at least 3072-bit RSA or 256-bit ECC keys.
]]
>
<not TLS:

ECC-based hierarchy dedicated to SMIME - 2024

ECC-based dedicated hierarchy in line with Root Program's new requirements exclusively for issuing Email (S/MIME) Certificates.
Each Certification Unit in this hierarchy uses at least 256-bit ECC keys.

- "e-Szigno SMIME Root CA 2024" – Root certification unit,
  issues subordinate Certificates for the Certification Units.
  This Certification Unit has a self-signed Certificate, based on 384-bit ECC key.

[[QUA:

- **"e-Szigno Qualified SMIME CA 2023"**

  This Certification Unit issues qualified S/MIME Certificates for natural and legal persons according to the qualified S/MIME Certificate Policy ([MSxxN] OID:1.3.6.1.4.1.21528.2.1.1.232) in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is certified also by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

]]

[[ADV:

- *"e-Szigno SMIME CA 2023"*

  This dedicated Certification Unit issues only Email (S/MIME) Certificates in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is certified also by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

]]

In this hierarchy, all the issued end-user Certificates use at least 3072-bit RSA or 256-bit ECC keys.

>

<UNI:

RSA-based hierarchy dedicated to CodeSigning - 2024

RSA-based dedicated hierarchy in line with Root Program's new requirements exclusively for issuing Code Signing Certificates.

Each Certification Unit in this hierarchy uses 4096-bit RSA keys.

- "e-Szigno CodeSigning Root CA 2024" – Root certification unit,

  issues subordinate Certificates for the Certification Units.

  This Certification Unit has a self-signed Certificate, based on 4096-bit RSA key.

- "e-Szigno CodeSigning CA 2024"

  This Certification Unit issues only Code Signing Certificates in the "e-Szigno CodeSigning Root CA 2024" hierarchy.

In this hierarchy, all the issued end-user Certificates use 4096- or 3072-bit RSA keys.

>

<UNI:

[[ADV:

RSA-based hierarchy dedicated to TimeStamps for CodeSigning - 2024

RSA-based dedicated hierarchy in line with Root Program's new requirements, exclusively for issuing RSA-based Time Stamp Certificates for Code Signing Certificates issued by Certification Service Provider.
Each Certification Unit in this hierarchy uses 4096-bit RSA keys.

- *"e-Szigno TSA Root CA 2024" – Root certification unit,*
  issues subordinate Certificates for the Certification Units.
  This Certification Unit has a self-signed Certificate, based on 4096-bit RSA key.

- *"e-Szigno CodeSigning TSA CA 2024"*
  This Certification Unit issues only RSA-based Time Stamp Certificates in the "e-Szigno TSA Root CA 2024" hierarchy.

In this hierarchy, all the issued end-user Certificates use 4096- or 3072-bit RSA keys.

ECC-based hierarchy dedicated to TimeStamps for CodeSigning - 2024

ECC-based dedicated hierarchy in line with Root Program's new requirements, exclusively for issuing ECC-based Time Stamp Certificates for Code Signing Certificates issued by Certification Service Provider.
Each Certification Unit in this hierarchy uses at least 384-bit ECC keys.

- *"e-Szigno ECC TSA Root CA 2024" – Root certification unit,*
  issues subordinate Certificates for the Certification Units.
  This Certification Unit has a self-signed Certificate, based on 384-bit ECC key.

- *"e-Szigno ECC CodeSigning TSA CA 2024"*
  This Certification Unit issues only ECC-based Time Stamp Certificates in the "e-Szigno ECC TSA Root CA 2024" hierarchy.

In this hierarchy, all the issued end-user Certificates use at least 256-bit ECC keys.
]]
>
<TLS:

ECC-based hierarchy dedicated to TLS - 2024

ECC-based dedicated hierarchy exclusively for issuing Website Authentication Certificates, in line with the new requirements of the Root Programs. The issued Certificates contain only "serverAuth" EKU.

Each of the Certification Units in this hierarchy uses at least a 256-bit ECC key-based Certificate.

- "e-Szigno TLS Root CA 2024" – Root certification unit

  issues subordinate Certificates for the Certification Units.

  This Certification Unit has a self-signed, 384-bit ECC key-based Certificate.

[[QUA:

- **"e-Szigno Qualified TLS CA 2025"**

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170 Certificate Policy in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

]]

[[ADV:

- *"e-Szigno DV TLS CA 2025"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno OV TLS CA 2025"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

]]

In this hierarchy, all issued end-user Certificates use at least a 256-bit ECC key.

Due to changes in requirements, this hierarchy has become unnecessary, so the Certification Service Provider plans to terminate the entire hierarchy in the near future.

>

<TLS:

ECC-based hierarchy dedicated to TLS - 2023

ECC-based dedicated hierarchy exclusively for issuing Website Authentication Certificates, in line with the new requirements of the Root Programs. The issued Certificates contain only "serverAuth" EKU.

Each of the Certification Units in this hierarchy uses at least a 256-bit ECC key-based Certificate.

Currently, by default, this system issues ECC key-based Website Authentication Certificates containing only "serverAuth" EKU values.

In accordance with the requirements of the "Chrome Root Program Policy" [68]:

- The certificates of the intermediate Certification Unit entities used in the hierarchy have a short validity period (3 years)
- Certification Authority uses a Certification Unit to issue new end-user Certificates for a maximum of one year; issuance is then regularly transferred to newly created Certification Units.
- "e-Szigno TLS Root CA 2023" – Root certification unit

  issues subordinate Certificates for the Certification Units.

  This Certification Unit has a self-signed, 521-bit ECC key-based Certificate.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

[[QUA:

- **"e-Szigno Qualified TLS CA 2023"**

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170 Certificate Policy in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- **"e-Szigno Qualified TLS CA 2026"**

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170 Certificate Policy in the "e-Szigno TLS Root CA 2023" hierarchy.

]]

[[ADV:

- *"e-Szigno DV TLS CA 2023"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno OV TLS CA 2023"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno DV TLS CA 2026"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

- *"e-Szigno OV TLS CA 2026"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

]]

In this hierarchy, all issued end-user Certificates use at least a 256-bit ECC key.

>

ECC-based multipurpose hierarchy - 2017

ECC-based hierarchy for issuing several types of certificates from dedicated subordinate CA units. Each of the Certification Units in this hierarchy uses at least a 256-bit ECC key-based Certificate.
<TLS:

The issuance of ECC-based Website Authentication Certificates will be gradually migrated to the "ECC-based hierarchy dedicated to TLS - 2023" system.

Currently, exclusively this system issues ECC key-based Website Authentication Certificates containing both "serverAuth" and "clientAuth" EKU values. >

- "e-Szigno Root CA 2017" – Root certification unit

  issues ECC-based Certificates to the Certification Units of the Certification Service Provider.

  This Certification Unit has a self-signed, 256-bit ECC key-based Certificate.

<not TLS:

- "e-Szigno TSA CA 2017"

  This Certification Unit issues only Certificates for Time Stamping Authorities in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- "e-Szigno TSA CA 2020"

  This Certification Unit issues only Certificates for Time Stamping Authorities in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

>

[[QUA:

<TLS:

- **"e-Szigno Qualified TLS CA 2018"**

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170 Certificate Policy in the "e-Szigno Root CA 2017" hierarchy.

>

<ALA:

- **"e-Szigno Qualified CA 2017"**

  This Certification Unit issues qualified Certificates for natural persons excluding pseudonym on Qualified Electronic Signature or Seal Creation Device, according to the [MATBN] (OID:1.3.6.1.4.1.21528.2.1.1.142) Certificate Policy in the "e-Szigno Root CA 2017" hierarchy. The issued Certificates can also be used in public administration.

  The Certification Unit is also certified by the KGYHSZ root.

>

<BEL:

- **"e-Szigno Qualified Organization CA 2017"**

  This Certification Unit issues qualified Certificates for legal persons on Qualified Electronic Signature or Seal Creation Device, according to the [MBJBN] (OID:1.3.6.1.4.1.21528.2.1.1.181) Certificate Policy in the "e-Szigno Root CA 2017" hierarchy.

> <not TLS:

- **"e-Szigno Qualified QCP CA 2017"**

  This Certification Unit issues qualified Certificates for natural and legal persons excluding pseudonym in the "e-Szigno Root CA 2017" hierarchy, according to Certificate Policies that do not require that the private key belonging to the Certificate shall reside on a Qualified Electronic Signature or Seal Creation Device:

  <ALA:

  - **OID:1.3.6.1.4.1.21528.2.1.1.143 [MATHN]**
  - **OID:1.3.6.1.4.1.21528.2.1.1.144 [MATSN]**

  >

  <BEL:

  - **OID:1.3.6.1.4.1.21528.2.1.1.182 [MBJHN]**

– **OID:1.3.6.1.4.1.21528.2.1.1.183 [MBJSN]**

>

The issued Certificates can also be used in public administration.

The Certification Unit is also certified by KGYHSZ root.

This Certification Unit may issue special time stamping Certificates for the Time Stamping Units of the Time Stamping service Providers.

>

<ALA:

- **"e-Szigno Qualified Pseudonymous CA 2017"**

  This Certification Unit issued qualified Certificates for natural persons according to pseudonymous qualified Certificate Policy [MATxA] (OID:1.3.6.1.4.1.21528.2.1.1.148) in the "e-Szigno Root CA 2017" hierarchy.

  Presently it is not used.

>

<not TLS:

- **"e-Szigno Qualified SMIME CA 2023"**

  This Certification Unit issues qualified S/MIME Certificates for natural and legal persons according to the qualified S/MIME Certificate Policy [MSxxN] (OID:1.3.6.1.4.1.21528.2.1.1.232) in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

>

]]

[[ADV:

<not TLS:

- *"e-Szigno Class3 CA 2017"*

  This Certification Unit issues Certificates exclusively for legal and natural persons excluding pseudonyms, according to the III. certification class in the "e-Szigno Root CA 2017" hierarchy.

<UNI:

- *"e-Szigno Class3 CodeSigning CA 2020"*

  This Certification Unit issues exclusively Code Signing Certificates for legal and natural persons excluding pseudonyms according to the III. certification class, for keys residing on Electronic Signature or Seal Creation Device in the "e-Szigno Root CA 2017" hierarchy.

>

- *"e-Szigno Class2 CA 2017"*

  This Certification Unit issues Certificates exclusively for legal and natural persons excluding pseudonyms, according to the II. certification class in the "e-Szigno Root CA 2017" hierarchy.

  This unit does not issue Code Signing Certificate.

<UNI:

- *"e-Szigno Class2 CodeSigning CA 2020"*

  This Certification Unit issues exclusively Code Signing Certificates for legal and natural persons excluding pseudonyms according to the II. certification class, for keys residing on Electronic Signature or Seal Creation Device in the "e-Szigno Root CA 2017" hierarchy.

> <not SEA:

- *"e-Szigno Pseudonymous CA 2017"*

  This Certification Unit issued exclusively pseudonymous Certificates for natural persons according to the II. and III. certification classes in the "e-Szigno Root CA 2017" hierarchy.

  Presently it is not used.

> > <TLS:

- *"e-Szigno Online SSL CA 2017"*

  This Certification Unit issues exclusively Website Authentication Certificates automatically in the "e-Szigno Root CA 2017" hierarchy.

- *"e-Szigno Class3 SSL CA 2017"*

  This Certification Unit issues exclusively Website Authentication Certificates and Certificates for networking authentication according to the III. certification class in the "e-Szigno Root CA 2017" hierarchy.

- *"e-Szigno Class2 SSL CA 2017"*

  This Certification Unit issues exclusively Website Authentication Certificates and Certificates for networking authentication according to the II. certification class in the "e-Szigno Root CA 2017" hierarchy.

>
<UNI:

- *"e-Szigno SMIME CA 2023"*

  This dedicated Certification Unit issues only Email (S/MIME) Certificates in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

>
]]
The aforementioned units have 256-bit ECC key-based Certificates.

In this hierarchy, all issued end-user Certificates use at least a 2048-bit RSA key or at least a 256-bit ECC key.

[[QUA:

<not TLS:

From 2026-01-01, all the issued end-user Certificates use at least a 3072-bit RSA key or at least a 256-bit ECC key.

>
]]

RSA-based multipurpose hierarchy - 2009

RSA-based hierarchy for issuing several types of certificates from dedicated subordinate CA units.

Each of the Certification Units in this hierarchy uses at least a 2048-bit RSA key-based Certificate.

<TLS:

The issuance of RSA-based Website Authentication Certificates will be gradually migrated to the "RSA-based hierarchy dedicated to TLS - 2025" system.

Currently, exclusivel this system issues RSA key-based Website Authentication Certificates containing both "serverAuth" and "clientAuth" EKU values. >

- "Microsec e-Szigno Root CA 2009" – Root certification unit

  issues SHA-256-based Certificates to the Certification Units of the Certification Service Provider.

  This Certification Unit has a self-signed, 2048-bit RSA key-based SHA-256 Certificate.

[[QUA:

<ALA:

- **"Qualified e-Szigno CA 2009"**

  This Certification Unit issues qualified Certificates for natural persons excluding pseudonym on Qualified Electronic Signature or Seal Creation Device, according to the [MATBN] (OID:1.3.6.1.4.1.21528.2.1.1.142) Certificate Policy in the "Microsec e-Szigno Root CA 2009" hierarchy.

> <BEL:

- **"Qualified e-Szigno Organization CA 2016"**

  This Certification Unit issues qualified Certificates for legal persons on Qualified Electronic Signature or Seal Creation Device, according to the [MBJBN] (OID:1.3.6.1.4.1.21528.2.1.1.181) Certificate Policy in the "Microsec e-Szigno Root CA 2009" hierarchy.

> <TLS:

- "Qualified e-Szigno TLS CA 2018"

  This Certification Unit issues Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170) Certificate Policy in the "Microsec e-Szigno Root CA 2009" hierarchy.

- "e-Szigno Qualified TLS CA 2023"

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170) Certificate Policy in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- "e-Szigno Qualified TLS CA 2025"

  This Certification Unit issues only Qualified Website Authentication Certificates according to the [MWJSN] (OID:1.3.6.1.4.1.21528.2.1.1.170) Certificate Policy in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

> <not TLS:

- "Qualified e-Szigno QCP CA 2012"

  This Certification Unit issues qualified Certificates for natural and legal persons excluding pseudonym in the "Microsec e-Szigno Root CA 2009" hierarchy, according to Certificate Policies that do not require that the private key belonging to the Certificate shall reside on a Qualified Electronic Signature or Seal Creation Device:

  <ALA:

  - OID:1.3.6.1.4.1.21528.2.1.1.143 [MATHN]
  - OID:1.3.6.1.4.1.21528.2.1.1.144 [MATSN]

  >

  <BEL:

  - OID:1.3.6.1.4.1.21528.2.1.1.182 [MBJHN]
  - OID:1.3.6.1.4.1.21528.2.1.1.183 [MBJSN]

  >

  This Certification Unit may issue special time stamping Certificates for the Time Stamping Units of the Time Stamping service Providers.

>

<ALA:

- **"Qualified Pseudonymous e-Szigno CA 2009"**

  This Certification Unit issued qualified Certificates for natural persons according to pseudonymous qualified Certificate Policy [MATxA] (OID:1.3.6.1.4.1.21528.2.1.1.148) in the "Microsec e-Szigno Root CA 2009" hierarchy.

  It is currently not in use.

> <not TLS:

- **"e-Szigno Qualified SMIME CA 2023"**

  This Certification Unit issues qualified S/MIME Certificates for natural and legal persons according to the qualified S/MIME Certificate Policy [MSxxN] (OID:1.3.6.1.4.1.21528.2.1.1.232) in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

>

]]

[[ADV:

<not TLS:

- *"Advanced Class 3 e-Szigno CA 2009"*

  This Certification Unit issues Certificates exclusively for legal and natural persons excluding pseudonyms, according to the III. certification class in the "Microsec e-Szigno Root CA 2009" hierarchy.

  This Certification Unit does not issue Code Signing Certificate.

  This Certification Unit may issue special time stamping Certificates for the Time Stamping Units of the Time Stamping service Providers.

<UNI:

- *"Advanced CodeSigning Class3 e-Szigno CA 2016"*

  This Certification Unit issued exclusively Code Signing Certificates for legal and natural persons excluding pseudonyms according to the III. certification class, until 2021-05-31 in the "Microsec e-Szigno Root CA 2009" hierarchy.

>

- *"Advanced Class 2 e-Szigno CA 2009"*

  This Certification Unit issued Certificates exclusively for legal and natural persons excluding pseudonyms, according to the II. certification class until 2016-06-30 in the "Microsec e-Szigno Root CA 2009" hierarchy.

- *"Advanced eIDAS Class2 e-Szigno CA 2016"*

  This Certification Unit issues Certificates exclusively for legal and natural persons excluding pseudonyms, according to the II. certification class since 2016-07-01 in the "Microsec e-Szigno Root CA 2009" hierarchy.

  This Certification Unit does not issue Code Signing Certificate.

<UNI:

- *"Advanced CodeSigning Class2 e-Szigno CA 2016"*

  This Certification Unit issued exclusively Code Signing Certificates for legal and natural persons excluding pseudonyms according to the II. certification class, until 2021-05-31 in the "Microsec e-Szigno Root CA 2009" hierarchy.

> <not SEA:

- *"Advanced Pseudonymous e-Szigno CA 2009"*

  This Certification Unit issued exclusively pseudonymous Certificates for natural persons according to the II. and III. certification classes in the "Microsec e-Szigno Root CA 2009" hierarchy.

  It is currently not in use.

> > <TLS:

- *"Online e-Szigno SSL CA 2016"*

  This Certification Unit issues exclusively Website Authentication Certificates automatically in the "Microsec e-Szigno Root CA 2009" hierarchy.

- *"e-Szigno SSL CA 2014"*

  This Certification Unit issues exclusively Website Authentication Certificates and Certificates for networking authentication according to the III. certification class in the "Microsec e-Szigno Root CA 2009" hierarchy.

- *"Class2 e-Szigno SSL CA 2016"*

  This Certification Unit issues exclusively Website Authentication Certificates and Certificates for networking authentication according to the II. certification class in the "Microsec e-Szigno Root CA 2009" hierarchy.

- *"e-Szigno DV TLS CA 2023"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno DV TLS CA 2025"*

  This Certification Unit issues only DV (Domain Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno OV TLS CA 2023"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2023" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

- *"e-Szigno OV TLS CA 2025"*

  This Certification Unit issues only OV (Organization Validated) Website Authentication Certificates in the "e-Szigno TLS Root CA 2024" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009".

>

<UNI:

- *"e-Szigno SMIME CA 2023"*

  This dedicated Certification Unit issues only Email (S/MIME) Certificates in the "e-Szigno Root CA 2017" hierarchy.

  The Certification Unit is also certified by "Microsec e-Szigno Root CA 2009" and "e-Szigno SMIME Root CA 2024".

>

]]

<not TLS:

Certification units for public administration

The following Certification Units of the Certification Service Provider issue Certificates for the public administration:

[[QUA:

<not UNI:

- **"Qualified KET e-Szigno CA 2009"**

  Productive qualified Certification Unit, certified by KGYHSZ and issued qualified Certificates for public administration usage until 2020-12-17.

- **"Qualified KET e-Szigno CA 2018"**

  Productive qualified Certification Unit, certified by KGYHSZ and "Microsec e-Szigno Root CA 2009" and issues qualified Certificates for public administration usage since 2020-05-13.

>

]]

[[ADV:

- *"Signature KET e-Szigno CA 2009"*

  Productive not qualified Certification Unit, certified by KGYHSZ and "Microsec e-Szigno Root CA 2009" and issued not qualified Certificates for public administration usage until 2020-12-17.

- *"Class3 KET e-Szigno CA 2018"*

  Productive not qualified Certification Unit, certified by KGYHSZ and issues not qualified Certificates for public administration usage since 2020-05-13.

]]

>

The aforementioned units have SHA-256-based Certificates, and issue SHA-256-based Certificates and OCSP responses.

In this hierarchy, all provider certificates use an RSA key with a key length of 2048 or 4096 bits.

In this hierarchy all the issued end-user Certificates use at least a 2048-bit RSA key or at least a 256-bit ECC key.

[[QUA:

<not TLS:

From 2026-01-01, all the issued end-user Certificates use at least a 3072-bit RSA key or at least a 256-bit ECC key.

>

]]

OCSP responders

Each active Certification Unit certifies a separate, dedicated OCSP responder unit that responds to the revocation status of Certificates issued by that Certification Unit.

The OCSP responder unit's name include the text "OCSP Responder" after the name of the given Certification Unit.

The Certificate of OCSP responders includes the "OCSPSigning" extended key usage.

From 2026-01-01, each OCSP responder use at least a 3072-bit RSA key or at least a 256-bit ECC key.

<not TLS:

Retired, RSA and SHA-1 based multipurpose hierarchy - 2005

The Certification Service Provider issued SHA-1 Certificates based "Microsec e-Szigno Root CA" Certification Unit beforehand. The Certification Service Provider does not issue Certificates according to this hierarchy. The Certification Service Provider keeps the SHA-1-based hierarchy for the verifiability of the previously <not UNI: created signatures and Time Stamps. > <UNI: issued Certificates. > The following Certification Units are in the hierarchy:

- "Microsec e-Szigno Root CA"

Root certification unit, which issued SHA-1 based Certificates to the Certification Units of the Certification Service Provider. This Certification Unit has a self-certified certificate.

[[QUA:
<ALA:

- **"Qualified e-Szigno CA"**

  Productive qualified Certification Unit, certified by the "Microsec e-Szigno Root CA" root certification unit. This Certification Unit issued certificates according to the pseudonym exluding qualified certificate policy.

- **"Qualified e-Szigno PCA"**

  Productive qualified Certification Unit, certified by the "Microsec e-Szigno Root CA" root Certification Unit. This Certification Unit issued certificates according to the pseudonymous qualified certificate policy.

- **"Qualified e-Szigno CA7"**

  Productive qualified Certification Unit certified by the Public Administration Root CA. With this Certification Unit the Certification Service Provider issued qualified certificates exclusively according to administrative certificate policies with this certification unit.

- **"Microsec e-Szigno Server CA"**

  The "Microsec e-Szigno Root CA" root Certification Unit, and the KGYHSZ certified it. This Certification Unit certified the SHA-1 based time stamp issuer time stamp units.

>

- **"e-Szigno OCSP CA" (self-certified)**

  The OCSP responder certificate issuer Certification Unit.

- **"e-Szigno OCSP Responder"**

  OCSP responder – certified by "e-Szigno OCSP CA".

]]
[[ADV:

- *"Advanced e-Szigno CA3"*

  This unit issued Certificates to natural persons and automatisms exclusively according to the III. certification class. Certified by "Microsec e-Szigno Root CA". This unit did not issue pseudonymous Certificates.

- *"Advanced e-Szigno CA2"*

  This unit issued Certificates to natural persons and automatisms exclusively according to the II. certification class. This unit issued III. class pseudonymous Certificates. Certified by "Microsec e-Szigno Root CA".

- *"Signature e-Szigno CA6"*

  This unit only issued non-qualified Certificates compliant with public administrative Certificate Policies. The Certificates were Certified by the Public Administrative Root Certification Authority (KGYHSZ).

- *"Microsec e-Szigno Server CA"*

  Certified by "Microsec e-Szigno Root CA" and KGYHSZ. This Certification Unit certified the time stamping units, and issued Certificates compliant with public administrative certificate policies to automatisms.

- *Time stamping units*

  that were certified by "Microsec e-Szigno Server CA". The e-Szignó Certification Authority issued SHA-1 based, non-qualified time stamps with the private keys of these units. The Certificates of the time stamping units contained "timeStamping" extended key usage.

- *"e-Szigno OCSP CA" (self certified)*

  OCSP responder certificate issuer Certification Unit.

- *"Advanced e-Szigno OCSP Responder"*

  OCSP responder – certified by the "e-Szigno OCSP CA".

]]

Intermediate Certification Units in the SHA-1 based hierarchy issued "closing CRLs".

<ALA: The Certification Service Provider terminated the OCSP services serving the SHA-1-based hierarchy in April 2017. The validity of the old electronic signatures can be verified by using the closing CRL-s.

After the 1st of January, 2012 there is no valid certificate used for end-user electronic signing in the Certification Service Provider's SHA-1 based system. Since that date, SHA-1 based time stamps are not issued by the Certification Service Provider.

> >

Publication of the Root Certificates

All Root Certificates are published via the e-Szignó Certification Authority website.

The Certification Service Provider published <not TLS: the hash of the Root Certificates belonging to "Microsec e-Szigno Root CA" and "e-Szigno OCSP CA" in the July 21, 2005 edition of Magyar Nemzet (a Hungarian daily newspaper),> the hash of the "Microsec e-Szigno Root CA 2009" Root Certificate in the June 17, 2010 issue of Expressz (a Hungarian daily newspaper).

<not TLS:

- "Microsec e-Szigno Root CA" Root Certificate
  SHA-1 fingerprint:
  `23 88 c9 d3 71 cc 9e 96 3d ff 7d 3c a7 ce fc d6 25 ec 19 0d,`
  SHA-256 fingerprint:
  `32 7a 3d 76 1a ba de a0 34 eb 99 84 06 27 5c b1 a4 77 6e fd ae 2f df 6d 01 68 ea 1c 4f 55 67 d0`

- "e-Szigno OCSP CA" Root Certificate
  SHA-1 fingerprint:
  56 2c 85 5b 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68,
  SHA-256 fingerprint:
  15 a9 45 a5 e4 92 c8 6c 3e 4e 0e a5 81 4c 9c 43 b0 4f 2e a6 83 1a 64 6c 37 8c d2 b1 82 05 aa 89

>

- "Microsec e-Szigno Root CA 2009" Root Certificate
  SHA-1 fingerprint[1] :
  89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e,
  SHA-256 fingerprint:
  3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8 e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78

- "e-Szigno Root CA 2017" Root Certificate
  SHA-1 fingerprint:
  89 d4 83 03 4f 9e 9a 48 80 5f 72 37 d4 a9 a6 ef cb 7c 1f d1,
  SHA-256 fingerprint:
  be b0 0b 30 83 9b 9b c3 2c 32 e4 44 79 05 95 06 41 f2 64 21 b1 5e d0 89 19 8b 51 8a e2 ea 1b 99

<TLS:

- "e-Szigno TLS Root CA 2023" Root Certificate
  SHA-1 fingerprint:
  6f 9a d5 d5 df e8 2c eb be 37 07 ee 4f 4f 52 58 29 41 d1 fe,
  SHA-256 fingerprint:
  b4 91 41 50 2d 00 66 3d 74 0f 2e 7e c3 40 c5 28 00 96 26 66 12 1a 36 d0 9c f7 dd 2b 90 38 4f b4

[1]The same root (trust anchor) formerly operated with a different Root Certificate. The SHA-1 fingerprint of the former Root Certificate is :
a6 5c b4 73 3d 94 a5 c8 65 a8 64 64 7c 2c 01 27 2c 89 b1 43,
and the SHA-256 fingerprint is:
8e 8c 6e bf 77 dc 73 db 3e 38 e9 3f 48 03 e6 2b 6b 59 33 be b5 1e e4 15 2f 68 d7 aa 14 42 6b 31.
the Certification Service Provider published this fingerprint in the 22 June 2009 issue of Magyar Hírlap (a Hungarian daily newspaper).

The same root also had an even earlier Root Certificate that has been never published in the printed media but has been published in early versions of the Microsec e-Szignó Signature Creation and Verification Program. The SHA-1 fingerprint of this first Root Certificate is:
59 32 E2 00 30 0B AE 8D D7 9D 28 E5 AE 9D B0 05 50 3E 3B 8F,
and the SHA-256 fingerprint is:
72 F9 AF 21 58 18 1B AF 16 D6 0C 9B 4E 6F 4B D7 CA 8D 23 41 AD 48 AF DB 67 CB 4C 83 32 D5 46 F6.
Signatures and Certificates which were verified with the usage of the former Root Certificate can also be considered valid.

>
<TLS:
[[QUA:

- **"e-Szigno Root CA 2024" Root Certificate**
  SHA-1 fingerprint:
  7C 6F E1 33 17 5A 0C FE EA F0 4B 30 80 FD 0E A7 06 8E 5B 7E,
  SHA-256 fingerprint
  F0 59 AF 12 81 59 EF 0B D1 D7 0B 6D 1E BB D2 6D 2A 48 C9 EB 90 61 7C F7 7F C7 B5 9D A8 30 08 97

]]
>
<UNI:

- "e-Szigno CodeSigning Root CA 2024" Root Certificate
  SHA-1 fingerprint:
  B3 5E E3 45 0B 45 E7 C7 10 5E A9 63 10 78 92 42 8E D2 6E 0E,
  SHA-256 fingerprint:
  5A F9 83 53 65 0C 2A C4 99 61 F5 18 83 60 0A E5 C6 11 01 03 5C DD 77 82 82 23 22 12 7F AC EC 6D

>
<BEL:
[[ADV:

- *"e-Szigno TSA Root CA 2024" Root Certificate*
  SHA-1 fingerprint:
  2F A4 43 48 E8 0E 24 0E D0 4B 68 5B E4 DE 79 28 66 95 52 58,
  SHA-256 fingerprint:
  3D 4F B8 4E 00 9C 3A 6E DC 43 89 DF E9 BE 9A 22 39 1D BD 9A BA 19 41 7D 0D 2A 9B A1 02 F0 BC C8

- *"e-Szigno ECC TSA Root CA 2024" Root Certificate*
  SHA-1 fingerprint:
  25 D3 B6 52 BA 24 FD FA CB F1 A0 25 77 87 7D E1 14 72 D0 6A,
  SHA-256 fingerprint:
  81 49 34 F6 10 FB F7 B8 57 9D CA 29 7D 3E BB 3F 66 7F 49 58 E1 8C DC A7 58 48 DE 0E 4C 9C CF 7F

]]
>
<not TLS:

- "e-Szigno SMIME Root CA 2024" Root Certificate
  SHA-1 fingerprint:
  E1 E1 BA 90 DA A5 1E 5D 7B A3 5A 9F 07 04 22 98 8A D4 63 4B,
  SHA-256 fingerprint:
  7A 42 2E C2 37 B4 DA 7D 32 6C 23 22 78 F6 DB E3 29 B0 C9 ED 5A 56 AA FC C1 10 A8 BC 83 ED 0A 96

>
<TLS:

- "e-Szigno TLS Root CA 2024" Root Certificate
  SHA-1 fingerprint:
  18 9A 41 10 80 91 8A 81 8F 77 F8 E0 3A A2 F8 03 86 DD C0 14,
  SHA-256 fingerprint:
  32 8C DF 63 62 2A FB 8A 3F BC 13 47 FD 33 89 F9 18 DA 4A 33 F8 0A F3 45 22 D3 4B 5B DA 9C CB 82
- "e-Szigno RSA TLS Root CA 2025" Root Certificate
  SHA-1 fingerprint:
  7C F1 E2 2E C6 49 B1 03 78 C9 20 AD E0 1C 9C C4 4B C9 7F EC,
  SHA-256 fingerprint:
  9E EF 0C 66 D1 D2 03 40 E4 E5 04 70 1D 3B 87 2B 59 8A 65 ED 7D 59 82 6D 59 E6 5C 5E DD 2B 92 1B

>

- "e-Szigno RSA Root CA 2025" Root Certificate
  SHA-1 fingerprint:
  D6 0F AE 9C 6A 74 FC C9 8E 64 9E CB 52 25 3D 75 1C 67 A8 7A,
  SHA-256 fingerprint:
  DD 2F B3 48 71 E9 0D F4 BB 99 D5 EA 5F 7E BE B8 4D 76 78 6A C5 45 3F E3 35 04 E0 BB DB B3 CA 83

<not TLS:

The following Trusted Root Certificate Stores contain and distribute the "Microsec e-Szigno Root CA" Root Certificate:

- Microsoft Windows certificate store,
- Network Security Services (NSS) certificate store,
- Google Android from the v2.3 (Gingerbread) version,

The expired Root Certificate will be phased out from these Trusted Root Certificate Stores. >

The following Trusted Root Certificate Stores contain and distribute the "Microsec e-Szigno Root CA 2009" Root Certificate:

<TLS:

- Google Chrome since its launch

>

- Google Android from the v2.3 (Gingerbread) version
- Apple iOS from the 7.1.2 version
- Apple Mac OS X from the 10.9.4 version
- Network Security Services (NSS) certificate store from version 3.12.8
- Mozilla Firefox browser from version 3.6.12
- Microsoft Windows certificate store

The following Trusted Root Certificate Stores already contain and distribute the "e-Szigno Root CA 2017" Root Certificate:
<TLS:

- Google Chrome since its launch

>

- Google Android from the v12 (2021-10-04) version.
- Network Security Services (NSS) certificate store from version 3.54,
- Mozilla Firefox browser from version 79
- Microsoft Windows certificate store since September 2021,

<TLS:

The inclusion of the "e-Szigno TLS Root CA 2023" Root Certificate into the Trusted Root Certificate Stores is in process.
The following Trusted Root Certificate Store already contains and distributes the "e-Szigno TLS Root CA 2023" Root Certificate:

- Microsoft Windows certificate store since 2024-03-15
- Network Security Services (NSS) certificate store from version 3.121
- Mozilla Firefox browser from version 149
- Google Chrome since 2026-04-19.

>

The inclusion of the following Root Certificates into the Trusted Root Certificate Stores is in process: <TLS:
[[QUA:

- **"e-Szigno Root CA 2024"**

]]
>
<UNI:

- "e-Szigno CodeSigning Root CA 2024"
- "e-Szigno TSA Root CA 2024"
- "e-Szigno ECC TSA Root CA 2024"

>
<not TLS:

- "e-Szigno SMIME Root CA 2024"

>
<TLS:

- "e-Szigno TLS Root CA 2024"
- "e-Szigno RSA TLS Root CA 2025"

>
The
`https://e-szigno.hu/browser-compatibility`
website contains more information on other browsers and certificate stores that contain the root certificates of the Certification Service Provider by default.

The other Certificates of the Certification Service Provider can be verified based on the self certified Root Certificates, so these Certificates are only published by the Certification Service Provider via its website. If – law or in the framework of a contract or agreement between Certification Service Providers – other Certification Service Provider issues certificates for the Certification Units of the Certification Service Provider, the Certification Service Provider shall publish the Certificates via its website. The Certification Service Provider undertakes that in case of Certificates issued for the Certification Service Provider in this manner, it complies with the cross certifying Certification Service Provider's Certificate Policy and considers the included information binding. <not TLS:
<not UNI:
According to this rule in case of Certificates issued for the public administration the Certification Service Provider follows the Certificate Policy of the Public Administration Root CA (KGYHSZ) [19] and – as a first level CA – considers the included requirements binding.
>>
Before the expiration date of the provider Certificates, the Certification Service Provider generates new provider keys and starts new Certification Units, and takes all the necessary steps, so that the change of the provider Certificates does not endanger the continuity of the services.

Chained Certification Service

The Certification Service Provider has the right to offer a chained certification service, where a Certification Unit of the Certification Service Provider issues a certificate to a Certification Unit controlled by another certification authority (hereinafter: cross-certified CA).

This cross-certification is arranged according to the following requirements:

- The Certification Service Provider and the cross-certified CA conclude a contract, the contract contains the exact conditions of the cross-certification. The cross-certified CA contracts the belonging Clients by itself, within this contract, the cross-certified CA is appointed as the certification authority.
- The Certification Service Provider takes full responsibility for the activities of the chained Certification Authority.
- The cross-certified certification authority can only issue Certificates for a well defined scope of users.
- The cross-certified certification authority shall publish its Certificate Policy, and it shall operate according to it.
- The Certification Service Provider is entitled to verify the operation of the cross-certified provider.
- The Certification Service Provider revokes the Certificate issued during the cross certification if the cross-certified certification authority does not comply with its own Certificate Policy, or if the cross-certified certification authority indicates that its cross certified provider key is compromised.
- If the Certification Service Provider issues provider Certificate for another Certification Authority, it announces the fact to the National Media and Infocommunications Authority. If the cross-certified CA issues Certificates that can be used natively and publicly, the cross-certified CA is bound to announce the cross-certification to the National Media and Infocommunications Authority, and ask for registration (except it is already registered at the National Media and Infocommunications Authority). These rules apply to other services related to electronic signatures as subordinate services (e.g. time stamp).

1.3.2 Registration Authorities

The Certification Service Provider implements registration and other tasks related to the issuing of Certificates, as well as further certificate management tasks centrally, within the framework of a customer service operating within its own organization.

Tasks of the office:

- registration of the Subject indicated on end user Certificates
- administration and registration activity related to the issuing of Certificates <ALA: and Electronic Signature or Seal Creation Devices)> <BEL: and Electronic Signature or Seal Creation Devices)> <UNI: and Electronic Signature or Seal Creation Devices)>

- maintaining contact with Clients (reception of questions, announcements, requests and complaints, and the initiation of their processing)
- performing certificate actions (revocation, <not TLS: suspension, reinstation, > certificate renewal, certificate modification and re-key).

The customer service operated by the Certification Service Provider receives requests pertaining to various Certificate actions and initiates their processing.
The Registration Authority may perform registration activities at the following locations:

- in the customer service office of the Certification Service Provider
- the associate of the Registration Authority may visit Clients and perform mobile registration activities on the site according to the internal statements of the Certification Service Provider.

1.3.3 Subscribers

The Clients of the services provided by the Certification Service Provider:

- Subscriber
  - signs the service agreement with the Certification Service Provider **[[QUA: <TLS: (acts as a Contract Signer in EV term)>]]**
  - accepts the General Terms and Conditions **[[QUA: <TLS: (acts as an Applicant Representative in EV term)>]]**
  - defines the scope of the Subjects or Applicants
  - consent to the inclusion of organizational data in the Certificate
  - may appoint Organizational Administrators
  - responsible for the payment of the fees arising from the usage of the service.

  <TLS:

  [[QUA:

  The Certification Service Provider issues Extended Validation Website Authentication Certificate only for the following type of Subscribers:

  - **Private Organization**
  - **Government Entity**

  ]]

  >

  <not TLS:

- Subject
  - the Certification Service Provider issues the Certificate for the Subject.

>

<TLS:

- Applicant
  - acts during the application for the given Website Authentication Certificate **[[QUA: (acts as a Certificate Requester and Certificate Approver in EV term)]]**

> <ALA:

- creator of the electronic signature or seal
  - the electronic signature certification service user party, who can create electronic signature with the help of the issued Certificate.
    The Subject is the creator of the electronic signature or seal.

> <BEL:

- creator of the electronic signature or seal
  - the electronic seal certification service user party, who can create electronic seal with the help of the issued Certificate.

>

1.3.4 Relying Parties

The Relying Party is not necessarily in a contractual relationship with the Certification Service Provider. The Certification Practice Statement sections 4.5.2, 4.9.6, 9.6.4 and 9.9.3 and the other policies mentioned in it contain the recommendations related to its operation.

The Certification Service Provider maintains its contacts with the Relying Partys mainly via its website.

1.3.5 Other Participants

The independent auditor who makes the conformity assessment audit.

The supervisory authority.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The private keys belonging to the end-user Certificates issued by the Certification Service Provider based on the present Certification Practice Statement can only be used for <TLS: website authentication. >

<ALA: electronic signature or seal creation, with the Certificates the creator of the electronic signature or seal can verify the authenticity of the documents signed by him. > <BEL: electronic signature or seal creation, with the Certificates the creator of the electronic signature or seal can

verify the authenticity of the documents sealed by him. > <UNI: purposes defined in the Certificate attribute values set by the Certification Service Provider, the Certificate Policy and the Certification Practice Statement. The purpose of usage typically can be encryption or authentication, but depending on the concrete usage scope, there can be differences within these in the set attribute values (see section 6.1.7.). >

The Clients are responsible how they use the issued Certificates.

The use of the Certificate in critical infrastructure, where an error in the Certificate or the lack of a valid Certificate may cause serious financial loss or interruption of any critical service, is recommended only if the Client can commit to an urgent and immediate replacement, if the revocation is necessary with short deadline (see in chapter 4.9.1).

<not TLS: <not UNI:

The public key in the Certificate, the Certificate itself, the Certificate Revocation Lists, the Time Stamps and the online revocation status responses can be used for the electronic signature or seal.

>>

1.4.2 Prohibited Certificate Uses

<not TLS: <not UNI:

Provider Certificates

The provider root and intermediate Certificates, and the associated private keys shall not be used for Certificate issuance prior to the disclosure of the provider Certificates.

End-User Certificates

>>

Certificates issued in accordance with the present Certificate Policies, and the private keys belonging to them <TLS: using for other purposes than website authentication is prohibited. It is prohibited to use the Certificate to conduct surreptitious interception by third parties (except with the domain registrant's permission). > <not TLS: <not UNI:

using for other purposes than the generation and verification of electronic signature or seal is prohibited.

>> <UNI:

using for other purposes than purposes defined in the Certificate attribute values set by the Certification Service Provider, the Certificate Policy and the Certification Practice Statement is prohibited.

>

1.5 Policy Administration

1.5.1 Organization Administering the Document

The data of the organization administering the present Certification Practice Statement can be found in the following table:

Organization name	Microsec e-Szignó Certification Authority
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

1.5.2 Contact Person

Questions related to the present Certification Practice Statement can be directly put to the following person:

Contact person	e-Szignó Certification Authority deputy director
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

<TLS:

High-Priority Certificate Problem Report

The Certification Service Provider maintains a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report. The person responsible for the processing of the received reports:

Contact person	Head of Customer Service Department
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.

High Priority Certificate Problem Reports shall be sent to the following email address:

HighPriorityCertificateProblemReport@e-szigno.hu

Further information and a web based incident report form is available on the following URL:

https://e-szigno.hu/security-events-report

The Certification Service Provider is only obliged to process High Priority Certificate Problem Reports submitted in Hungarian or in English, the processing of High Priority Certificate Problem Reports submitted in other languages is uncertain, and the Certification Service Provider may reject them without substantive processing.

Problem reports are processed as described in section 4.9 of the present Certification Practice Statement.

>

<UNI:

Certificate Problem Reports shall be sent to the following email address:

info@e-szigno.hu

Revocation Requests shall be sent to the following email address:

`revocation@e-szigno.hu`

The Certification Service Provider is only obliged to process Certificate Problem Reports and Revocation Requests submitted in Hungarian or in English, the Reports or Requests submitted in other languages is uncertain, and the Certification Service Provider may reject them without substantive processing.

>

1.5.3 Person or Organization Responsible for the Suitability of the Practice Statement for the Certificate Policy

Person responsible for compliance with the present Certification Practice Statement and the Certificate Policy referenced therein is:

Responsible person	e-Szignó Certification Authority director
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	`info@e-szigno.hu`

<not UNI:

The Certification Practice Statements and the provision of the services are supervised by the National Media and Infocommunications Authority. The National Media and Infocommunications Authority maintains a register on the Certificate Policies and on the Certification Service Providers applying these policies.

The register of the National Media and Infocommunications Authority on trust services is available on the following link:

`https://esign.nmhh.hu/bszny/setLanguageAction.do?lang=en`

>

1.5.4 Practice Statement Approval Procedures

Preparing, modifying, acceptance and issuance of a new version of the Certification Practice Statement is implemented according to unified processes as described in detail in section 9.12.1.

1.6 Definitions and Acronyms

1.6.1 Definitions

II. certification class	A group of non-qualified Certificate Policies, that make possible the Certificate issuance based on the Applicant's remote registration.
III. certification class	A group of non-qualified Certificate Policies, that bound the Certificate issuance to the Applicant's personal registration.
<TLS: ACME	It is a communications protocol for automating interactions between certificate authorities and their users' servers, allowing the automated deployment of public key infrastructure at lower cost.
> Data Centre	A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and security systems.
Subject	<TLS: In case of a Website Authentication Certificate the Subject is the webserver, which is identified by a domain name *[[ADV: or IP address]]* . > <ALA: A natural person with an identity or attribute verified by the Trust Service Provider with the Certificate, so the signatory especially in case of an electronic signature certificate. > <BEL: A legal person with an identity or attribute verified by the Trust Service Provider with the Certificate. > <UNI: A natural person, Organization, or IT device, system, unit identified by the Certificate. The Subject can be the Applicant itself or the device under the control of the Applicant. >
Subject Unique Identifier	The globally unique identifier of the Subject, given by the Certification Service Provider. The identifier is in the "Subject DN / SerialNumber" field of the Certificate, according to the requirements of section 3.1.1.
<ALA: Signatory	A natural person who creates an electronic signature.

>
<UNI:

Authentication	The public key certificate-based authentication is that process, when the Relying Party verifies the identity of the Certificate Subject (natural person, organization or application, website, service, server) by means of a method for this purpose, in which the private key of the Subject is used to be identified, and the identity is verifiable with the Certificate.

>
<not TLS:

Certificate for Automatism	A Certificate in which the name of the IT device (application, system) that is applied by the Subject to use the Certificate is to be recorded among the Subject's data.

>
<BEL:

Creator of a Seal	A legal person who creates an electronic seal.

>

Trust Service Supervisory Body	The National Media and Infocommunications Authority, the supervising authority monitoring the Trust Services.

[[QUA:

Trusted List	**For the Member States of the European Union, a list issued by a Member State in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council containing information on trust service providers under the responsibility of that Member State. It can be validated on the basis of a list of central trust lists issued by the Commission in accordance with Official Journal of the European Union 2019 / C 276/01.**

]]

Trust Service	Means an electronic service normally provided for remuneration which consists of: • the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or • the creation, verification and validation of Website Authentication Certificate, or • the preservation of electronic signatures, seals or certificates related to those services.
Trust Service Policy	A set of rules in which a Trust Service Provider, relying party or other person requires conditions for the usage of the Trust Service for a community of the relying parties and/or a class of applications with common security requirements.
Trust Service Provider	A natural or a legal person who provides one or more Trust Services either as a qualified or as a non-qualified Trust Service Provider.
<TLS: Certificate Transparency (CT) Log provider	CT Log provider defined by Certificate Transparency [54], which stores the issued Certificates and the corresponding PreCertificates.
>	
<ALA: Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Certificate for Electronic Signature	Means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.
[[QUA: **Qualified Certificate for Electronic Signature**	**A Certificate for electronic signatures issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex I of eIDAS [1].**
]]	

Electronic Signature Creation Data	Means unique data which is used by the signatory to create an electronic signature. Typically, cryptographic private key, formerly known as the signature creation data.
Electronic Signature Creation Device	Means configured software or hardware used to create an electronic signature. Formerly known as signature-creation device (ALE).

>

<BEL:

Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
[[QUA: **Qualified Certificate for Electronic Seal**	**A Certificate for an electronic seal issued by a Qualified Trust Service Provider and meets the requirements laid down in eIDAS Annex III [1].**

]]

Certificate for Electronic Seal	An electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person.
Electronic Seal Creation Data	Means unique data, which is used by the creator of the electronic seal to create an electronic seal. Typically cryptographic private key.
Electronic Seal Creation Device	Means configured software or hardware used to create an electronic seal.

>

Electronic Document	Means any content stored in electronic form, in particular text or sound, visual or audiovisual recording
Electronic Time Stamp	Means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

<ALA:

Electronic signature for electronic administration	At least advanced level electronic signature can be used by bodies providing electronic administration services, which fulfils the requirements of the E-Signature Government Decree [16] 7. § b) and c) point.

>

<BEL:

Electronic seal for electronic administration	At least advanced level electronic seal can be used by bodies providing electronic administration services, which fulfils the requirements of the E-Signature Government Decree [16] 7. § b) and c) point.

>

Subscriber	A person or organization signing the service agreement with the Certification Service Provider in order to use some of its services.

<TLS:

[[QUA:

Applicant Representative	**An Applicant Representative is a natural person who is either the Subscriber, employed by the Subscriber, or an authorized agent who has express authority to represent the Subscriber, and who has authority on behalf of the Subscriber to acknowledge and agree to the General Terms and Conditions.**

]]

Precertificate	Digitally signed data structure (PreCert) defined by Certificate Transparency [54], which contains Subject data to be presented in the Certificate to be issued.

>

<UNI:

Email Certificate	A Certificate conforming to the S/MIME standard that can be used to encrypt email and ensure the integrity of content in internet-based email systems.

>

[[QUA:

<ALA:

Email Certificate	**A Certificate conforming to the S/MIME standard that can be used to encrypt email and ensure the integrity of content in internet-based email systems.**

>

<BEL:

Email Certificate	**A Certificate conforming to the S/MIME standard that can be used to encrypt email and ensure the integrity of content in internet-based email systems.**

>

]]

Relying Party	<TLS: That communicating party, who identifies a webserver when accessing the website based on its Website Authentication Certificate, furthermore, those software vendors who produce Internet browsers or applications in which they use Website Authentication Certificate at their operation. > <ALA: Recipient of the electronic document, who acts relying on the electronic signature based on a given certificate. > <BEL: Recipient of the electronic document, who acts relying on the electronic seal based on a given certificate. > <UNI: In case of encryption, the party who encrypts the electronic document for the recipient. In case of authentication, the party who verifies the identity of the party seeking to be identified during a procedure for this purpose. >
<not TLS: <not UNI: Validation	Means the process of verifying and confirming that an electronic signature or a seal is valid.
>> <not TLS: Validation Chain	The electronic document or its hash, and the series of information assigned to one another (especially those certificates, information related to certificates, data used for signature or seal creation, the current status of the certificate, information on the withdrawal, as well as information on the validity data of the certificate issuer provider and its revocation information), with the help of which it can be established that the advanced or qualified electronic signature, seal or time stamp placed on the electronic document was valid at the time of the signature, seal or time stamp placement.
> <not TLS: <not UNI: Validation Data	Means data that is used to validate an electronic signature or an electronic seal.
>> Suspension	A temporary pause of the Certificate's validity before the end of the validity period indicated on the Certificate. The Certificate suspension is not definitive; the suspended Certificate's validity can be restored.

<ALA: Advanced Electronic Signature	Means an electronic signature which meets the following requirements: a/ it is uniquely linked to the signatory b/ it is capable of identifying the signatory c/ it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, and d/ it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
>	
<BEL: Advanced Electronic Seal	Means an advanced electronic seal that meets the following requirements: a/ it is uniquely linked to the creator of the seal b/ it is capable of identifying the creator of the seal c/ it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation, and d/ it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
>	
Root Certificate	Also known as top level certificate. Self-signed Certificate, which is issued by a specific Certification Unit for itself, which is signed with its own private key, so it can be verified with its own public key – indicated on the certificate.
HSM: Hardware Security Module	A hardware-based secure device that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions.
Certification Authority	A Trust Service Provider, who/which identifies the requester within the confines of the certification service, issues Certificates, keeps a record, receives the Certificate related data changes, and publishes the regulations belonging to the Certificate<ALA: , the Certificate-Verifier Data> <UNI: , the public keys> and the information on the current state (especially on possible revocation) of the Certificate.
Certification Unit	A unit of the Certification Service Provider's system that signs the Certificates. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a Certification Unit. It is possible that a Certification Authority simultaneously operate several Certification Units.

Certificate Policy	A Trust Service Policy which concerns the Certificate issued within the framework of the Trust Service.
<TLS: Validation Specialist	An employee of the Certification Authority with trusted role "Registration officer", who performs the information verification duties specified by the CABF Baseline Requirements.
> IP Reverse Zone Suffix <TLS:	One of the two FQDNs that consist of the Domain Labels "in-addr.arpa" or "ip6.arpa". These two FQDNs serve as the root of the IP version 4 and IP version 6 reverse mapping space. "in-addr.arpa" is the root of the IP version 4 reverse mapping space and "ip6.arpa" is the root of the IP version 6 reverse mapping space.
> Applicant	That natural person who acts during the application for the given Certificate.
Dual Control	A procedure that uses two or more separate entities (persons, processes or devices) operating in concert to increase the reliability of the procedure.
Represented Organization	The Organization, which is represented by the Organizational Administrator during the actions related to the Certificates issued to the given Organization.
<not TLS: <not UNI: *[[ADV:* *Code Signing Certificate*	*A Certificate, which can be used for justifying the origin and integrity of applications.*
]] >> Compromise	A cryptographic key is considered as compromised, when it can be assumed, that unauthorized person has access to it.
<not TLS: Public Administration Root CA	Organization unit defined in the E-Signature Government Decree [16] in section 3. § (2).

> <ALA:

Electronic signature for public administration	At least advanced level electronic signature can be used by government bodies providing electronic administration services, which fulfils the requirements of the E-Signature Government Decree [16] 7. § a), b) and c) point.

>
<BEL:

Electronic seal for public administration	At least advanced level electronic seal can be used by government bodies providing electronic administration services, which fulfils the requirements of the E-Signature Government Decree [16] 7. § a), b) and c) point.

>

Intermediate Certification Unit	A Certification Unit whose Certificate was issued by another Certification Unit.
Cryptographic Key	A unique digital data string controlling a cryptographic transformation, the knowledge of which is required for encryption, decryption and the creation and verification of electronic signatures and seals.
Key Management	The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation and termination of keys which are closely linked to the used security method.

<not TLS: <not UNI:

Hash	A specific length bit string assigned to the electronic document, during the creation of which the used procedure (hashing procedure) fulfils the requirements defined in Act CIII. of 2023. [13] at the time of the creation. The hash in practice a fixed-length bit string that is clearly dependent on the electronic document, from which it is derived from, with a very small probability that two different documents would have the same hash, and it is practically impossible given the hash prepare a document, which has the same hash.

>>

Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to the key-pair owner that the <not TLS: Subject > <TLS: Applicant > shall keep strictly secret. <TLS: In case of webserver authentication, the webserver shall use its private key during its authentication procedure. > <ALA: In case of electronic signatures the creator of the electronic signature or seal generates the signature with the help of the private key. > <BEL: In case of electronic seals the creator of the electronic signature or seal generates the seal with the help of the private key. > <UNI: In case of encryption, the recipient needs his private key for decrypt the document that was encrypted for him. In case of authentication, the party to be identified shall use his private key during the verification procedure. > During the issuance of Certificates, the Certification Authority uses the private keys of the Certification Unit for placing an electronic signature or seal on the Certificate to protect it.
[[QUA: **Qualified Trust Service**	**A Trust Service that meets the applicable requirements laid down in the eIDAS Regulation.**
]] **[[QUA:** **Qualified Trust Service Provider**	**A Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualified status by the supervisory body.**
]] <ALA: Qualified Electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Qualified Electronic Signature Creation Device	Means an electronic signature creation device that meets the requirements laid down in Annex II of eIDAS [1]. Previously known as Secure Signature Creation Device (BALE).

>
<BEL:

Qualified Electronic Seal	An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
Qualified Electronic Seal Creation Device	Means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II of eIDAS

>
[[QUA:
<not TLS:

Qualified Electronic Time Stamp	**An electronic Time Stamp which meets the requirements laid down in Article 42 of the eIDAS Regulation [1].**

>
<TLS:

Qualified Certificate for Website Authentication	**Means a certificate for Website Authentication Certificate, which is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex IV of eIDAS [1].**

>
]]
<TLS:

Internationalized Domain Name	An internationalized domain name is an Internet domain name that contains at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet, like "ékezet.example.com". Internationalized domain names are stored in the Domain Name System as ASCII strings using Punycode transcription.

>

Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to key-pair owner, which should be made public. The disclosure is typically in the form of a Certificate, which links the name of the actor with its public key. <TLS: In case of webserver authentication, the public key of the webserver is needed for the verification of its identity. > <ALA: In case of an electronic signature, the public key of the signature creator party is needed to verify the signature authenticity (this is the Certificate-Verifier Data). > <BEL: In case of an electronic seal, the public key of the seal creator party is needed to verify the seal authenticity (this is the Certificate-Verifier Data). > <UNI: In case of encryption, the recipient public key is needed for creating an encrypted document for him. In case of authentication, the public key of the party to be identified is needed, to verify his identity. > The authenticity of the Certificates can be verified with the public key of the Certification Unit.
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices.

<not SIG:

[[QUA:

Open Banking	**Regulated environment for payment services outside the scope of EU PSD2 but operating on the basis of identical or very similar requirements.**

]]

>

<UNI:

Open Banking	Regulated environment for payment services outside the scope of EU PSD2 but operating on the basis of identical or very similar requirements.

>

Registration Claim	The data and statement given beforehand for the preparation of the Certificate Application and the service agreement to the Certification Service Provider by the Client in which the Client authorizes the Certification Service Provider for data management.
Registration Authority	Organization that checks the authenticity of the Certificate holder's data and verifies that the Certificate Application is authentic, and it has been submitted by an authorized person.
Extraordinary Operational Situation	An extraordinary situation causing disturbance in the course of the operation of the Certification Service Provider, when the continuation of the normal operation of the Certification Service Provider is not possible either temporarily or permanently.
<TLS:	
SCT - Signed Certificate Timestamp	Digitally signed answer (the time stamp of the signed Certificate) sent by the CT Log provider during the publication of the Certificate and the corresponding PreCertificate, which proves the inclusion of the Certificate and the corresponding PreCertificate into the given CT Log.
[[ADV:	
Server Authentication Certificate	*Certificate which is used to authenticate a server or one of its services. The CN field of these Certificates always contains a FQDN or an IP address. These type of Certificates are issued for example for the CISCO VPN server, domain controller, SCEP server, VPN server.*
]]	
>	
Organization	Legal person.
<UNI:	
Organization-validated Certificate	An email Certificate, which includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated Certificate	An email Certificate, which combines Individual (Natural Person) attributes in conjunction with an associated Legal Entity attribute.
>	

Organizational Certificate	<TLS: A Certificate, which contains the name of an Organization. > <not TLS: A Certificate, the Subject of which is the Organization, or which presents that the natural person Subject belongs to an Organization. > In this case the name of the Organization is indicated in the "O" field of the Certificate. <BEL: Every seal certificate is an Organizational Certificate. >
Organizational Administrator	The natural person who is acting in the name of the Subscriber, and <TLS: **[[QUA:** **in case of special authorization definitely for EV Certificates** **]]** > is eligible to issue the Certificate Application, to grant the issuance of the Certificate, to act during the <TLS: application, replacement and revocation> <not TLS: application, replacement, suspension, reinstatement and revocation> of the Certificates issued to the Subscriber.
<TLS: **[[QUA:** **Contract Signer**	**A Contract Signer is a natural person who is either the Subscriber, employed by the Subscriber, or an authorized agent who has express authority to represent the Subscriber, and who has authority on behalf of the Subscriber to sign the service agreement.**
]] >	
Trust Service Practice Statement	The statement of the Trust Service Provider of the detailed procedures or other operational requirements used in connection with the provision of particular Trust Services.
Service Agreement	The contract between the Trust Service Provider and the Trust Service client, which includes the conditions for the provision of the Trust Service and for using the services.

Certificate	The electronic signature certificate, the electronic seal certificate and the Website Authentication Certificate, and all those electronic verifications issued within the framework of the Trust Service by the service provider, which includes the certificate related verification data and the certificate usage related information, and which as an electronic document is reliably protected against the available counterfeiting technologies at the time of the issuance and during its validity period.

<TLS:
[[QUA:

Certificate Requester	**A Certificate Requester is a natural person who is either the Subscriber, employed by the Subscriber, an authorized agent who has express authority to represent the Subscriber, or a third party that completes and submits an EV Certificate Request on behalf of the Subscriber.**
Certificate Approver	**A Certificate Approver is a natural person who is either the Subscriber, employed by the Subscriber, or an authorized agent who has express authority to represent the Subscriber to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.**

]]
>

Certificate Application	The data and statements given by the Applicant to the Certification Service Provider for Certificate issuance, in which the Applicant reaffirms the authenticity of data to be indicated on the Certificate.
Certificate Repository	Data repository containing various Certificates. A Certification Authority has a Certificate Repository in which the issued Certificates are disclosed, but the system containing Certificates available to the application <ALA: (certificate manager system)> on the computer of the <not TLS: Subject and the> Relying Party is also called Certificate Repository.

<not TLS:
[[QUA:

Remote Key Management Service	**A Trust Service in which a service provider manages Customers' private keys under secure conditions, ensures the necessary technical and procedural conditions in order that the Customers could carry out remote key operations with their private keys stored at the service provider, such as creating electronic signatures or electronic seals.**

]]
>
<UNI:

Encryption	During the public-key cryptography, the process by which the sender using the recipient's public key encrypts the document, which then can be only decrypted by the addressed party private key.

>

Client	The collective term for the Subscriber and every related Subject or Applicant denomination.
Customer Portal	It is a web-based service created and continuously improved by e-Szignó Certification Authority, in which customers - based on two-factor authentication - can easily manage their individual matters related to the services in one place and receive immediate, up-to-date information about the services used.
Revocation	The termination of the Certificate's validity before the end of the validity period indicated on the Certificate too. The Certificate revocation is permanent, the revoked Certificate cannot be reinstated any more.
Revocation Status Records	The internal records of the suspended and revoked Certificates which includes the fact of the suspension or revocation and the time of the suspension or revocation given in seconds maintained by the Certification Authority.

<TLS:

Certificate for Website Authentication	Means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. The webserver domain name *[[ADV: or IP address]]* is indicated in the name field of a Website Authentication Certificate.
Wildcard Domain Name	A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

Wildcard Certificate	A Website Authentication Certificate containing at least one Wildcard Domain Name in the "Subject Alternative Names" in the Certificate.
LDH-Label	A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets.
P-Label	A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
XN-Label	The class of labels that begin with the prefix "xn–" (case independent), but otherwise conform to the rules for LDH labels.
>	
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
Network Perspective	Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check.
Primary Network Perspective	The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

1.6.2 Acronyms

<TLS:

ACME	Automatic Certificate Management Environment

>

CA	Certification Authority

<TLS:

CAA	Certification Authority Authorization

>

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List

CSPRNG	Cryptographically Secure Pseudo-Random Number Generator

[[ADV:
<TLS:

DVC	*Domain Validation Certificate*
DVCP	*Domain Validation Certificate Policy*

>
]]

eIDAS	electronic Identification, Authentication and Signature

[[QUA:
<TLS:

EVC	**Extended Validation Certificate**
EVCP	**Extended Validation Certificate Policy**

>
]]
<TLS:

FQDN	Fully-Qualified Domain Name

>
<TLS:

IDN	Internationalized Domain Name

>
[[ADV:
<TLS: >
]]
<not TLS:

KGYHSZ	Public Administration Root CA	Kormányzati Gyökér Hitelesítés Szolgáltató

> LDAP Lightweight Directory Access Protocol

MPIC	Multi-Perspective Issuance Corroboration
NMHH	National Media and Infocommunications Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier

<UNI:

OV	Organization-validated (Email certificate)

>
[[ADV:
<TLS:

OVC	*Organizational Validation Certificate*
OVCP	*Organizational Validation Certificate Policy*

>

]]

PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy

[[QUA:

<TLS:

QGIS	**Qualified Government Information Source**

>

]]

RA	Registration Authority

<UNI:

S/MIME	Secure/Multipurpose Internet Mail Extensions
SV	Sponsor-validated (Email certificate)

>

TSP	Trust Service Provider

<UNI:

WRPAC	Wallet Relying Party Access Certificate

>

2 Publication and Repository Responsibilities

2.1 Repositories

The Certification Service Provider discloses the contractual conditions and policies electronically via its website on the following link:

`https://e-szigno.hu/en/terms-and-information`

The draft version of the new documents to be introduced are disclosed via the website **[[QUA: 30 days]]** before coming into force.

The documents in force are available via the website in addition to all previous versions of all documents.

The actual version of policies and contractual conditions is readable at the customer service of the Certification Service Provider.

After concluding the contract, the Certification Service Provider makes the General Terms and Conditions, <not UNI: *[[ADV: the Disclosure Statement,]]* > **[[QUA: the Disclosure Statement,]]** the Certificate Policy and the Certification Practice Statement available to

the Client in the form of an electronically signed PDF file that can be downloaded via its website. The Certification Service Provider makes the individual Service Agreement available to the Client on paper, authenticated with a handwritten signature and seal, or in the form of an electronic document in PDF format with a qualified electronic signature or a qualified electronic seal.

The Certification Service Provider notifies its Clients about the change of the General Terms and Conditions.

2.2 Publication of Certification Information

The Certification Service Provider publishes via its website (`https://www.e-szigno.hu`) and via LDAP protocol (`ldap://ldap.e-szigno.hu`)

- its provider Certificates
- the end user Certificates in case of the Subject or Applicant's prior consent.

Service Provider Certificates

With the following methods the Certification Authority discloses the Certificates of the <not TLS: <not UNI: time stamping units, >> certification units and the online certificate status service units it operates:

- The denomination of the root certification units, and the hash of its root certificates in the Certification Practice Statement (see section: 1.3.1). The information related to their change of status are available via the website of the Certification Authority.
- The status change of Certificates of intermediate (non-root) certification units <not TLS: <not UNI: and the Time Stamping Units >> is disclosed on the Certificate Revocation Lists, its website and within the confines of the online certificate status response services.
- For the signers of the online certificate status responses the Certification Service Provider – compliant with the best international practice – issues a Certificate with extremely short period of validity (for 10 minutes) thereby eliminating the need for Certificate revocation status verification.

  Each OCSP responder Certificate contains an indication ("nocheck"), that indicates that its revocation status doesn't need to be checked.

End-User Certificates

With the following methods the Certification Service Provider discloses status information related to the end-user Certificates which it had issued:

- on Certificate Revocation Lists
- within the confines of the Online Certification Status Response service.

The end-user Certificate revocation status information is disclosed by the Certification Service Provider, and the Subject or Applicant's consent is not required for it. For status information disclosing methods, see Section 4.10.

The Certification Service Provider guarantees, that the availability of its system publishing its service Certificates, the Certificate Repository and the revocation status information on an annual basis will be at least 99.9% per year, while service downtimes may not exceed at most 3 hours in each case.

<TLS:

The Certification Service Provider publishes through Certificate Transparency Log providers listed on the web page of the Certification Service Provider those PreCertificates, which publication is consented by the Applicant.

The Certification Service Provider doesn't store the issued PreCertificates in its own Certificate Repository and doesn't publish them through its own services.

>

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the service are contained in the service contract to be signed by the Client during the conclusion of the contract, or in the General Terms and Conditions [79] document referenced therein.

The Certification Service Provider reviews the General Terms and Conditions annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document will be published via the website of the Certification Service Provider and it will be sent for review to the National Media and Infocommunications Authority 30 days prior to the planned entry into force date.

The Certification Service Provider will accept comments connected to the General Terms and Conditions published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

In case of observations that require substantive changes, the document will be amended.

The Certification Service Provider will finalize and publish the annotated version of the amended General Terms and Conditions on the 7th day prior to their entry into force.

2.3.2 Frequency of the Certificates Disclosure

The Certification Service Provider, regarding the disclosure of Certificates, follows the practices below:

- the Certificates of the root certification units operated by it are disclosed before commencing the service

- the Certificates of the intermediate certification units operated by it are disclosed within 5 workdays after issuance

<TLS:

- the Certification Service Provider publishes the PreCertificate corresponding to the end-user Certificate before the issuance of the Certificate through CT Log providers

>

- the Certification Service Provider discloses the end-user Certificates in its Certificate Repository after issuance without delay.

2.3.3 The Changed Revocation Status Publication Frequency

The status information related to the end-user Certificates issued by the Certification Service Provider and the provider Certificates are available immediately within the confines of the online certificate status service.

The information related to the status of the Certificates are disclosed in the Certificate Repository and on the Certificate Revocation Lists. The practices related to the issuance of the Certificate Revocation Lists are discussed in Section 4.10.

2.4 Access Controls on Repositories

The provided information is freely available for anybody for reading purposes according to the specifics of the publication method.

The information disclosed by the Certification Service Provider shall only be amended, deleted or modified by the Certification Service Provider. The Certification Service Provider prevents the unauthorized changes to the information with various protection mechanisms.

<TLS:

2.5 Websites for testing

The Certification Service Provider operates special test websites to test and demonstrate the operation and usability of the

- valid Website Authentication Certificates for each supported CABF OID
- expired Website Authentication Certificates
- revoked Website Authentication Certificates

The test websites are available via the following links:

2.5.1 RSA based Certificates issued under "Microsec e-Szigno Root CA 2009"

Valid DV Certificate

`https://osslca2016-dv-valid.e-szigno.hu`

Valid OV Certificate

https://ssl2ca2016-ov-valid.e-szigno.hu

Valid EV Certificate

https://qtlsca2018-valid.e-szigno.hu

Expired EV Certificate

https://qtlsca2018-expired.e-szigno.hu

Revoked EV Certificate

https://qtlsca2018-revoked.e-szigno.hu

2.5.2 ECC based Certificates issued under "e-Szigno Root CA 2017"

Valid DV Certificate

https://eosslca2017-dv-valid.e-szigno.hu

Valid OV Certificate

https://ec2sslca2017-ov-valid.e-szigno.hu

Valid EV Certificate

https://eqtlsca2018-valid.e-szigno.hu

Expired EV Certificate

https://eqtlsca2018-expired.e-szigno.hu

Revoked EV Certificate

https://eqtlsca2018-revoked.e-szigno.hu

2.5.3 ECC based Certificates issued under "e-Szigno TLS Root CA 2023"

Valid DV Certificate

https://edvtlsca2023-valid.e-szigno.hu

Valid OV Certificate

https://eovtlsca2023-ov-valid.e-szigno.hu

Valid EV Certificate

https://eqtlsca2023-valid.e-szigno.hu

Expired EV Certificate

https://eqtlsca2023-expired.e-szigno.hu

Revoked EV Certificate

https://eqtlsca2023-revoked.e-szigno.hu

2.5.4 ECC based Certificates issued under "e-Szigno TLS Root CA 2024"

Valid DV Certificate

https://edvtlsca2025-valid.e-szigno.hu

Valid OV Certificate

https://eovtlsca2025-ov-valid.e-szigno.hu

Valid EV Certificate

https://eqtlsca2025-valid.e-szigno.hu

Expired EV Certificate

https://eqtlsca2025-expired.e-szigno.hu

Revoked EV Certificate

https://eqtlsca2025-revoked.e-szigno.hu

2.5.5 RSA based Certificates issued under "e-Szigno RSA TLS Root CA 2025"

Valid DV Certificate

https://dvtlsca2025-valid.e-szigno.hu

Valid OV Certificate

https://ovtlsca2025-valid.e-szigno.hu

Expired OV Certificate

https://ovtlsca2025-expired.e-szigno.hu

Revoked OV Certificate

`https://ovtlsca2025-revoked.e-szigno.hu`

>

3 Identification and Authentication

3.1 Naming

The section contains requirements for the data indicated in the Certificates issued to end-users in accordance with the applied Certificate Policies.

The indicated Issuer ID and the Subject ID amongst the basic fields of the Certificate comply with the ITU X.520 standard [61], the RCF 5280 [48] and IETF RFC 6818 [51] recommendations name-specific format requirements, in addition the Certification Service Provider supports the "Subject Alternative Names" and "Issuer Alternative Names" fields located amongst the extensions.

The Certification Service Provider may shorten the content of the Certificate fields in the frame of the name-specific format requirements or may indicate certain types of names in multiple instances.

3.1.1 Types of Names

Denomination of the Subject

The denomination of the Certificate Subject (content of the Subject field) consists of:

- commonName (CN) – OID: 2.5.4.3 The name of the Subject

  <TLS:

  This field contains exactly one entry that is one of the values contained in the Certificate's "Subject Alternative Names" extension.

  The value of the field shall be encoded as follows:

  Fully-Qualified Domain Name ***[[ADV: or Wildcard Domain Name]]*** :
  If the value is a Fully-Qualified Domain Name *[[ADV: or Wildcard Domain Name]]* , then the value shall be encoded as a character-for-character copy of the "dNSName" entry value from the "Subject Alternative Names" extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name *[[ADV: or FQDN portion of the Wildcard Domain Name]]* shall be encoded as LDH-Labels, and P-Labels shall not be converted to their Unicode representation.

  [[ADV:

  IPv4 address *:*
  If the value is an IPv4 address, then the value shall be encoded as an "IPv4Address" as specified in RFC 3986 [42], Section 3.2.2.

IPv6 address *:*

If the value is an IPv6 address, then the value shall be encoded in the text representation specified in RFC 5952 [50], Section 4. pg. 81

]]

Only that domain name *[[ADV: or IP address]]* is indicated that exists and legally used by the Applicant.

Always filled out.

The Website Authentication Certificate shall not be pseudonymous.

>

<ALA:

The name of the natural person Subject is in this field in the same form as verified by the Certification Service Provider according to the section 3.2.3.

>

<BEL:

The organization's full or shortened name is in this field in the same form as verified by the Certification Service Provider according to the section 3.2.2.

If neither the full nor the shortened name of the Organization fits because of the size limit of the Certificate, then the unambiguous abbreviation of the Organization name is presented here.

>

<UNI:

In case of natural persons, the name of the natural person Subject is in this field in the same form as verified by the Certification Service Provider according to the section 3.2.3.

In case of an Organization the organization's full or shortened name is in this field in the same form as verified by the Certification Service Provider according to the section 3.2.2.

If neither the full nor the shortened name of the Organization fits because of the size limit of the Certificate, then the unambiguous abbreviation of the Organization name is presented here.

>

<not TLS:

The name of the automatism by the help of the Certificate is used can be indicated in this field for the Applicant's request (Certificate for Automatism).

Always filled out.

>

<UNI:

In the case of Code Signing Certificate, the value of the field can also be presented without an accent.

In the case of Email (S/MIME) Certificate, instead of the real name of the Subject, this field may contain the same email address of the Subject, as the email address indicated in the "RFC822name" field of the "Subject Alternative Names" extension.

>

- Surname – OID: 2.5.4.4 – Surname of the natural person

<TLS:

[[QUA:

It is not filled.

]]

[[ADV:

It is not filled.

]]

>

<ALA:

The surname of the Subject is in this field, where the Certification Service Provider generates the surname from the full name in the CN field.

The Certification Service Provider always fills it.

>

<BEL:

It is not filled.

>

<UNI:

In case of natural person Subjects the surname of the Subject is in this field, where the Certification Service Provider generates the surname from the full name in the CN field.

If the Subject of the Certificate is an Organization, it is not filled.

In the case of Code Signing Certificate, the value of the field can also be presented without an accent.

In case of Organization-validated Email (S/MIME) Certificate it is not filled out.

>

- Given Name – OID: 2.5.4.42 – The given name of the natural person.

<TLS:

[[QUA:

It is not filled.

]]

[[ADV:

It is not filled.

]]

>

<ALA:

The given name of the Subject is in this field, where the Certification Service Provider generates the given name from the full name in the CN field.

The Certification Service Provider always fills it.

>

<BEL:

It is not filled.

>

<UNI:

In case of natural person Subjects the given name of the Subject is in this field, where the Certification Service Provider generates the given name from the full name in the CN field.

If the Subject of the Certificate is an Organization, it is not filled.

In the case of Code Signing Certificate, the value of the field can also be presented without an accent.

In case of Organization-validated Email (S/MIME) Certificate it is not filled out.

>

- Initials – OID: 2.5.4.43 – the initials of some or all of the individual's names

<TLS:

It is not filled.

>

<ALA:

The field may contain the initials of some or all of the Subject's names except the "Surname" and the "Givenname", like "J.P.".

This field may contain some titles of the Subject, which are not included in the "Surname" field, like "Dr.", "Phd."

In case of pseudonymous Certificate it shall not be filled out.

In case of not pseudonymous Certificate it is optional.

[[QUA:

In case of Email (S/MIME) Certificate it is not filled out.

]]

>

<BEL:

It is not filled.

>

<UNI:

In case of natural person Subject, the field may contain the initials of some or all of the Subject's names except the "Surname" and the "Givenname", like "J.P.".

This field may contain some titles of the Subject, which are not included in the "Surname" field, like "Dr.", "Phd."

In case of pseudonymous Certificate it shall not be filled out.

In case of not pseudonymous Certificate it is optional.

If the Subject of the Certificate is an Organization, it is not filled.

In case of Email (S/MIME) Certificate it is not filled.

>

- Generation Qualifier – OID: 2.5.4.44 – provides generation information to qualify an individual's name

<TLS:

It is not filled.

>

<ALA:

The field may contain generation information as an addition to the official name of the Subject, like "Jr.", "Sr.", when more than one person with the same name exists in the same family .

In case of pseudonymous Certificate it shall not be filled out.

In case of not pseudonymous Certificate it is optional.

[[QUA:

In case of Email (S/MIME) Certificate it is not filled out.

]]

>

<BEL:

It is not filled.

>

<UNI:

In case of natural person Subject, the field may contain generation information as an addition to the official name of the Subject, like "Jr.", "Sr.", when more than one person with the same name exists in the same family .

In case of pseudonymous Certificate it shall not be filled out.

In case of not pseudonymous Certificate it is optional.

If the Subject of the Certificate is an Organization, it is not filled.

In case of Email (S/MIME) Certificate it is not filled.

>

- Pseudonym (PSEUDO) – OID: 2.5.4.65 Pseudonym of the Subject

  The Certification Service Provider doesn't fill this field.

- Serial Number – OID: 2.5.4.5 Unique identifier of the Subject.

  <not TLS: The indication of at least one filled out "Serial Number" field is in the Certificate which complies with the following requirements, so that it is able to form a part of the Subject permanent unique identifier in case of the usage of "Permanent Identifier" extension according to the IETF RFC 4043 [44] recommendation:

  – the identifier value belongs to the Subject named in the Certificate, identified by the Certification Service Provider, and it is unique within the system of the Certification Service Provider

  – the Certification Service Provider guarantees that the identifier value of any two Certificates it issued only matches with each other, if both of the Certificates belong to the same Subject.

  This field is part of the Subject denomination, and is not the same as the Certificate serial number defined by IETF RFC 5280. >

  <TLS:

  [[QUA:

  The Certificate always contains one filled out "Serial Number" field.

  ]]

  [[ADV:

  The Certificate never contains the "Serial Number" field.

  ]]

  >

  <TLS:

  [[QUA:

  – **The mandatory "Serial Number" field contains the Registration Number of the Subject.**
    - **For Private Organizations this field contains the Registration Number given by the Incorporating or Registration Authority. If there is no Registration number than the date of the Incorporation or Registration is indicated here in "YYYY-MM-DD" format.**
    - **For Government Entities that do not have a Registration Number or readily verifiable date of creation, the field contains the following string:**
      - **"Government Entity".**

  ]]

  >

  <not TLS:

- The unique identifier issued by the Certification Service Provider to the Subject is OID formatted: "1.3.6.1.4.1.21528.2.x.y.z".
  - In it, the first numbers are fixed (1.3.6.1.4.1.21528.2: is the unique identifier of the Certification Service Provider),
  - "x" is the inner identifier used by the Certification Service Provider,
  - "y" is the inner identifier used by the Certification Service Provider,
  - "z" is an automatically issued, a unique identifier within a specific "x.y" value pair.

  So the "x.y.z" value set is the unique identifier of the Subject within the system of the Certification Service Provider.

  Because the first part of the identifier identifies the Certification Service Provider globally, and the rest of the identifier specifies the Subject within the system of the Certification Service Provider, so the full identifier identifies the Subject in a unique way globally by itself.

  This identifier is part of the "Permanent Identifier" according to IETF RFC 4043 [44] recommendation if the Certificate "Subject Alternative Names" extension contains the "assigner" but not the "identifierValue" according to IETF RFC 4043 recommendation.

  There may be multiple OIDs belonging to the same Subject, but only one Subject may belong to an OID. The Subject is always entitled to request a new (unassigned) OID.

  The Certification Service Provider only issues the same OID for two Certificates if it made sure that the Subject belonging to the two Certificate is the same.

>
<ALA:

- The Certificate may contain further Serial Number fields. The identifier may be given in a format
  - specified in the ETSI EN 319 412-1 section 5.1.3 (for example: "TINHU-8123456790"),
  - in (Name:Value) format (for example: "ID card number:AAAAAA"), or
  - in other format requested by the Clients.

>
<UNI:

- The Certificate issued for a natural person Subject may contain further Serial Number fields.

  The identifier may be given in a format
  - specified in the ETSI EN 319 412-1 section 5.1.3 (for example: "TINHU-8123456790"),
  - in (Name:Value) format (for example: "ID card number:AAAAAA"), or
  - in other format requested by the Clients.

>
<TLS:

[[QUA:

In the "Serial Number" field the Certification Service Provider – compliant with the standards – does not indicate accents.

]]

>

<not TLS:

In the "Serial Number" field the Certification Service Provider – compliant with the standards – does not indicate accents.

>

- Organization (O) – OID: 2.5.4.10 The name of the Organization

<TLS:

[[ADV:

In case of DVCP Certificate it is not filled.

]]

[[QUA:

The

]]

[[ADV:

In case of OVCP Certificate the

]]

full or shortened legal name of the Organization is indicated in the "O" field according to the name verified by the Certification Service Provider according to the section 3.2.2.

[[QUA:

This field is always filled.

The Certification Service Provider abbreviate the organization prefixes or suffixes in the organization name (e.g company form).

If the combination of names or the organization name by itself exceeds 64 characters, the Certification Service Provider may abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the Certification Service Provider does not issue the Extended Validation Website Authentication Certificate.

]]

[[ADV:

The name of an Organization can be indicated in a Website Authentication Certificate only if the Organization is the legal user, owner of the domain or IP address, or has the authorisation of them.

]]

>

<ALA:

In case of an Organizational Certificate the full or shortened legal name of the Organization is indicated in the "O" field according to the name verified by the Certification Service Provider according to the section 3.2.2.

>

<BEL:

The full or shortened legal name of the Organization is indicated in the "O" field according to the name verified by the Certification Service Provider according to the section 3.2.2.

>

<UNI:

In case of an Organizational Certificate the full or shortened legal name of the Organization is indicated in the "O" field according to the name verified by the Certification Service Provider according to the section 3.2.2.

>

<ALA:

In case of an Organizational Certificate the field is always filled out.

[[QUA:

In case of personal – not related to any organization – Certificates this field is not filled out.

]]

[[ADV:

In case of Code Signing Certificate issued to a natural person, the field is mandatory, the Certification Service Provider writes here the name of the natural person.

In case of Certificate issued to a natural person, the field is not filled out.

]]

>

<BEL:

The field is always filled out.

>

<UNI:

In case of an Organizational Certificate the field is always filled out.

In case of Code Signing Certificate issued to a natural person, the field is mandatory, the Certification Service Provider writes here the name of the natural person. The value of the field can also be presented without an accent.

In case of other Certificate issued to a natural person, the field is not filled out.

>

In case of a provider Certificate issued for a Trust Service Provider, the "O" field is always filled, and the real name of the organization providing the service is indicated in it.

- Organization Identifier (OrgId) – OID: 2.5.4.97 – Identifier of the organization

  <TLS:

  The identifier of the Organization indicated in the "O" field can be in this field according to Section 5.1.4 of ETSI EN 319 412-1 [25].

  >

  <ALA:

  In case of an Organizational Certificate the identifier of the Organization indicated in the "O" field can be in this field according to Section 5.1.4 of ETSI EN 319 412-1 [25].

  >

  <BEL:

  The identifier of the Organization indicated in the "O" field is in this field according to Section 5.1.4 of ETSI EN 319 412-1 [25].

  >

  <UNI:

  In case of an Organizational Certificate the identifier of the Organization indicated in the "O" field can be in this field according to Section 5.1.4 of ETSI EN 319 412-1 [25].

  >

  Only such data may be indicated, which was verified by the Certification Service Provider.

  <TLS:

  [[ADV:

  In case of DVCP Certificate this field is not filled.

  In case of OVCP Certificate filling out the field is optional.

  ]]

  [[QUA:

  Filling out the field is optional.

  It is filled out only in case of Open Banking or PSD2 Certificates.

  ]]

  >

  <ALA:

  In case of an Organizational Certificate filling out the field is optional.

  In case of personal – not related to any organization – Certificates this field is not filled out.

  [[QUA:

  In case of Sponsor-validated Email (S/MIME) Certificate it is always filled out.

  ]]

  >

  <BEL:

Filling out the field is mandatory.

>

<UNI:

In case of an Organizational Certificate filling out the field is optional.

Filling out this field is mandatory in case the Subject is a legal person.

In case of personal – not related to any organization – Certificates this field is not filled out.

In case of Organization- and Sponsor validated Email (S/MIME) Certificate it is always filled out.

>

<TLS:

[[QUA:

If the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then this field contains either an identifier consisting of the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the Subject, the abbreviation of the NCA and the two character ISO 3166 country code of the NCA, structured as defined in the ETSI TS 119 495 specification [34], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [25] specification.

]]

>

<BEL:

[[QUA:

If the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then this field contains either an identifier consisting of the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the Subject, the abbreviation of the NCA and the two character ISO 3166 country code of the NCA, structured as defined in the ETSI TS 119 495 specification [34], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [25] specification.

]]

>

<UNI:

[[ADV:

If the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then this field contains either an identifier consisting of the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the

Subject, the abbreviation of the NCA and the two character ISO 3166 country code of the NCA, structured as defined in the ETSI TS 119 495 specification [34], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [25] specification.

]]

>

- Organizational Unit (OU) – OID: 2.5.4.11 – The name of the organizational unit

<TLS:

This field will not be filled out in Certificates.

>

<ALA:

In case of an Organizational Certificate the name of the organizational unit related to the organization named in the "O" field, or other information may be in this field.

>

<BEL:

The name of the organizational unit related to the organization named in the "O" field, or other information may be in this field.

>

<UNI:

In case of an Organizational Certificate the name of the organizational unit related to the organization named in the "O" field, or other information may be in this field.

>

<not TLS:

Only that data may be indicated here that the Certification Service Provider verified and that the Organization has the right to use.

The "OU" field may be filled only if the "O", "L" and "C" fields are filled.

Optional field.

>

<ALA:

In case of personal – not related to any organization – Certificates this field is not filled out.

>

<UNI:

In case of personal – not related to any organization – Certificates this field is not filled out.

>

[[QUA:

<TLS:

- **Business Category – OID: 2.5.4.15 – Business category Type**

  The type of the Organization indicated in the field "O", it contains one of the following strings:

  - **Private Organization,**
  - **Government Entity.**

  Mandatory.

- **jurisdictionOfIncorporationLocalityName – OID: 1.3.6.1.4.1.311.60.2.1.1 – Jurisdiction of Incorporation Locality Name**

  The full name of the applicable jurisdiction, if it operates on locality level.

  It is included only if it contains relevant information.

- **jurisdictionOfIncorporationStateOrProvinceName – OID: 1.3.6.1.4.1.311.60.2.1.2 – Jurisdiction of Incorporation State or Province Name**

  The full name of the applicable jurisdiction, if it operates on state or province level.

  It is included only if it contains relevant information.

- **jurisdictionOfIncorporationCountryName – OID: 1.3.6.1.4.1.311.60.2.1.3 – Jurisdiction of Incorporation Country Name**

  The two-letter ISO country code - according to ISO 3166-1 [36] - of the applicable jurisdiction.

  It is always filled.

  >

  ]]

- CountryName (C) – OID: 2.5.4.6 – Identifier of the country.

  <TLS:

  [[QUA:

  The two-letter country code - according to ISO 3166-1 [36] - of the place of incorporation of the Organization indicated in the "O" field.

  ]]

  [[ADV:

  In case of DVCP Certificate the two-letter country code - according to ISO 3166-1 [36] - of the country belonging to the [[ADV: IP address or]] domain, or if this cannot be clearly decided, then the country of the Applicant.

  In case of OVCP Certificate the two-letter country code - according to ISO 3166-1 [36] - of the place of incorporation of the Organization indicated in the "O" field.

  ]]

  >

  <ALA:

In case of an Organizational Certificate the two-letter country code - according to ISO 3166-1 [36] - of the place of incorporation of the Organization indicated in the "O" field.

In case of a natural person Subject not related to an Organization the two-letter country code - according to ISO 3166-1 [36] - of the country which issued the document used for the identification of the Subject.

>

<BEL:

The two-letter country code - according to ISO 3166-1 [36] - of the place of incorporation of the Organization indicated in the "O" field.

>

<UNI:

In case of an Organizational Certificate the two-letter country code - according to ISO 3166-1 [36] - of the place of incorporation of the Organization indicated in the "O" field.

In case of a natural person Subject not related to an Organization the two-letter country code - according to ISO 3166-1 [36] - of the country which issued the document used for the identification of the Subject.

>

Always filled out.

In case of Hungary the value of the "C" field is: "HU".

- Street Address (SA) – OID: 2.5.4.9 – Address data

  Not filled.

- Locality Name(L) – OID: 2.5.4.7 – Name of settlement

  <TLS:

  [[QUA:

  The city name of the place of incorporation of the Organization indicated in the "O" field.

  It is always filled out.

  ]]

  [[ADV:

  In case of DVCP Certificate it is not filled.

  In case of OVCP Certificate the city name of the place of incorporation of the Organization indicated in the "O" field.

  ]]

  >

  <ALA:

  In case of an Organizational Certificate the locality name of the Organization's place of incorporation.

In case of a Certificate not related to an Organization, it is not filled.

>

<BEL:

The locality name of the Organization's place of incorporation.

>

<UNI:

In case of an Organizational Certificate the locality name of the Organization's place of incorporation.

In case of Code Signing Certificate issued to a natural person, the field is mandatory, the Certification Service Provider writes here the locality of the official address of the natural person. The value of the field can also be presented without an accent.

In case of other Certificate not related to an Organization, it is not filled.

>

- State or Province Name – OID: 2.5.4.8 – Member state, province name

<TLS:

[[QUA:

The member state or province name, or the full name of the country – given in the "C" field – of the place of incorporation of the Organization indicated in the "O" field.

Optional field.

]]

[[ADV:

In case of DVCP Certificate it is not filled.

In case of OVCP Certificate the member state or province name, or the full name of the country – given in the "C" field – of the place of incorporation of the Organization indicated in the "O" field.

Optional field.

]]

>

<ALA:

In case of Organizational Certificate the state, province or county name of the Organization's place of incorporation.

In case of a Certificate not related to an Organization, it is not filled.

>

<BEL:

The state, province or county name of the Organization's place of incorporation.

>

<UNI:

In case of Organizational Certificate the state, province or county name of the Organization's place of incorporation.

In case of a Certificate not related to an Organization, it is not filled.

>

- Postal Code – OID: 2.5.4.17 – Zip code

<TLS:

[[QUA:

Zip or postal information of the place of incorporation of the Organization indicated in the "O" field.

Optional field.

]]

[[ADV:

In case of DVCP Certificate it is not filled.

In case of OVCP Certificate zip or postal information of the place of incorporation of the Organization indicated in the "O" field.

Optional field.

]]

>

<ALA:

In case of Organizational Certificate, the postal code of the Organization's place of incorporation. If filled, only verified information can be indicated.

In case of a Certificate not related to an Organization, it is not filled.

[[QUA:

In case of Email (S/MIME) Certificate it is not filled out.

]]

>

<BEL:

The postal code of the Organization's place of incorporation. If filled, only verified information can be indicated.

[[QUA:

In case of Email (S/MIME) Certificate it is not filled out.

]]

>

<UNI:

In case of Organizational Certificate, the postal code of the Organization's place of incorporation. If filled, only verified information can be indicated.

In case of a Certificate not related to an Organization, it is not filled.

In case of Email (S/MIME) Certificate it shall not be filled out.

>

- Title (T) – OID: 2.5.4.12 – Title of the subject

<TLS:

Not filled.

>

<ALA:

The natural person Subject's role, title or job.

In case of Organizational Certificate it is filled out based on the official document presented by the Represented Organization indicated in the "O" field.

In case of Certificate for Profession it is filled out based on the official document presented by an Organization independent of the Subject.

The field may contain further information about the Subject's role in the Organization.

In special cases the Certification Service Provider may include more "Title" fields in the Certificate.

>

<BEL:

The natural person Subject's role, title or job.

Not filled.

>

<UNI:

The natural person Subject's role, title or job.

In case of Organizational Certificate it is filled out based on the official document presented by the Represented Organization indicated in the "O" field.

In case of Certificate for Profession it is filled out based on the official document presented by an Organization independent of the Subject.

The field may contain further information about the Subject's role in the Organization.

In special cases the Certification Service Provider may include more "Title" fields in the Certificate. >

- Email Address (EMAIL) – OID: 1.2.840.113549.1.9.1 – The email address of the Subject

<TLS:

Not filled.

>

<not TLS:

Filling is optional.

If filled, it is the same as the email address indicated in the "RFC822name" field of the "Subject Alternative Names" extension.

>

The Certificates issued in accordance with the present Certification Practice Statement might contain further – in accordance with the referenced Certificate Policies – "Subject DN" fields.

Only verified text values may be indicated on these fields (they shall not contain values indicating lack of data for example: ".", "-" or " ").

Extensions

- Subject Alternative Names - "Subject Alternative Names"

  The "Subject Alternative Names" extension is included as a non-critical extension in the Certificate. The content will be filled as follows.

  <TLS:

  – The "Subject Alternative Names" extension always contains at least one entry.
  Each entry is *[[ADV: one of the following types:]]* **[[QUA: the following type:]]**

  dNSName :

  The entry shall contain either a Fully-Qualified Domain Name *[[ADV: or Wildcard Domain Name]]* that the Certification Service Provider has validated in accordance with Section 3.2.2.2.
  The entry shall not contain an Internal Name.
  The Fully-Qualified Domain Name *[[ADV: or the FQDN portion of the Wildcard Domain Name]]* contained in the entry shall be composed entirely of LDH-Labels joined together by a U+002E FULL STOP "." character. The zero-length Domain Label representing the root zone of the Internet Domain Name System shall not be included (e.g. "example.com" shall be encoded as "example.com" and shall not be encoded as "example.com.").
  The Fully-Qualified Domain Name *[[ADV: or the FQDN portion of the Wildcard Domain Name]]* shall consist solely of Domain Labels that are P-Labels or Non-Reserved LDH-Labels. As an explicit exception from IETF RFC 5280 [48], P-Labels are permitted to not conform to IDNA 2003. These Requirements allow for the inclusion of P-Labels that do not conform with IDNA 2003 to support newer versions of the Unicode character repertoire, among other improvements to the various IDNA standards.

  [[ADV:

  iPAddress *:*

  The entry shall contain an IPv4 or IPv6 address that the Certification Service Provider has validated in accordance with Section 3.2.2.3.
  The entry shall not contain a Reserved IP Address.

  ]]

  Wildcard FQDNs are **[[QUA: not]]** permitted.

The "Subject Alternative Names" extension shall not contain *[[ADV: a Reserved IP Address or]]* an Internal Name.

The "dNSName" field shall be in the "preferred name syntax", as specified in IETF RFC 5280 [48], and thus shall not contain domain name containing underscore ("_") character.

>

<ALA:

- In case of natural person Subjects, for the Subject's request, his name written in different notation than in the field "Subject DN / commonName" can be indicated here (typically in the "CN" field of the "Subject Alternative Names" extension). That name can be written with or without accent marks. The Certification Service Provider is entitled to denote the nature of the name indicated.

  The Certification Service Provider verifies the names to be indicated on "Subject Alternative Names" extension. It takes a decision based on whether the name requested by the Client is indeed the name of the Subject, and that it does not mislead others. If the Subject in the exercise of its profession does not use its name indicated on its document used for identification, then it can request the Certification Service Provider to use that alternative name in the "Subject Alternative Names" extension.

>

<UNI:

- In case of natural person Subjects, for the Subject's request, his name written in different notation than in the field "Subject DN / commonName" can be indicated here (typically in the "CN" field of the "Subject Alternative Names" extension). That name can be written with or without accent marks. The Certification Service Provider is entitled to denote the nature of the name indicated.
- The Certification Service Provider verifies the names to be indicated on "Subject Alternative Names" extension. It takes a decision based on whether the name requested by the Client is indeed the name of the Subject, and that it does not mislead others. If the Subject in the exercise of its profession does not use its name indicated on its document used for identification, then it can request the Certification Service Provider to use that alternative name in the "Subject Alternative Names" extension.

>

<BEL: >

<UNI:

- The Certification Service Provider also verifies the content to be in the "Subject Alternative Names" extension, and decides on the names on an individual basis. A decision will be made on the basis whether it is proven that the Organization in question uses the name requested by the Client legally.

>

<not TLS:

– The Subject's email address can be given in the "Subject Alternative Names" extension "rfc822Name" field. If there's an email address indicated on the Certificate, then this field is definitely filled out. The Certification Service Provider verifies the validity of the email address according to chapter 3.2.7.

<UNI:

In case of Email (S/MIME) Certificate it always shall be filled out.

>

[[QUA:

<ALA:

In case of Email (S/MIME) Certificate it always shall be filled out.

>

<BEL:

In case of Email (S/MIME) Certificate it always shall be filled out.

>

]]

The same email address might be displayed in the "EMAIL" field of the Certificate.

<UNI:

– In case of national WRPAC Certificate, the "Subject Alternative Names" extension always contains one entry as follows:

dNSName :

The entry shall contain either a Fully-Qualified Domain Name that the Certification Service Provider has validated in accordance with Section 3.2.2.2.
The Fully-Qualified Domain Name contained in the entry shall be composed entirely of LDH-Labels joined together by a U+002E FULL STOP "." character.
The zero-length Domain Label representing the root zone of the Internet Domain Name System shall not be included (e.g. "example.com" shall be encoded as "example.com" and shall not be encoded as "example.com.").
The Fully-Qualified Domain Name shall consist solely of Domain Labels that are P-Labels or Non-Reserved LDH-Labels.

Wildcard FQDNs are not permitted.

The "Subject Alternative Names" extension shall not contain an Internal Name.

The "dNSName" field shall be in the "preferred name syntax", as specified in IETF RFC 5280 [48], and thus shall not contain domain name containing underscore ("_") character.

>

– Furthermore, the IETF RFC 4043 [44] "Permanent Identifier" can be included in the "Subject Alternative Names" extension. This is a different name forms that only contains the "assigner" field, in this the unique OID of the Certification Service Provider is indicated. Then according to the IETF RFC 4043 recommendation, this "assigner" OID together with the first "Serial Number" value – containing the OID allocated by the

Certification Service Provider– of the "Subject" field makes up the Subject permanent identifier.
<UNI:
Email (S/MIME) Certificate shall not contain this field.
>
[[QUA:
<ALA:
Email (S/MIME) Certificate shall not contain this field.
>
<BEL:
Email (S/MIME) Certificate shall not contain this field.
>
]]

>

<TLS:
[[QUA:

- **CA/Browser Forum Organization Identifier "cabfOrganizationIdentifier" – OID: 2.23.140.3.1**

  Filling is optional.

  It shall be filled, when the field "subject:organizationIdentifier" is filled in the Certificate.

  When the field is filled, it shall contain the same value as indicated in the "subject:organizationIdentifier" field.

]]
>

The Denomination of the Certificate Issuer Certification Unit

The identifier of the Certificate issuer (Issuer field) is made up as follows:

- commonName (CN) – OID: 2.5.4.3
  The name of the Certificate issuer certification unit in English (see section: 1.3.1).
- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  The name of the Certification Service Provider in English without accents.
- Organization Identifier (OrgId) – OID: 2.5.4.97
  Filling out is optional.

- Organizational Unit (OU) – OID: 2.5.4.11

  <TLS: It is not filled.>

  <not TLS:

  "e-Szigno CA"
  The name of the Certification Service Provider organization unit's name without accents. It was filled in the SHA-1 based provider Certificates, but it is not filled in the SHA-256 based provider Certificates.

  >

- Locality (L) – OID: 2.5.4.7
  "Budapest"
  City of the seat of the Certification Service Provider without accents.

- CountryName (C) – OID: 2.5.4.6
  "HU"
  Two letter code of the country of the seat of the Certification Service Provider according to ISO 3166-1 [36].

- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  "`info@e-szigno.hu` "
  Filling out is optional.

The same data is indicated in the provider Certificate of the Certificate issuer, in the subject identifier field.

The Alternative Names of the Certificate Issuer Certification Unit

The Issuer Alternative Names field is not filled in the end user Certificates.
Denominations indicated in the end user Certificate issuer's provider Certificate:

- In case of provider Certificates based on SHA-256 only the email address is indicated in the alternative names field (rfc822Name).

<BEL:

The Denomination of the Time stamping Unit

- commonName (CN) – OID: 2.5.4.3

  The name of the Time Stamping Unit.

- Organization (O) – OID: 2.5.4.10

  The name of the Time Stamping Service Provider.

- Organization Identifier (OrgId) – OID: 2.5.4.97

  The tax number of the Time Stamping Service Provider.
  Filling out is optional.

- Organizational Unit (OU) – OID: 2.5.4.11

  The name of the organizational unit of the Time Stamping Service Provider.
  The filling out is optional.

- Locality (L) – OID: 2.5.4.7
  "Budapest"
  City of the seat of the Certification Service Provider without accents.
  City of the seat of the Time Stamping Service Provider.

- CountryName (C) – OID: 2.5.4.6

  Two letter code of the country of the seat of the Time Stamping Service Provider according to ISO 3166-1 [36].

- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  It is not filled.

The Alternative Names of the Time Stamping Unit

This field is not included in the Certificates issued for Time Stamping Units.
>

The Denomination of the OCSP Responder

- commonName (CN) – OID: 2.5.4.3
  The field contains the name of the Certification Unit operating the OCSP Responder according to its "CN" concatenated with the following string:
  "OCSP Responder"

- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  The name of the Certification Service Provider in English without accents.

- Organization Identifier (OrgId) – OID: 2.5.4.97
  "VATHU-23584497"
  The tax number of the Certification Service Provider.
  Filling out is optional.

- Organizational Unit (OU) – OID: 2.5.4.11
  It is not filled.

- Locality (L) – OID: 2.5.4.7
  "Budapest"
  City of the seat of the Certification Service Provider without accents.
- CountryName (C) – OID: 2.5.4.6
  "HU"
  Two letter code of the country of the seat of the Certification Service Provider according to ISO 3166-1 [36].
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  It is not filled.

The Alternative Names of the OCSP Responder

This field is not included in the Certificates issued for OCSP Responders.

3.1.2 Need for Names to be Meaningful

The following rules are applied to the "SubjectDN" field:

- the identifier shall be meaningful

<TLS:
[[ADV:

- *the personal name in the Certificate shall be indicated the same way as verified by the Certification Service Provider according to the section 3.2.3.*

]]
>
<ALA:

- the personal name in the Certificate shall be indicated the same way as verified by the Certification Service Provider according to the section 3.2.3.

>
<UNI:

- the personal name in the Certificate shall be indicated the same way as verified by the Certification Service Provider according to the section 3.2.3.

>

- the name of the Organization in the Certificate shall be indicated the same way as verified by the Certification Service Provider according to the section 3.2.2.

3.1.3 Anonymity or Pseudonymity of Subscribers

<TLS: Website Authentication Certificate shall not be pseudonymous. >

<ALA: The Certification Service Provider doesn't issue Certificate with pseudonym.>

<BEL: Seal certificate shall not be pseudonymous. >

<UNI: The Certification Service Provider doesn't issue Certificate with pseudonym.>

3.1.4 Rules for Interpreting Various Name Forms

In order to interpret the identifiers, it is recommended for the Relying Parties to act as described in this document. If the Relying Party is in need for help related to the interpretation of the identifier or any other data indicated in the Certificate, it can contact directly the Certification Service Provider. In such case, the Certification Service Provider shall not give any further information on the Client than indicated in the Certificate, – provided that the law does not require it – only provides the information to help interpret the indicated data.

3.1.5 Uniqueness of Names

The Subject has a unique name in the Certificate Repository of the Certification Service Provider.

To ensure uniqueness, the Certification Service Provider assigns each Subject an identifier (OID) that is unique in the Certification Service Provider's registry. The assignment of unique identifiers to Subject is done in the order in which the received Certificate Applications are processed.

<not TLS:

The Subject's unique identifier is included in the "Subject DN Serial Number" field of the Certificate, which in itself guarantees the uniqueness of the "Subject" field.

>

<TLS:

Every Website Authentication Certificate contains an FQDN or IP address value in the "Subject DN CommonName" field of the Certificate, which in itself ensures the uniqueness of the "Subject" field.

The OVCP **[[QUA: and EVCP]]** Certificate also contains the name of the organization exercising control over the domain or IP address in the "Subject DN Organization" field. The "Subject DN Organization Identifier" field may optionally contain the official business registration number of the organization named in the Certificate.

[[QUA: In the case of an EVCP Certificate, the Subject's unique company registration number must be included in the "Subject DN Serial Number" field of the Certificate.]]

>

<not TLS:

The Certification Service Provider can indicate other unique identifier (for example, identity card number, tax number, and identification within the organization) on request.

>

Procedures to Resolve Disputes Relating the Names

The Certification Service Provider ensures that the Client is entitled to use the indicated names.

The Certification Service Provider revokes the Certificate in case of illegal use of the name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Certification Service Provider never includes trademark in the issued Certificate.

The Certification Service Provider uses the e-Szignó trademark during its service provision. The owner has given his consent to use the trademark.

3.2 Initial Identity Validation

The Certification Service Provider can use any communication channel within the limits provided by law, for the verification of the identity of the person or organization requesting the Certificate, and for checking the authenticity of the data provided.

Evidence obtained during the identity validation carried out as part of the initial registration can be reused by the Certification Service Provider in the future when issuing new Certificates, if the identified natural or legal person is verifiably the same as the person to be identified in the new procedure.

During the procedure, it is necessary to confirm the validity of the personal data registered by the Certification Service Provider, the previously recorded data can be used for a maximum of <TLS: 398 days > <not TLS: 3 months> without performing another data check.

The Certification Service Provider may, in its sole discretion, refuse the issuance of the requested Certificate without any specific justification.

3.2.1 Method to Prove Possession of Private Key

Prior to the issuance of a Certificate, the Certification Service Provider ensures and makes sure that the Applicant actually owns or manages the private key belonging to the public key of the Certificate.

<ALA:

[[QUA:

If the Certification Service Provider generates within its organization the private key belonging to the qualified Certificate of the Subject – typically on Qualified Electronic Signature or Seal Creation Device or on Cryptographic Hardware Device in case of Certificate Policies requiring such – , then it does not have to specially verify that the Applicant owns the private pair of the public key to be verified.

]]

>

<BEL:

[[QUA:

If the Certification Service Provider generates within its organization the private key belonging to the qualified Certificate of the Subject – typically on Qualified Electronic Signature or Seal Creation Device or on Cryptographic Hardware Device in case of Certificate Policies requiring such – , then it does not have to specially verify that the Applicant owns the private pair of the public key to be verified.

]]

>

<UNI:

If the Certification Service Provider generates within its organization the private key belonging to the Certificate of the Subject – typically on Cryptographic Hardware Device in case of Certificate Policies requiring such – , then it does not have to specially verify that the Applicant owns the private pair of the public key to be verified.

>

<TLS:

The Certification Service Provider receives the Certificate Application in PKCS#10 format, which also certifies that the holder of the private key has indeed requested the Certificate for the given Subject.

>

<not TLS:

If the Applicant requests the issuance of a Certificate for the key provided by it -– typically in the case of software certificates -– then the Certification Service Provider receives the Certificate Application in PKCS#10 format, which also certifies that the holder of the private key has indeed requested the Certificate for the given Subject.

>

<ALA:

The Certification Service Provider considers equivalent evidence that the Subject submits the Certificate Application with the public key to be included in the requested Certificate signed with the use of a valid **[[QUA: qualified]]** Certificate based electronic signature.

>

<not TLS:

[[QUA:

If the Subject private key is generated and managed by another Trust Service Provider, then the Trust Service Provider verifies that, the referred Trust Service Provider owns the private key, and it is under the sole control of the Subject. The Certification Service Provider may accept the authentic statement of the referred Trust Service Provider about this. The format of the statement may be electronic. The Certification Service Provider verifies the authenticity of the statement.

The verification of the ownership happens with the acceptance of a PKCS#10 formatted Certificate Application.

]]

>

3.2.2 Authentication of an Organization Identity <TLS: or a Domain>

<TLS:

3.2.2.1 Authentication of organization identity

>
The identity of the Organization is verified in the following cases:

- if the Subject of the Certificate to be issued is the Organization
- if the Subject of the Certificate to be issued is the device or system operated by the Organization <TLS: (including the Website Authentication Certificates requested by the Organization) >

<ALA:

- if the Certificate is issued to a natural person, but the name of the Organization is indicated on the Certificate as well.

>
<UNI:

- if the Certificate is issued to a natural person, but the name of the Organization is indicated on the Certificate as well.

>
Prior to the issuance of an Organizational Certificate the Certification Service Provider verifies the organizational data authenticity to be included on the Certificate based on authentic public registers<TLS: **[[QUA: (Qualified Government Information Source)]]** >.
<TLS:
[[QUA:

Other documents

In case of EVCP Certificates:

- **During the validation process of Private Organizations, the Certification Service Provider verifies that the Organization**
  - **legally exists, listed in the official company registration and has an active registered status**
  - **physically exists, the registered address is a real address where the Organization conducts business operations**
  - **is active, conducts real business operations.**
- **During the validation process of Government Entities, the Certification Service Provider verifies that the Organization**

  - **legally registered government unit in the proper government structure**
  - **has an active status**
  - **the name given in the Certificate Application is exactly the same as the officially registered name of the Organization**
  - **the exact date of the establishment the Organization or the identifier of the legal act which established it if exists.**

- **During the validation process of Government Entities, the Certification Service Provider receives the information directly from the following government information sources:**
  - **reliable source of government information from the same government body**
  - **reliable source of government information from the superior government body**
  - **from a judge who is an active member of the State Judiciary in that political subdivision**

]]

>

Furthermore, it is verified in these cases, that:

- whether the natural person acting on behalf of the Organization is entitled to act on behalf of the Organization
- whether the Organization consented to the issuance of the Certificate.

For performing the verification, the Client shall give the following data:

- the official denomination, registered office and legal status of the Organization
- official registration number of the Organization (e.g. company registration number, tax identification number), if applicable
- the name of the organization unit within the Organization, if its indication in the Certificate is requested,

<ALA:

- in case of an Organizational Certificate issuance to a natural person, the role of the Subject within the Organization, if its indication in the Certificate is requested.

>

<UNI:

- in case of an Organizational Certificate issuance to a natural person, the role of the Subject within the Organization, if its indication in the Certificate is requested.

- If the Subject is a legal person and the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then the Client shall give the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the Subject or another registration identifier of the Subject recognized by the NCA, the type of the payment service(s) and the name of the NCA.

>
<TLS:
[[QUA:

- **If the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then the Client shall give the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the Subject or another registration identifier of the Subject recognized by the NCA, the type of the payment service(s) and the name of the supervisory authority.**

]]
>
<BEL:
[[QUA:

- **If the Client requests the inclusion of the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] in the Certificate, then the Client shall give the authorization number of the Subject issued by the national competent authority (NCA) supervising the payment services of the Subject or another registration identifier of the Subject recognized by the NCA, the type of the payment service(s) and the name of the supervisory authority.**

]]
>
The following certificates and evidences have to be attached to the Certificate Application:

- the submitter's statement, justifying that the data given for the Organization identification is correct and comply with reality

<not SIG:

- a certificate regarding that on behalf of the organization the Certificate Application submitter natural person is entitled to submit the application [2]

>
<ALA:

[2]Section 3.2.5 contains the details regarding the verification of the authorizations and privileges.

- in case of an Organizational Certificate issuance to a natural person, the certificate regarding that the organization consents to that the name of the organization is indicated on the certificate issued to the natural person [3]

>
<UNI:

- in case of an Organizational Certificate issuance to a natural person, the certificate regarding that the organization consents to that the name of the organization is indicated on the certificate issued to the natural person [4]

>

- In case of paper based documents the specimen signature of the person entitled to represent the Organization or other, official document equal to the specimen signature, which contains the name and signature of the persons entitled to represent the Organization [5]
- the Organization existence, name and the legal status verification document [6].

The Certification Service Provider is bound to verify the validity and authenticity of the presented documents.

3.2.2.1.1 Identity validation of foreign Organizations

The Certification Service Provider does not exclude the verification of Organizations registered abroad, as far as the data verification with adequate records of the country or obtaining a certificate issued by a trusted third party is feasible.

In respect of data verification, the Certification Service Provider accepts:

- information obtained directly from the government register of the foreign country by the Certification Service Provider or queried by a third party but authenticated by the primary data provider
- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information is correct
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the given information is correct.

[3] Section 3.2.5 contains the details regarding the verification of the authorizations and privileges.
[4] Section 3.2.5 contains the details regarding the verification of the authorizations and privileges.
[5] In case of Court of Registration registered firms the above documents can be acquired by the Certification Service Provider.
[6] In case of Court of Registration registered firms the above documents can be acquired by the Certification Service Provider.

The Certification Service Provider may accept other documents and evidences too, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the Certification Service Provider is the Client's responsibility.

The Certification Service Provider only accepts valid documents, and evidences not older than 3 months.

The Certification Service Provider does not issue the Certificate if it considers that based on its internal rules it can not verify with corresponding confidence a certificate issued abroad, a document or the data of the foreign organization.

<TLS:

3.2.2.1.2 Identity validation traced back to a certificate of an electronic seal

The Certification Service Provider may also trace the identity of the organization to a Certificate of an electronic seal, if the seal Certificate used as the basis for identity validation was issued to the same organization to which the Certificate is issued.

In this case:

- The Applicant submits the Certificate Application in electronic form with *[[ADV: an electronic seal]]* **[[QUA: a qualified electronic seal.]]** *[[ADV: based on a Certificate with a security classification (see section 1.2.3) not lower than the requested Certificate.]]*
- The seal Certificate used as the basis for identity validation shall contain all data needed for the unambiguous identification of the organization.
- The Certification Service Provider verifies the authenticity and confidentiality of the Certificate Application on the entire certification chain.

[[QUA:

- **The Certification Service Provider accepts only those electronic seals which are based on a Certificate issued by a Trust Service Provider according to a Trust Service, which is listed on a national Trusted List published on the EU List of Lists and was valid at the time of the signature creation.**
- **The Certification Service Provider may accept only those electronic seals, which are based on such a Certificate, which was issued based on the identity validation of the natural person acting on behalf of the organization in compliance with the paragraph (1) point (a) or (b) of Article 24 of the eIDAS regulation [1].**

]]

>

<not TLS: <not SIG:

Identity validation traced back to a certificate of an electronic seal

The Certification Service Provider may also trace the identity of the organization to a Certificate of an electronic seal, if the seal Certificate used as the basis for identity validation was issued to the same organization to which the Certificate is issued.

In this case:

- The Applicant submits the Certificate Application in electronic form with **[[QUA: a qualified electronic seal.]]** *[[ADV: an electronic seal based on a Certificate with a security classification (see section 1.2.3) not lower than the requested Certificate.]]*
- The seal Certificate used as the basis for identity validation shall contain all data needed for the unambiguous identification of the organization.
- The Certification Service Provider verifies the authenticity and confidentiality of the Certificate Application on the entire certification chain.

[[QUA:
In case of a qualified Certificate:

- **The Certification Service Provider accepts only those electronic seals which are based on a Certificate issued by a Trust Service Provider according to a Trust Service, which is listed on a national Trusted List published on the EU List of Lists and was valid at the time of the signature creation.**
- **The Certification Service Provider may accept only those electronic seals, which are based on such a Certificate, which was issued based on the identity validation of the natural person acting on behalf of the organization in compliance with the paragraph (1) point (a) or (b) of Article 24 of the eIDAS regulation [1].**

]]
>>
<TLS:

3.2.2.2 DBA/Tradename

See in section 3.1.6.

3.2.2.3 Verification of Country

See in section 3.1.1 at "CountryName (C) – OID: 2.5.4.6 – Identifier of the country".

3.2.2.4 Validation of Domain Authorization or Control

At least one domain name *[[ADV: or IP address]]* shall be in the Website Authentication Certificates.

Before the issuance of Website Authentication Certificates, the Certification Service Provider ensures about the genuineness of the domain name *[[ADV: or IP address]]* to be indicated in the

Certificate, and the Applicant shall demonstrate in practice that he has control over the given domain name *[[ADV: or IP address]]* .

If more than one domain name *[[ADV: or IP address]]* is indicated in the Certificate, the aforementioned verification shall be carried out in each case.

The Certification Service Provider issues Certificates for public domain names *[[ADV: and IP addresses]]* used on the Internet, not for domain names *[[ADV: and IP addresses]]* reserved for internal use.

The Certification Service Provider issues Certificates only for those top-level domains which can be found on the actual IANA Root Zone Database.

The Certification Service Provider supports the usage of the Internationalized Domain Names according to the IDNA2003 [39] requirements.

The Certification Service Provider doesn't issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

The Certification Service Provider doesn't issue Certificate for the ".onion" 'special use' top level domain.

The Certification Service Provider shall confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below in line with the requirements of the latest version of the CA/Browser Forum Baseline Requirements [63].

DNSSEC validation back to the IANA DNSSEC root trust anchor will be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective will :

- perform DNSSEC validation using the algorithm defined in RFC 4035 [43] Section 5, and
- support NSEC3 as defined in RFC 5155 [47], and
- support SHA-2 as defined in RFC 4509 [45] and RFC 5702 [49], and
- properly handle the security concerns enumerated in RFC 6840 [52] Section 4.

DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The Certification Service Provider will not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of the logging requirements of Section 5.4.1.

The Certification Service Provider maintains a record of which of the following domain validation methods was used, including the relevant CABF BR version number.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This validation method is not used.

3.2.2.4.2 Email to Domain Contact

This validation method is not used.

3.2.2.4.3 Phone Contact with Domain Contact

This validation method is not used.

3.2.2.4.4 Constructed Email to Domain Contact

This validation method is not used.

3.2.2.4.5 Domain Authorization Document

This validation method is not used.

3.2.2.4.6 Agreed-Upon Change to Website

This validation method is not used.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Request Token containing a Random Value in a DNS TXT record for an Authorization Domain Name.

The Certification Service Provider provides unique Request Token for each Certificate Application which is valid only for 30 days.

The Certification Service Provider uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [63].

The use of his validation method is supported by the Certification Service Provider also by using ACME protocol.

Once the FQDN has been validated using this method, the Certification Service Provider may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

[[ADV:

This method is suitable for validating Wildcard Domain Names.

]]

3.2.2.4.8 IP Address

This validation method is not used.

3.2.2.4.9 Test Certificate

This validation method is not used.

3.2.2.4.10 TLS Using a Random Number

This validation method is not used.

3.2.2.4.11 Any Other Method

This validation method is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact

This validation method is not used.

3.2.2.4.13 Email to DNS CAA Contact

This validation method is not used.

3.2.2.4.14 Email to DNS TXT Contact

This validation method is not used.

3.2.2.4.15 Phone Contact with Domain Contact

This validation method is not used.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

This validation method is not used.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

This validation method is not used.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token including a Random Value is contained in the contents of a file.

- The entire Request Token shall not appear in the request used to retrieve the file, and
- the Certification Service Provider shall receive a successful HTTP response from the request (meaning a 2xx HTTP status code shall be received).

The file containing the Request Token:

- shall be located on the Authorization Domain Name, and
- shall be located under the "/.well-known/pki-validation" directory, and

- shall be retrieved via either the "http" or "https" scheme, and
- shall be accessed over an Authorized Port.

The Certification Service Provider doesn't accept redirects (3xx HTTP status code).
The Random Value included in the Request Token:

- is unique to each Certificate Application
- will remain valid for use in a confirming response for 30 days from its creation.

The Certification Service Provider shall not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the Certification Service Provider performs a separate validation for that FQDN using an authorized method.
The Certification Service Provider uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [63].
[[ADV:
This method is not suitable for validating Wildcard Domain Names.
]]

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over the FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555 [55].

- the Certification Service Provider shall receive a successful HTTP response from the request (meaning a 2xx HTTP status code shall be received).
- the Certification Service Provider doesn't accept redirects (3xx HTTP status code).

The Random Value included in the Request Token:

- is unique to each Certificate Application
- will remain valid for use in a confirming response for 30 days from its creation.

The Certification Service Provider uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [63].
[[ADV:
This method is not suitable for validating Wildcard Domain Names.
]]

3.2.2.4.20 TLS Using ALPN

This validation method is not used.

3.2.2.4.21 DNS Labeled with Account ID - ACME

This validation method is not used.

3.2.2.4.22 DNS TXT Record with Persistent Value

This validation method is not used.

3.2.2.5 Authentication for an IP Address

[[QUA:
The EV Certificate shall not contain IP Address so there is no need to validate IP Addresses.
]]
[[ADV:
This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.

The Certification Service Provider confirms that prior to issuance, the Certification Service Provider validates each IP Address listed in the Certificate using at least one of the methods specified in this section.

Completed validations of Applicant's authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation shall have been initiated within the time period specified in the Section 4.2.1 of this document prior to Certificate issuance.

The Certification Service Provider maintains a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

3.2.2.5.1 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested IP Address by confirming the presence of a Random Value contained in the content of a file under the "/.well-known/pki-validation" directory on the IP Address that is accessible by the Certification Service Provider via HTTP/HTTPS over an Authorized Port.

The Random Value shall not appear in the request.

The Certification Service Provider shall provide a Random Value unique to the Certificate Application and shall not use the Random Value longer than 30 days.

The Certification Service Provider uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [63].

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

This validation method is not used.

3.2.2.5.3 Reverse Address Lookup

This validation method is not used.

3.2.2.5.4 Any Other Method

This validation method is not used.

3.2.2.5.5 Phone Contact with IP Address Contact

This validation method is not used.

3.2.2.5.6 ACME "http-01" method for IP Addresses

This validation method is not used.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

This validation method is not used.

3.2.2.5.8 DNS TXT Record with Persistent Value in the Reverse Namespace

This validation method is not used.
]]

3.2.2.6 Wildcard Domain Validation

[[QUA:
Issuance of qualified Website Authentication Certificates for wildcard domains is not allowed.
]]
[[ADV:
If a domain name containing a wildcard "" character is indicated in the Certificate (wildcard certificate), the Certification Service Provider ensures that, the Applicant is the authorized user of the entire domain namespace covered by the wildcard domain name. The Certification Service Provider does not issue a Certificate, in which the domain name space to be covered by the wildcard domain name is a registered gTLD or ccTLD (for example: "*.com", "*.co.uk"), or a subdomain under these TLDs under which public domain name registration is directly possible. The Certification Service Provider checks the public domain names open for direct registration in the "ICANN DOMAINS" section of "Public Suffix List" (https://publicsuffix.org/list/public_suffix_list.dat).*
]]

3.2.2.7 Data Source Accuracy

The Certification Service Provider, when available, uses Qualified Government Information Sources (QGIS) to obtain validation information about private and legal persons.

When QGIS is not available, the Certification Service Provider may use other information source, but before using the source it evaluates the reliability of the data source considering the following:

- the age of the information provided
- the frequency of updates to the information source
- the data provider and purpose of the data collection
- the public accessibility of the data availability
- the relative difficulty in falsifying or altering the data

[[QUA:

Information Source

The Certification Service Provider maintains a register of the public registers and their contact details accepted during the investigation, which shall be published via the Certification Service Provider's website at the following location:

`https://e-szigno.hu/all-documents`

]]

3.2.2.8 CAA records

As part of the issuance process, the Certification Service Provider retrieves and processes CAA records in accordance with IETF RFC 8659 [56] for each dNSName in the subjectAltName extension of the Website Authentication Certificate to be issued.

The Certification Service Provider will only issue the requested Website Authentication Certificate if the following conditions are independently met for each dNSNames in the subjectAltName extension of the Website Authentication Certificate to be issued:

[[QUA:

- **the first filled CAA record**
  - **does not contain an entry 'issue', or**
  - **contains the entry 'issue "e-szigno.hu"'**
- **there is now filled CAA record in the chain**

]]

[[ADV:

- *in case of Wildcard FQDN*
  - *the first filled CAA record*
    - *contains neither 'issue' nor 'issuewild' entries, or*
    - *does not contain the entry 'issuewild' and contains the entry 'issue "e-szigno.hu"', or*
    - *contains the entry 'issuewild "e-szigno.hu"'*

- *there is now filled CAA record in the chain*

- *in case of non-Wildcard FQDN*
  - *the first filled CAA record*
    - *does not contain an entry 'issue', or*
    - *contains the entry 'issue "e-szigno.hu"'*
  - *there is now filled CAA record in the chain*

]]

The presence of other known Property Tags, such as 'issuemail', does not restrict the issuance of Website Authentication Certificates. The Certification Service Provider does not issue a Website Authentication Certificate if it encounters an unrecognized property tag with critical flag set.

In case of any CAA authorization issue is detected, the Certification Service Provider attempts to contact the Applicant using the trusted communication channel verified earlier, or the contact details stipulated in the CAA 'iodef' property tag, if present, to resolve the issue. The Certification Service Provider only supports the "mailto:" URL scheme in the 'iodef' record.

The Certification Service Provider documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances.

In any case, right before issuing the Website Authentication Certificate, the Certification Service Provider automatically rechecks the CAA records.

3.2.2.8.1 DNSSEC Validation of CAA Records

DNSSEC validation back to the IANA DNSSEC root trust anchor will be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective will :

- perform DNSSEC validation using the algorithm defined in RFC 4035 [43] Section 5, and
- support NSEC3 as defined in RFC 5155 [47], and
- support SHA-2 as defined in RFC 4509 [45] and RFC 5702 [49], and
- properly handle the security concerns enumerated in RFC 6840 [52] Section 4.

The Certification Service Provider will not use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.

DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) will not be treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor MAY be performed on all DNS queries associated with CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

The set of responses from the relied upon Network Perspectives shall provide the CA with the necessary information to allow it to affirmatively assess:

- the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and 3.2.2.5 and
- the CA's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Results or information obtained from one Network Perspective shall not be reused or cached when performing validation through subsequent Network Perspectives. All communications between a remote Network Perspective and the CA shall take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers shall be at least 500 km. CAs may immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method, but when retrying Multi-Perspective Issuance Corroboration, CAs shall not rely on corroborations from previous attempts.

If any of the above considerations are performed by a Delegated Third Party, the CA may obtain reasonable evidence from the Delegated Third Party to ascertain assurance that one or more of the above considerations are followed. As an exception to Section 1.3.2, Delegated Third Parties are not required to be within the audit scope described in Section 8 of these Requirements to satisfy the above considerations.

Deadline	min. number of Remote Network Perspectives	allowed non-Corroborations
2025-03-15	2	—
2025-09-15	2	1
2026-03-15	3	1
2026-06-15	4	1
2026-12-15	5	1

Implementation requirements

In case of more than 6 Remote Network Perspectives the allowed non-Corroborations is 2.

>

3.2.3 Authentication of an Individual Identity

<TLS:

The identity of the Website Authentication Certificate requester natural person shall be verified.

>
<not TLS:
The natural person's identity shall be verified:
<ALA:

- if the Subject of the Certificate to be issued is a natural person

>
<UNI:

- if the Subject of the Certificate to be issued is a natural person

>

- if a natural person is acting on behalf of an Organization for Organizational Certificate application.

>
[[QUA:
When issuing a qualified Certificate, the identity of the natural person shall be verified according to (1a) paragraph of Article 24 of the eIDAS regulation [1] modified by Regulation (EU) 2024/1183 [4] . The Certification Service Provider uses the identification methods described in the (1a) paragraph of Article 24. as follows.
]]
The Certification Service Provider verifies the identity of the natural person applying one of the following methods, subject to the availability of technical and other conditions.

1. **During face to face identity validation**

   [[ADV: In case of ***[[QUA: qualified Certificates and non-qualified]]*** *Certificates belonging to the III. certification class:]]*

   - the natural person shall appear in person before the person performing the identity validation, who may be one of the following:
     - officer of the Registration Authority
     - state notary, as a third party in accordance with the Hungarian legislation
     - a reliable third party in a contractual relationship with the Certification Service Provider
   - the identity of the natural person is verified during personal identification based on a suitable official proof of identity card

     The identification can be based on the following official documents:
     - in case of natural persons within the scope of Act LXVI. of 1992. (henceforth: Nytv. [6]) official cards appropriate for verifying identity defined in Nytv.

  - in case of natural persons outside the scope of Nytv. [6] on the basis of a travel document defined in the Act on the entry and residence of persons enjoying the right of free movement and residence or the law on entry and residence of third-country nationals [8]
  - in case of identification of natural persons who have none of the documents mentioned above the Certification Service Provider applies personal identity validation in accordance with Dap tv. 85.§ (5) [13] only in the case of identifying European citizens. In such case a personal identity card or a card format driver's licence listed in the public online database of "PRADO - Public Register of Authentic identity and travel Documents Online" [76], issued by the European country of natural person's nationality is accepted as a trusted document for identity validation.
- the natural person shall declare the correctness of the personal identification data used for the identity validation with a written statement signed with a handwritten signature in the presence of the identification person

<ALA:

- In case of natural persons within the scope of Nytv. [6] the validity of the data on the identity card used for personal identification and the validity of the identity card is validated by the Registration Authority by using an authentic public register. In case of any other natural persons the Certification Service Provider doesn't validate the validity of the data on the identity card used for personal identification and the validity of the identity card by using an authentic public register, if such register is not available, it is not accessible to the Certification Service Provider or the costs of access and control are disproportionately high.

>

<TLS:

- the natural person's address shall be checked against a residence card suitable for identification

>

- The person performing the identity validation verifies, whether any alteration or counterfeiting happened to the presented identity cards.

<ALA:

During the initial identity validation the Certification Service Provider may accept the identification of a natural person carried out by a state notary as equivalent to the identity validation made by its own Registration Authority, if it can be stated on the basis of the notarial certification clause attached to the Certificate Application signed before the notary that the state notary had compared the personal data of the Applicant having appeared before the notary with the content of an authentic public registry or other central database.

>

<not SIG:

During the initial identity validation the Certification Service Provider may accept the identification of a natural person carried out by a state notary as equivalent to the identity validation made by its own Registration Authority.

>

[[ADV:

In case of Certificates belonging to the II. certification class:

- *there's no need for personal meeting for the identification of the person, in such cases the Certification Service Provider can identify the Subject or Applicant remotely*
  During remote identification, the Certification Service Provider may ask the natural person to be identified to take a photograph of herself/himself in accordance with the prescribed conditions and send it to the Certification Service Provider.
- *the Subject or Applicant sends a copy of one of its official identity cards suitable for identity validation to the Certification Service Provider.*

<TLS:

- *the Subject or Applicant sends the copy of its official identity cards suitable for the validation of its address to the Certification Service Provider.*

>

- *the natural person shall verify the accuracy of the data for the registration and identity validation with a statement signed with a handwritten signature*

<not UNI:

- *the Certification Service Provider performs data reconciliation with authentic public registers in case of certificates belonging to the II. certification class.*

>

<TLS:

- *the natural person's address shall be checked against a residence card suitable for identification*
- *The Registration Authority verifies the authenticity of the presented cards in this case too. Furthermore, the Certification Service Provider verifies that the Certificate Application was really sent by the identified Subject or Applicant through a trustable communication channel. Then the Certification Service Provider asks for confirmation from the Subject or Applicant through such a contact that was not given during the application procedure, but it originates from other sources. There is no need for confirmation through more reliable communication channel, in case of identification performed by an appropriate electronic identification device or by a Certificate Application submitted with an appropriate electronic signature.*

>

- *The Subject or Applicant can prove its identity at its own discretion according to the III. certification class.*

]]

Further rules for the identity validation of foreign citizens

The Certification Service Provider may accept the identification carried out by a public notary as equivalent to the identity validation made by its own Registration Authority, if the public notary registered in such foreign country,

- which concluded an international bilateral treaty with Hungary on the mutual recognition of public deeds or
- which country ratified the "Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents" of 5th October 1961. (Apostille)

The document issued by the public notary shall follow the requirements specified in the given agreement.

The Certification Service Provider may accept the Certificate Application signed before the notary public if the notarial certification clause shows that

- the notary public has verified the identity of the Applicant based on a suitable official document for identity validation (ID card, passport etc.)
- the Applicant has signed the Certificate Application in the presence of the notary public.

The Certification Service Provider always accepts the original documents when issued in Hungarian or English language. In case of documents issued on any other language the Certification Service Provider may request the official Hungarian translation of the documents translated by the OFFI (Hungarian Office for Translation and Attestation).

The Certification Service Provider may also accept other documents and evidences, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the Certification Service Provider is the Client's responsibility.

The Certification Service Provider only accepts valid documents and evidences not older than 3 months.

The Certification Service Provider does not issue the Certificate if it considers that based on its internal rules, that it can not verify with corresponding confidence the certificate, document or the data of the foreign organization.

2. **By identification traced back to a certificate of an electronic signature**

In this case:

- The Applicant submits the Certificate Application in electronic form with **[[QUA: a qualified electronic signature based on a non-pseudonymous qualified Certificate.]]** *[[ADV: an electronic signature based on a non-pseudonymous Certificate with a security classification (see section 1.2.3) not lower than the requested Certificate.]]*
- The electronically signed Certificate Application shall contain the data needed for the unambiguous identification of the natural person.

- The Certification Service Provider verifies the authenticity and confidentiality of the Certificate Application on the entire certification chain.

[[QUA:

- **The Certification Service Provider accepts only those electronic signatures which are based on a Certificate issued by a Trust Service Provider according to a Trust Service, which is listed on a national Trusted List published on the EU List of Lists and was valid at the time of the signature creation.**
- **The Certification Service Provider may accept only those electronic signatures which are based on such a Certificate which was issued in compliance with the paragraph (1a) point (a), (c) or (d) of Article 24 of the eIDAS regulation [1].**

]]

<ALA:

- depending on the Subject data included in the Certificate used to authenticate the Certificate Application
  - if the identity of the Subject cannot be clearly determined based on the data, the Certification Service Provider will only include Subject data in the new Certificate
    - that matches the Subject data in the Certificate used to authenticate the Certificate Application
    - other data may only be included in the Certificate to be issued if the Subscriber is authorized to include the new data (e.g. organization, organizational unit, title, etc.) and the Subscriber credibly proves that the new data relates to the Subject of the Certificate used to authenticate the Certificate Application
  - if the identity of the Subject can be clearly established based on the data (e.g. it contains the Subject's identity card number or other unique identification data), the Certification Service Provider may include data in the new Certificate that is different from the Subject data contained in the Certificate used to authenticate the Certificate Application.

>

<UNI:

3. **By identification traced back to an authentication certificate**

   In this case:

   - the Applicant logs into a protected website supported by Certification Service Provider by using a non-pseudonymous Certificate with a security classification (see section 1.2.3) not lower than the requested Certificate
   - the Certification Service Provider verifies the validity of the Certificate on the entire certification chain

- the Applicant submits the Certificate Application in electronic form by using the certificate request form of the website
- The Certificate Application shall contain all the data needed for the unambiguous identification of the natural person.
- the Certification Service Provider verifies that the data given in the Certificate Application and the data included in the authentication Certificate match
- the Certification Service Provider includes the same Subject data into the new Certificate which were in the authentication Certificate.

>

4. **By using other identification methods that ensure the identification of the person at a high level of reliability, and the conformity of which must be certified by a conformity assessment organization**

   - The Certification Service Provider can also establish the identity of the natural person by means of an electronic communication device providing video technology (hereinafter: video technology identification)

   During the video technology identification, the Certification Service Provider:

   (a) In the case of video technology identification, the Certification Service Provider takes a video image of the Client during a live telecommunication connection, then compares the image taken of the Client with the photograph in the document used for identification (hereinafter: ID document). Identification is appropriate if it can be clearly established by the Certification Service Provider that the person in the ID document is the same as the Client in the video.

   (b) The Certification Service Provider sets out in detail in the "Information on online video identification terms" [80] document the conditions for the use of video technology identification, in particular the minimum requirements for the quality of the video connection. The document will be published via the Certification Service Provider's website in accordance with the public regulations.
   In order to perform a successful video technology identification, it is advisable to provide the following conditions:
      - ID document in good condition
      - properly lit environment
      - quiet, undisturbed environment
      - exclusion of the presence of other persons
      - IT device with two-way audio and video capability
      - camera with min. 2-megapixel video resolution
      - stable internet connection at a speed of min 1.5Mbps.

   (c) By presenting the Certification Practice Statement and the "Information on online video identification terms" [80] document and during the video recording, the Certification Service Provider ensures that the Client can get to know the conditions of the video technology identification in detail, and has expressly agreed to comply with them, and acts accordingly.

(d) The Certification Service Provider records and keeps for at least 10 years from the date of recording the entire communication established between the Certification Service Provider and the Client during the video technology identification, the detailed information of the Client related to video technology identification, and the Client's express consent to this in a retrievable way, on video and audio, on a way that does not degrade the quality of the image and sound recording.

(e) The condition of successful video technology identification is that the image resolution of the electronic communication device enabling video technology identification and the illumination of the image be suitable for recognizing the gender, age and facial features of the Client, and the Client

- shall look into the camera so that his or her portrait can be recognized, captured and identified on the basis of the portrait shown on the ID document presented by him or her
- shall communicate in a comprehensible manner the identifier of the document used for video identification
- present his / her ID document in such a way that the security features and data sets contained therein can be identified, recorded and verified, and
- the data contained in the ID document can be matched with the data available about the Client at the Certification Service Provider, and the Client can be identified with the image shown on the ID document based on his / her image.

(f) The Certification Service Provider makes sure that the document is suitable for performing video technology identification, so

- the document complies with the requirements of the issuing authority
- the individual security features, in particular the hologram, the kinegram or other equivalent security features, are recognizable and undamaged, and
- the document ID is the same as the document ID provided by the Client, recognizable and undamaged.

(g) During the video technology identification, the Certification Service Provider makes sure that

- the Client's portrait is recognizable and identifiable by the portrait on the document presented by him, and
- the data contained in the document can be logically corresponded to the data available about the Client at the Certification Service Provider.

(h) A live telecommunications connection is also eligible if the Certification Service Provider examines the terms by machine or after the termination of the telecommunications connection, but makes sure that the Client is in a live connection during the identification.

The Certification Service Provider shall issue the Certificate only if the video technology identification fully complies with the above requirements.

5. **Using other nationally recognized methods of identification offering security equivalent to personal presence**

Until May 26, 2026 at the latest, the Certification Service Provider may also verify the identity of the natural person in accordance with Article 51 (4) of the eIDAS Regulation [1]

541/2020. (XII. 2.) Hungarian Government Decree [18], using the following method which are recognized as equivalent to the face to face validation at national level.

- identification using the identification service provided by the Hungarian Government pursuant to Section 4 (1) of the Decree (hereinafter: eID (KASZ) identification)

In this case, the Certification Service Provider shall proceed as prescribed during the identification based on personal presence, with the difference that the personal presence shall be replaced by an identification procedure recognized as equivalent at the national level.

During the eID (KASZ) identification, the Certification Service Provider:

(a) In the case of eID (KASZ) identification, the IT system provided by the Certification Service Provider allows the Client, if it has an electronic identification service provided by the Hungarian Government, to identify himself / herself in front of the Certification Service Provider with an electronic identification service provided by means of an identity card containing a storage element provided by the Hungarian Government.

(b) The Certification Service Provider uses the central and regulated electronic administration services required for identification as a market participant.

(c) The Certification Service Provider may use the authentication service through the central authentication agent service or independently.

The Certification Service Provider uses the data reconciled during a previous natural person identification procedure, if the Subject or Applicant requests new Certificate instead of an expired or a revoked one, or if he requests a new Certificate besides the existing one during the validity period of the service agreement. The authenticity of the Certificate Application, the validity of the data to be included in the Certificate and the identity of the Applicant is validated by the Certification Service Provider.

3.2.4 Non-Verified Subscriber Information

Only that data can be in the Certificate issued by the Certification Service Provider which has been verified by the Certification Service Provider.

3.2.5 Validation of Authority

<not SIG: The identity of the natural person representing the legal person shall be verified according to the requirements of Section 3.2.3 before issuing an Organizational Certificate. >

The right of representation of the natural person shall be verified.

Persons entitled to act on behalf of an Organization:

- a person authorized to represent the given Organization
- a person who is mandated for that purpose by an authorized person to represent the Organization
- an Organizational Administrator appointed by an authorized person to represent the Organization.

The Organizational Administrator can be appointed during Certificate Application, or anytime later with the help of the corresponding form. The identifier information of the designated person(s) shall be given on the form, by which he/she can be identified in later litigation. The form shall be signed (manually or by creating a qualified electronic signature based on a non pseudonymous Certificate) by the representative of the Organization, which is verified by the registration associate of the Certification Service Provider when received.

Appointing an Organizational Administrator is not mandatory, and multiple Organizational Administrators can be appointed too. If there is no appointed Organizational Administrator, then the person entitled to represent the Organization can perform this task.

<TLS:

[[QUA:

The Certification Service Provider maintains a list of the natural persons who are allowed to issue a Certificate Application behalf of the Organization.

The Certification Service Provider provides an Organization with a list of its authorized Organizational Administrators upon the Organization's verified written request.

]]

>

3.2.6 Criteria for Interoperation

The Certification Service Provider does not work together with other Certification Authorities during the provision of the service.

3.2.7 Email address validation

<not TLS:

This section defines the used processes and procedures for confirming the Applicant's control of Mailbox Addresses to be included in issued Certificates.

The Certification Service Provider verifies that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf.

The Certification Service Provider never delegates the verification of mailbox authorization or control.

The Certification Service Provider maintains a record of which validation method was used to validate every domain or email address in issued Certificates, including the relevant version number from the S/MIME Baseline Requirements [62] or TLS Baseline Requirements [63].

Completed validations of Applicant's authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation shall have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.

Validating control over mailbox via domain

The Certification Service Provider may confirm that the Applicant has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate.

The Certification Service Provider uses only the following approved methods in Section 3.2.2.4 of the TLS Baseline Requirements [63] to perform this verification:

- DNS Change (BR 3.2.2.4.7)
- Agreed-Upon Change to Website v2 (BR 3.2.2.4.18)
- Agreed-Upon Change to Website - ACME (BR 3.2.2.4.19)

Validating control over mailbox via email

>

For applications submitted on the Certification Service Provider's web site, the Certification Service Provider validates the Applicant's email address by verifying the email address before completing the Certificate Application form. The web page asks for the Applicant's email address before filling in the form and does not allow other details to be filled in. The Certification Service Provider will send a unique URL with a limited validity period, including a unique random number, to the email address provided.

The information required for validation will only be sent to the email address to be validated, it will not be shared in any other way.

The Applicant can only complete the form by clicking on the unique link provided.

Each incoming Certificate Application therefore has an email address that is verified during operation.

In the case of a Certificate Application submitted otherwise, the Certification Service Provider sends an email with a unique URL with a limited validity period, including a unique random number, to the email address to be verified.

The information required for validation will only be sent to the email address to be validated, it will not be shared in any other way.

Applicant shall respond and confirm the request by clicking on the unique link provided.

The random number is valid for no more than 24 hours from its generation.

The random value exhibits at least 112 bits of entropy.

3.3 Identification and Authentication for Re-key Requests

Re-key is the process when the Certification Service Provider issues a Certificate to a Subject with a replaced public key. Re-key can only be requested during the validity period of the service agreement.

In case of a re-key request, the Certification Service Provider verifies the existence and checks the validity of the affected Certificate.

The Certification Service Provider accepts re-key requests in case of valid and not valid <TLS: (revoked or expired)> <not TLS: (suspended, revoked or expired)> Certificates too.

Details related to the re-key process can be read in section 4.7.

3.3.1 Identification and Authentication for valid Certificate

The identification of the Subject or Applicant takes place as described in section 3.2.3.

When the expiry date of the new Certificate is not later than the Certificate to be re-keyed, the Certification Service Provider re-uses the results and evidences collected during the original validation process.

3.3.2 Identification and Authentication for invalid Certificate

The Certification Service Provider accepts re-key requests – only during the validity period of the service agreement– in case of Certificates <not TLS: suspended, > revoked or expired.

The identification of the Subject or Applicant takes place as described in section 3.2.3.

3.4 Identification and Authentication in Case of Certificate Renewal Requests

Certificate renewal is the process when the Certification Service Provider issues a certificate with unchanged Subject identification information but for new validity period to a Subject. Certificate renewal can only be requested during the validity period of the service agreement and for valid Certificates.

3.4.1 Identification and Authentication in Case of a Valid Certificate

The identification of the Subject or Applicant takes place as described in section 3.2.3.

In case of Certificate renewal initiated by the Certification Service Provider, the Certification Service Provider may re-use the results and evidences collected during the original validation process, when the expiry date of the new Certificate is not later than the Certificate to be re-newed.

3.4.2 Identification and Authentication in Case of an Invalid Certificate

Invalid Certificate can't be renewed.

3.5 Identification and Authentication for Certificate Modification requests

Certificate modification is the process, when the Certification Service Provider issues a new Certificate to the same Subject with an unchanged public key, but with different Subject identification data.

3.5.1 Identification and Authentication in Case of a Valid Certificate

The identification of the Subject or Applicant takes place as described in section 3.2.3.

If the modified Certificate expires on the same time as the original Certificate, during the procedure, the Certification Service Provider may use the results of inspections performed prior to the issuance of the original Certificate.

3.5.2 Identification and Authentication in Case of an Invalid Certificate

Invalid Certificate can't be renewed.

3.6 Identification and Authentication for <not TLS: Suspension and> Revocation Request

The Certification Service Provider receives and processes the requests related to the <not TLS: suspension and> revocation of the Certificates, and the announcements (for example related to the private key compromise or to the improper use of the Certificate) concerning the revocation of the Certificates.

The Certification Service Provider ensures that the requests only get accepted from authorized parties besides the rapid processing of the <not TLS: suspension and> revocation requests.

In each case, the Certification Service Provider verifies the authenticity of the submitted request and the eligibility of the person submitting the request.

The identification and authentication aspects of such requests are described in section 4.9.

<TLS:

In case of Website Authentication Certificates, suspension is not possible.

>

3.7 Verified Method of Communication

To assist in securely communicating with the Applicant <TLS: and confirming that the Applicant is aware of and approves issuance,> the Certification Service Provider verifies an email address, telephone number, fax number or postal delivery address as a "Verified Method of Communication" with the Applicant.

To verify a "Verified Method of Communication" with the Applicant, the Certification Service Provider

- verifies that the "Verified Method of Communication" belongs to the Applicant based on
  - records provided by the applicable Telecommunication Service Provider in case of telephone number or fax number
  - a Qualified Government Information Source
  - a Verified Professional Letter issued by a public notary
  - based on the identity validation of the Subject or Applicant.
- confirms the "Verified Method of Communication". The registration officer of the Certification Service Provider contacts the Applicant by using the "Verified Method of Communication". The reliability of the "Verified Method of Communication" is proved by physical presence of the Applicant or by using a "Communication Channel Verification Password".

<TLS:

[[QUA:

3.8 Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and the EV Certificate Request shall be signed. The Subscriber Agreement shall be signed by the authorized representative of the Subscriber. The EV Certificate Request shall be signed by the Applicant. In all cases, applicable signatures shall be legally valid that binds the Subscriber to the terms of each respective document:

- **for paper based documents handwritten signature and company seal if needed according to the registered signature method in the company register**
- **for electronic documents an eIDAS compliant qualified signature**

During the signature validation the Certification Service Provider authenticates each signature in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

The Certification Service Provider authenticates each signature by using one of the following methods:

- **in case of paper documents the Applicant creates the handwritten signature in the presence of the registration officer of the Certification Service Provider after the successful natural person identity validation made by the registration officer**
- **the eIDAS conformant valid qualified electronic signatures are accepted by the Certification Service Provider as authentic**
- **in case of Notarization by a notary the Certification Service Provider verifies by using an authentic information source that such notary is a legally qualified notary in the jurisdiction of the Signatory and confirms by contacting the notary that the document really issued by the notary**
- **The registration officer of the Certification Service Provider contacts the Applicant or Subscriber using a Verified Method of Communication, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant or Subscriber**

]]

>

4 Certificate Life-Cycle Operational Requirements

The issuance of a new Certificate for a new Subject shall precede the transmission of the Registration Application required to the Certification Service Provider and signing of the service agreement on the Subscriber's part as well as signing of the Certificate Application of the Subject or Applicant's part.

Certificate replacement is the process, when previously registered (and during that, identified) Subject requests a new Certificate instead of the existing one (issued pursuant to a valid service agreement).

Certificate replacement can take place for the below reasons:

- *Certificate renewal* means requesting a Certificate with the same data indicated in it as in the previous one by the Subject and both Certificates are issued for the same public key. The details of *Certificate renewal* are discussed in section 4.6.
- *Certificate modification* means requesting the modification of the Subject's Certificate considering the change of the Subject's data included in the Certificate. The Certification Service Provider receives *Certificate modification* requests during the validity period of the Certificate. Over the course of Certificate modification, the new Certificate is issued to the same public key. The details of *Certificate modification* are described in section 4.8.
- *Re-key* means a new Certificate issuance by the Certification Service Provider for a new public key at the request of the Subject during the Certificate's validity period or after expiration. The details of *Certificate renewal* are discussed in section 4.7.

When Clients – with a valid service agreement– request a new Certificate, then the modification of the service agreement is necessary.

The status of a Certificate can be valid, <not TLS: suspended, > revoked or expired. Regulations related to the status changes are discussed in section 4.9, and the Certificate status service is discussed in section 4.10.

The Certification Service Provider provides Certificate maintenance only under the force of the related service agreement. The requirements related to the termination of service agreement are discussed in section 4.11.

<TLS:

In order to facilitate and speed up the performance of tasks related to the management of Certificates, and to reduce errors, the Certification Service Provider supports the use of the Automatic Certificate Management Environment Protocol (ACME) according to RFC 8555 [55]. The ACME service operated by the Certification Service Provider is available 24 hours a day at the following address:

`https://acme.e-szigno.hu/acme/directory`

The ACME server supports the following features:

- newAccount
- newNonce
- newOrder
- keyChange
- revokeCert

>

4.1 Application for a Certificate

For each new Certificate issuance, Certificate Application submission is required. Prior to submitting the first Certificate Application, the Subject or Applicant shall submit a Registration Application to the Certification Service Provider, this can be done via the website of the Certification Service Provider, for instance. The Subject or Applicant shall specify their data to be indicated in the Certificate and shall specify what kind of Certificate they request, and they shall authorize the Certification Service Provider for the management of their personal data in the Registration request.

The Certification Service Provider doesn't consider the data indicated in the Registration Application authentic until the Subject or Applicant confirms them in a Certificate Application.

In case the conclusion of a new service agreement is necessary, the Certification Service Provider prepares the Subscriber's service agreement based on the information given in the Registration Application.

The service agreement shall contain the types of Certificates available for specific Subjects in the frame of the services within the confines of the Agreement.

A new Certificate can be requested within the confines of a previously concluded service agreement. If the Certificate (Certificate replacement) is issued as a replacement of a Certificate indicated in the service agreement, it is not necessary to modify the service agreement. If the Client requests a new Certificate in addition to the extant ones, the service agreement shall be modified.

The Certification Service Provider informs the Subscriber about the Certificate usage terms and conditions prior to the conclusion of the contract.

If the Subject or Applicant is not the same as the Subscriber, then the aforementioned information is also given to the Subject or Applicant.

The Certification Service Provider publishes the documents containing the information in an intelligible form, in an electronically downloadable form via its website, and upon request makes it available at the customer service office for on-site reading. At the Customer Service Office, the Client has the opportunity to read the documents and consult.

In the Certificate Application the Subject shall at least include the data below:

<TLS:

- data to be indicated in the Certificate (for example domain name, *[[ADV: IP address,]]* name of Organization, city, country)

>

<ALA:

- data to be indicated in the Certificate (for example name, title, name of Organization, name of organizational unit, city, country, email address)

>

<BEL:

- data to be indicated in the Certificate (for example name of Organization name of organizational unit, city, country, email address)

>
<UNI:

- data to be indicated in the Certificate (for example name, title, name of Organization, name of organizational unit, city, country, email address)

>

- the personal identification information of the
  <TLS: Applicant >
  <BEL: person entitled to represent the Subject >
  <ALA: Subject – in case of an Organization the Organization representative –>
  <UNI: Subject – in case of an Organization the Organization representative –>
  (full name, number of the identity document, mother's name, date and time of birth)
- the contact of the
  <TLS: Applicant >
  <BEL: person entitled to represent the Subject >
  <ALA: Subject – in case of an Organization the Organization representative –>
  <UNI: Subject – in case of an Organization the Organization representative –>
  (telephone number, email address)

<not SEA:

- in case of Organizational Certificate application, the data of the Organization (official name, domicile, optionally: identification data, denomination ot the organization department)

>

- the Subscriber's data (billing information)

In conjunction with the Certificate Application the Certification Service Provider ask for and check at least the following documents, certifications, procurations and declarations (in case of remote identification the copies of these):

- documents necessary to identify the
  <TLS: Applicant >
  <BEL: person entitled to represent the Subject >
  <ALA: Subject – in case of an Organization the Organization representative –>
  <UNI: Subject – in case of an Organization the Organization representative –>
  according to Section 3.2.3
- <not SEA: in case of Organizational Certificate application,> the documents for the identification of the Organization according to Section 3.2.2

<TLS:

- in case of Organizational Certificate application, the evidence issued by the Organization that the Subject or Applicant is entitled for representing the Organization according to section 3.2.5

>
<not TLS:

- <not SEA: if the Subject is an Organization, then> the certification or procuration delivered by the Organization, that the Subject or Applicant is entitled to represent the Organization according to section 3.2.5

<not SEA:

- if the Subject is a natural person requesting the indication of belonging to an Organization, then the evidence of the consent of the Organization, to that according to section 3.2.2

> >

4.1.1 Who May Submit a Certificate Application

Certificate Application may only be submitted by natural persons, to request a Certificate <TLS: for the organization represented. > <ALA: **[[QUA: for themselves.]]** *[[ADV: for themselves or for other employees of the organization represented.]]* > <BEL: for the organization represented.> <UNI: *[[ADV: for themselves, for other employees of the organization represented or for the organization represented.]]* >

In case of Organizational Certificate representatives may only be natural persons according to section 3.2.5. Certificate Application submitted by any other person is automatically rejected.

The precondition of Certificate issuance is a valid service agreement (signed by the Subscriber and the Certification Service Provider) concerning Certificate issuance and maintenance.

<TLS: The Applicant >

<ALA: The Subject – in case of an Organization the Organization representative –>

<BEL: The person entitled to represent the Subject >

<UNI: The Subject – in case of an Organization the Organization representative –>

may submit the Certificate Application in the following ways:

- on paper signed manually at the customer service of the Certification Service Provider or at the mobile registration associate of the Certification Service Provider, on a date previously agreed **[[QUA: (in this case,]]** *[[ADV: (in case of Certificates belonging to the III. certification class,]]* the personal identification takes place this time)
- on paper signed manually and sent to the customer service of the Certification Service Provider

  [[QUA:

  (in this case, the personal identification will take place another time)

]]

[[ADV:

(then, in case of Certificates belonging to the III. certification class the personal identification will take place another time)

]]

- in electronic form with an electronic signature <not SIG: or electronic seal> based on a non-pseudonymous **[[QUA: qualified]]** Certificate *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3)]]* and <not TLS:

  [[QUA:

  – sent through the Organizational Administrator's e-Szignó Account, or

  ]]

  >

  – sent to the Certification Service Provider's `info@e-szigno.hu` email address.

<TLS: The Subscriber and the Applicant >

<ALA: The Subscriber and the Subject – in case of an Organization the Organization representative –>

<BEL: The Subscriber and the person entitled to represent the Subject >

<UNI: The Subscriber and the Subject – in case of an Organization the Organization representative –>

shall provide their contact information during the Registration Application.

4.1.2 Enrolment Process and Responsibilities

During the process of the application the Certification Service Provider ascertains the identity of the person submitting the Certificate Application (see section 3.2.3).

<TLS:

The Certification Service Provider verifies that the Certificate Application was really sent by that person whose data (personal ID documents) is in the Certificate Application through a different – reliable – communication channel.

>

In case of Organizational Certificate application, the Certification Service Provider identifies the Organization (see section: 3.2.2) and it ensures, that the Subject or Applicant is entitled to represent the Organization (see section: 3.2.5) and to request a Certificate related to the Organization (see section: 3.2.2).

<not TLS:

The Subscriber determines which Subject or Applicant is entitled to request a Certificate according to which Certificate Policy.

>

The Applicant shall provide all the necessary information for the conduct of the identification processes.

If it is necessary, the Certification Service Provider performs data reconciliation with authentic government registers <TLS: **[[QUA: (QGIS)]]** > such as the personal data and address register or the company register). In case of a database if it can be arranged, the Certification Service Provider performs the data reconciliation electronically.

During the process the Certification Service Provider specifies the unique name of the Subject and assigns a globally unique ID (OID) to the Subject. This happens as defined in section 3.1.

The Certification Service Provider registers all the necessary information on the identity of the Subject or Applicant and the Organization for the provision of service and for keeping contact.

The Certification Service Provider registers the service agreement signed beforehand by the Subscriber that shall contain the Subscriber's statement that the Subscriber is aware of its obligations and undertakes the compliance.

The Certification Service Provider registers the Certificate Application signed by the Applicant which shall contain the following:

- a confirmation, that the data provided in the Certificate Application are accurate
- a consent, that the Certification Service Provider records and processes the data provided in the application

<TLS:

- the consent about the disclosure of the PreCertificate

>

- the declaration whether it consents to the disclosure of the Certificate

The Certification Service Provider keeps the aforementioned records for the time period required by law.

The Certification Service Provider archives the contracts, the Certificate Application form and every attestation that the <not SEA: Represented Organization, the> Subject or Applicant or the Subscriber handed in.

<TLS: If the identity of the Applicant or in case of an Organizational Certificate the identity of the Organization >

<ALA: If the identity of the Subject – in case of an Organization, its representative – or in case of an Organizational Certificate the identity of the Organization, or in case of an Organizational Certificate issued to a natural person , the Subject's inherency to the Represented Organization >

<BEL: If the identity of the person entitled to represent the Subject or the identity of the Organization >

<UNI: If the identity of the Subject – in case of an Organization, its representative – or in case of an Organizational Certificate the identity of the Organization, or in case of an Organizational Certificate issued to a natural person , the Subject's inherency to the Represented Organization > can not be verified without a doubt or any of the indicated data in the Certificate Application is incorrect, then the Certification Service Provider gives the Client the opportunity to correct the missing or incorrect data, and to provide the missing attestations within 3 months from the submission of the Certificate Application according to its inner regulations.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Certification Service Provider identifies the Subject or Applicant according to Section 3.2, and it verifies the authenticity of the request.

<not SEA: In case of requesting an Organizational Certificate, the Organization is going to be identified too, and the verification of the privileges takes place according to section 3.2. The Certification Service Provider registers all the information used by the Subject or in case of an Organizational Certificate the Organization to certify its identity, including the registration number of the documentation used for the certification and the incidental limitations related to its validity. > <BEL: The Certification Service Provider identifies the Organization too, and verifies the eligibility according to section 3.2. The Certification Service Provider registers all the information used by the Organization to certify its identity, including the registration number of the documentation used for certification and the incidental limitations related to its validity. >

The Certification Service Provider may use the original authentic documents in its possession or the authentic electronic copies made of them during the validation until the validity period indicated on the document or until the given document is invalidated in some other way.

The Certification Service Provider may use the documents and data provided in Section 3.2 to verify certificate information or may reuse previous validations themselves for no more than <TLS: 398 days.> <not TLS: 3 months.>

<TLS:

For domain validations as described in section 3.2.2.4, the domain validation data is valid for 30 days.

>

[[QUA:

<not UNI: <not TLS: A different rule applies to the validity period of the validation result of the email address included in the Email (S/MIME) Certificate, which is:

- **30 days in case of individual email-based validation**
- **398 days in case of validation of control over the domain**

>>

]]

<UNI:

A different rule applies to the validity period of the validation result of the email address included in the Email (S/MIME) Certificate, which is:

- 30 days in case of individual email-based validation
- 398 days in case of validation of control over the domain

>

<TLS:

The Certification Service Provider maintains a list of the High Risk Certificate Requests which contains the rejected Certificate Applications and all the Certificates revoked due to any security issue.

Prior to the Certificate's approval the Certification Service Provider checks this list. If any of the requested domain, the Subscriber or the Applicant is included in the list, the Certification Service Provider handles the request with high priority to ensure that such requests are properly verified.

[[QUA:

In case of EVCP Certificate:

The Certification Service Provider verifies whether

- **any of the Subscriber or the Applicant is identified on any government denied list or list of prohibited persons,**
- **is the Organization registered or making business in any country where doing business is prohibited.**

The Certification Service Provider will not issue the requested Certificate, if anything was included on any such list.

]]

>

4.2.2 Approval or Rejection of Certificate Applications

To avoid any conflicts of interests, the Certification Service Provider ensures its personal and operational independence contrary to the Subscribers. It does not constitute a breach of conflicts of interests, if the Certification Service Provider issues Certificates for its associates.

The Certification Service Provider verifies the authenticity of all the information given in the Certificate Application to be indicated on the Certificate before issuing the Certificate.

<not TLS:

If the Subject requests a Certificate containing an email address, the Certification Service Provider verifies the email address to be indicated in the Certificate. It ascertains that the email address exists and verifies that it is the Subject's email address indeed.

>

After processing the Certificate Application, the Certification Service Provider accepts or rejects the Certificate Application.

<TLS:

If the identity of the natural person or the organization which is to be identified, or in case of a personal Certificate, or any of the indicated data on the Certificate Application form is incorrect and is not corrected by the Client upon request of the Certification Service Provider, then the Certification Service Provider rejects the application.

>

<ALA: If the identity of the natural person or the organization which is to be identified, or in case of a personal Certificate, the Subject's inherency to the Represented Organization can not be verified without a doubt or any of the indicated data on the Certificate Application form is

incorrect, and the Client did not correct it for the request of the Certification Service Provider, then the Certification Service Provider rejects the application. >

<BEL:

If the identity of the natural person or the organization can not be verified without a doubt, or any of the indicated data in the Certificate Application form is incorrect, and is not corrected by the Client upon request of the Certification Service Provider, then the Certification Service Provider rejects the application.

>

<UNI: If the identity of the natural person or the organization which is to be identified, or in case of a personal Certificate, the Subject's inherency to the Represented Organization can not be verified without a doubt or any of the indicated data on the Certificate Application form is incorrect, and the Client did not correct it for the request of the Certification Service Provider, then the Certification Service Provider rejects the application. >

In case of rejection of the Certificate Application, the Certification Service Provider informs the Subject or Applicant and the Subscriber about the fact of the rejection, but the Certification Service Provider is not obliged to justify its decision.

[[ADV:

<UNI:

Managing High-Risk Certificates

The Certification Service Provider maintains a register of high-risk Code Signing Certificates and the natural and legal persons who may be associated with them, in accordance with the requirements of the CA/Browser Forum.

The Certification Service Provider shall register the data to be registered, if

- *rejects a submitted Certificate Application due to security concerns,*
- *a valid Code Signing Certificate must be revoked due to a security incident,*

The Certification Service Provider shall exercise extreme caution when assessing new Certificate Application submitted by natural or legal persons included in the register.

The Certification Service Provider issues Code Signing Certificate only on cryptographic hardware devices which have proper certification.

If a Client requests the revocation of the Code Signing Certificate for the second time due to a key compromise, no further Code Signing Certificate may be issued to the Subject.

>

]]

<not TLS:

4.2.2.1 CAA records

As part of the issuance process, the Certification Service Provider retrieves and processes CAA records in accordance with IETF RFC 9495 [57] for each Email Address in the Email (S/MIME) Certificate to be issued.

The Certification Service Provider will only issue the requested Email (S/MIME) Certificate if the following conditions are independently met for each Email Address in the Email (S/MIME) Certificate to be issued:

- the first filled CAA record
  - does not contain an entry 'issuemail', or
  - contains the entry 'issuemail "e-szigno.hu"'
- there is now filled CAA record in the chain

The presence of other known Property Tags, such as 'issue' or 'issuewild', does not restrict the issuance of Email (S/MIME) Certificates. The Certification Service Provider does not issue a Email (S/MIME) Certificate if it encounters an unrecognized property tag with critical flag set.

In case of any CAA authorization issue is detected, the Certification Service Provider attempts to contact the Applicant using the trusted communication channel verified earlier, or the contact details stipulated in the CAA 'iodef' property tag, if present, to resolve the issue. The Certification Service Provider only supports the "mailto:" URL scheme in the 'iodef' record.

The Certification Service Provider documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances.

In any case, right before issuing the Email (S/MIME) Certificate, the Certification Service Provider automatically rechecks the CAA records.

4.2.2.1.1 DNSSEC validation of CAA records

DNSSEC validation back to the IANA DNSSEC root trust anchor will be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective will :

- perform DNSSEC validation using the algorithm defined in RFC 4035 [43] Section 5, and
- support NSEC3 as defined in RFC 5155 [47], and
- support SHA-2 as defined in RFC 4509 [45] and RFC 5702 [49], and
- properly handle the security concerns enumerated in RFC 6840 [52] Section 4.

The Certification Service Provider will not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor may be performed on all DNS queries associated with the validation of domain authorization or control by Remote Network Perspectives used for Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

4.2.2.2 Multi-perspective issuance corroboration

When issuing Email (S/MIME) Certificates, the Certification Service Provider uses Multi-perspective issuance corroboration according to CABF TLS Baseline Requirements [63] chapter 3.2.2.9 to verify CAA records and domain control in order to increase the reliability of validation.
>

4.2.3 Time to Process Certificate Applications

The Certification Service Provider undertakes the processing of the Certificate Application within 5 workdays if all the necessary data and document is available.

4.3 Certificate Issuance

[[QUA:

The Certification Service Provider only issues the Certificate to the Subject in case of the acceptance of the Certificate Application.

]]

[[ADV:

In case of certificates belonging to the III. certification class, the Certification Service Provider only issues the Certificate to the Subject in case of the acceptance of the Certificate Application.

]]

The issued Certificate only contains the data that was indicated in the Certificate Application and that was verified by the Certification Service Provider during the evaluation process.

<not TLS:

If the the Certification Service Provider provides the personal Qualified Electronic Signature or Seal Creation Device to the Subject, as a part of the personalization process, the Certification Service Provider generates the Subject or Applicant's keypairs, but the Certificate's will not be issued. The handover of the Qualified Electronic Signature or Seal Creation Device containing the private key takes place in a controlled environment in accordance with the security regulations defined in section 6.1.2.

- If the identity validation related to the Certificate application takes place during a personal face to face meeting, during the personal meeting, the employee of the Certification Service Provider provides the Subject or Applicant with the Qualified Electronic Signature or Seal Creation Device containing the Subject's private key.

  The Subject or Applicant confirms receipt of the Qualified Electronic Signature or Seal Creation Device by signing a receipt declaration.

- In other cases, after carrying out the personal identity validation, the Certification Service Provider delivers the Qualified Electronic Signature or Seal Creation Device containing the Subject's private key to the Subject or Applicant via a reliable channel.

  The Subject or Applicant may receive his device after personal identification, during which he must identify himself with a personal identification card. The transferring party checks whether the Subject or Applicant's face image corresponds to the face image on his identity

card and whether the Subject or Applicant's signature corresponds to his signature on his identity card.

The Subject or Applicant certifies the receipt of the Qualified Electronic Signature or Seal Creation Device by signing a declaration of receipt, which the transferor returns to the the Certification Service Provider.

The Certification Service Provider will issue the requested Certificate to the Subject or Applicant only if it is reliably ascertained that the Qualified Electronic Signature or Seal Creation Device is already in the Subject or Applicant's possession.

Following the issuance of the Certificate, the Certification Service Provider places the activation code in encoded form in the Subject or Applicant's e-Szignó Account account, which is required to activate the Qualified Electronic Signature or Seal Creation Device. The activation code is generated in accordance with chapter 6.4. The Subject or Applicant can decrypt the activation code by re-entering the e-Szignó Account's access code.

[[QUA:

If the Subject's private key is managed by a Remote Key Management Service Provider, the Certification Service Provider will also send the issued Certificate directly to the trust service provider managing the key.

]]

>

[[ADV:

In case of Certificates belonging to the II. certification class, the Certification Service Provider only issues the Certificate to the Subject after verifying the data given in the Registration Application and receiving the signed Certificate Application and service agreement. The issued Certificate only contains that Subject data, that was given in the Registration Application, and that the Certification Service Provider verified during the evaluation.

]]

4.3.1 CA Actions During Certificate Issuance

Certificates are issued according to strictly regulated and controlled processes, the details of which are set out in the internal policies and regulations of the Certification Service Provider.

[[QUA:

<TLS:

In case of EVCP Certificate, the Certification Service Provider guarantees by the proper usage of the trusted roles and the internal administrative processes that during the Certificate issuance process at least two employees needed by proper trusted roles. Recording and verification the authenticity of the data included in the Certificate shall not be performed by the same person.

>

<not TLS:

The Certification Service Provider has developed its internal administrative processes by analyzing the risks, and uses automated validation tools when recording the data included in the Certificate and verifying the authenticity of the data.

>

]]

[[ADV:

The Certification Service Provider has developed its internal administrative processes by analyzing the risks and uses automated validation tools when recording the data included in the Certificate and verifying the authenticity of the data.

]]

Pre-issuance linting

<not TLS:

In order to prevent the issuance of faulty Email (S/MIME) Certificates, the Certification Service Provider introduced pre-issuance testing of Email (S/MIME) Certificates, during which it validates the content to be signed using automatic verification tools (certlint and its own tools) as follows:

>

<TLS:

In order to prevent the issuance of incorrect Certificates, the Certification Service Provider validates the content to be signed using automatic verification tools (certlint, zlint and its own tools) before issuing the PreCertificate, as follows:

>

- issues the test Certificate, which is signed with a provider key whose self-signed Certificate cannot be traced back to any publicly trusted CA Certificate
- the issued test Certificate is validated by automatic tools
  - In case of any "ERROR" message the Certification Service Provider suspends the issuance of the <TLS: PreCertificate > <not TLS: Email (S/MIME) Certificate > and starts an investigation to analyze the problem
    - in case of really faulty test Certificate
      - the issuance process is terminated
      - the Certification Service Provider starts an investigation to find the source of the problem
    - in case of false alarm
      - the Certification Service Provider continues the issuance of the <TLS: PreCertificate > <not TLS: Email (S/MIME) Certificate > according to the normal process
      - the Certification Service Provider upgrades the configuration of the automated tools
      - the Certification Service Provider informs the developer of the tool about the potential problem
  - In the case of a test Certificate that has successfully passed the verification, the Certification Service Provider will continue the normal process by issuing the <TLS: PreCertificate > <not TLS: Email (S/MIME) Certificate >

<TLS: The issued PreCertificate is added immediately - with a technical processing delay not longer than 15 minutes - to the internal Certificate Repository of the Certification Service Provider. From this time, it can be revoked, the revocation status information will be available through the OCSP and CRL services of the Certification Service Provider. >

<TLS:

The Certification Service Provider publishes the PreCertificate corresponding to the Certificate through the CT Log providers listed on the web page of the Certification Service Provider and puts the digitally signed SCT(s) sent by the CT Log provider(s) into the Certificate to be issued.

>

The issued Certificate is added immediately to the internal Certificate Repository of the Certification Service Provider From this time it can be <not TLS: suspended and> revoked, the revocation status information will be available through the OCSP and CRL services of the Certification Service Provider.

<TLS: The issued Certificate is added immediately to at least one CT Log usable in Chrome at the time of issuance. >

Post-issuance linting

The Certification Service Provider verifies the issued Certificate by using automated <TLS: tools (certlint, zlint).> <not TLS: tool (certlint).>

- In case of any "ERROR" message the Certification Service Provider suspends the publication of the Certificate and starts an investigation to analyze the problem
  - in case of really faulty Certificate
    - the Certification Service Provider terminates the issuance and the Certificate will not be published
    - the Certification Service Provider starts an investigation to find the source of the problem
  - in case of false alarm
    - the Certification Service Provider continues the publication of the Certificate according to the normal process
    - the Certification Service Provider upgrades the configuration of the automated tools
    - the Certification Service Provider informs the developer of the tool about the potential problem
- the Certificate which successfully passed the automated test will be published according to the process described in section 4.3.2.

The beginning of the validity period of the Certificate shall not be earlier than the real issuance time of the Certificate.

The Certification Service Provider never backdates Certificates.

4.3.2 Notification of the Subscriber about the Issuance of the Certificate

The Certification Authority informs the Subject or Applicant and the Subscriber on the issuance of the Certificate and enables the Subject or Applicant to receive the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

[[ADV: In case of Certificates belonging to the III. certification class]] **[[QUA: The]]** <TLS: Applicant > <ALA: Subject > <BEL: person entitled to represent the Subject > <UNI: Subject – in case of a certificate issued to an Organization, the representative of the Subject – > shall verify the accuracy of the data indicated in the Certificate during the takeover of the Certificate.

[[ADV:

In the case of Certificates belonging to the II. certification class, the Subject or Applicant (or its representative) verifies the correctness of the data included in the Certificate. By signing the service agreement, the Subscriber also confirms acceptance of the Certificate Policy the Certification Practice Statement and other documents containing the terms and conditions of the agreement.

]]

The Subject or Applicant accepts the Certificate by using the Certificate, no separate declaration is required.

4.4.2 Publication of the Certificate by the CA

After the issuance of the Certificate, in case of the Subject or Applicant's prior consent, the Certification Service Provider discloses the Certificate in its public Certificate Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

<not SEA:

<TLS: In case of an Organizational Certificate,> <ALA: If the Certificate was issued for the Subject to create electronic signature behalf of an Organization,> <UNI: In case of an Organizational Certificate,> the contact person of the Represented Organization is notified by the Certification Service Provider on the Certificate issuance without delay.

>

<BEL:

The person entitled to represent the Subject is notified by the Certification Service Provider without delay about the issuance of the Certificate.

>

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

<TLS:

The private key belonging to the Website Authentication Certificate shall only be used for website or - if the Website Authentication Certificate makes it possible - client authentication, and any other usage is prohibited.

A private key corresponding to an expired or revoked Certificate can not be used.

>

<ALA:

The Subject shall only use its private key corresponding to the Certificate for electronic signature creation, and any other usage (for example, authorization and encryption) is prohibited.

A private key corresponding to an expired, revoked, or suspended Certificate shall not be used for electronic signature creation.

>

<BEL:

The Subject shall only use its private key corresponding to the Certificate for electronic seal creation, and any other usage is prohibited.

A private key corresponding to an expired, revoked, or suspended Certificate shall not be used for electronic seal creation.

>

<UNI:

The private key corresponding to the Certificate of the Subject can be only used according to the key usage (section 6.1.7) , of the Certificate, and any other usage is prohibited.

A private key corresponding to an expired, revoked, or suspended Certificate shall not be used.

>

The Subject is bound to ensure the adequate protection of the private key and the activation data. The limitations determined in Section 1.4 have to be followed during the usage.

4.5.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the Certification Service Provider, in the course of <TLS: performing the webserver authentication,> <ALA: accepting the electronic signature or seal verified,> <BEL: accepting the electronic signature or seal verified,> <UNI: performing tasks (e.g. identifying remote party, encrypt document for the recipient),> the Relying Party is recommended to proceed carefully, particularly regarding to the following:

- the Relying Party shall verify the validity and revocation status of the Certificate

<TLS:

- the public keys belonging to the Website Authentication Certificates shall only be used for website or - if the Website Authentication Certificate makes it possible - client authentication

>

<ALA:

- Certificates for electronic signatures and the corresponding public keys shall only be used for electronic signature validation

>
<BEL:

- Certificates for electronic seals and the corresponding public keys shall only be used for electronic seal validation

>
<UNI:

- public keys shall only be accepted in such applications that are in line with the content of the „Key Usage" and "Extended Key Usage" fields of the Certificate

>

- the verifications related to the Certificate should be carried out for the entire certificate chain up to a trusted root or intermediate provider Certificate

[[QUA:

- **when building the certificate chain, accept a Trust Service Provider Certificate as a trusted issuer (trust anchor) that**
  - **is listed in a national Trusted List (which can be validated against the EU list of trusted lists, as for example the Hungarian Trusted List [75]) as a trust service entitled to issue qualified end-user Certificates**

  <not TLS:

  - **it is accompanied by a Service Provider Certificate that was valid at the time of creating the <ALA: signature> <BEL: seal> and at the time of issuing the end-user Certificate used to create the <ALA: signature> <BEL: seal>**

  >

]]
<ALA:

- the electronic signature or seal verification shall be performed with a reliable application, which complies with the related technical specifications, can be resiliently configured, and has been set correctly, and it runs within a virus-free environment
- in case of personal Certificates related to an organization, it is recommended to verify that the title of the Signatory by which it is entitled to sign the document can be identified by the certificate (for example indicated in the Title field)

>
<BEL:

- the electronic signature or seal verification shall be performed with a reliable application, which complies with the related technical specifications, can be resiliently configured, and has been set correctly, and it runs within a virus-free environment

>

- it is recommended to verify that the Certificate was issued according to the appropriate Certificate Policy

[[QUA:
<ALA:

- **when accepting a qualified electronic signature or seal it is recommended to verify that the Certificate was issued based on a Certificate Policy requiring Qualified Electronic Signature or Seal Creation Device**

>
<BEL:

- **when accepting a qualified electronic signature or seal it is recommended to verify that the Certificate was issued based on a Certificate Policy requiring Qualified Electronic Signature or Seal Creation Device**

>
]]
<ALA:

- if it is indicated in the Certificate, it is recommended to verify the highest value of the obligation undertaken at one time (the Certification Authority is not responsible for the claims arising from electronic documents issued and signed concerning transactions in excess of those limits and for the damage caused this way.)

>
<BEL:

- if it is indicated in the Certificate, it is recommended to verify the highest value of the obligation undertaken at one time (the Certification Authority is not responsible for the claims arising from electronic documents issued and sealed concerning transactions in excess of those limits and for the damage caused this way.)

>

- the Relying Party shall consider any restrictions indicated in the Certificate or in the regulations referenced in the Certificate

The Certification Service Provider makes available a service for its Clients and Relying Parties that they can use to verify the issued Certificates.

4.6 Certificate Renewal

The process when the Certification Service Provider issues a new Certificate for a new validity period for the same public key with unchanged Subject identity information is called Certificate renewal.

If the Subject would like to use the Certificate after the expiration, then it shall initiate the Certificate renewal. The Certificate renewal technically means the issuance of a new Certificate, with the same Subject identification data, but new validity period. Other data can change in the Certificate, like the CRL, OCSP references or the provider key used for signing the Certificate.

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is only permitted when all of the following conditions are met:

- the Certificate renewal request was submitted within the validity period of the Certificate
- the Certificate to be renewed is not <not TLS: suspended or > revoked
- the private key corresponding to the Certificate is not compromised
- the Subject identity information indicated in the Certificate is still valid.

The Certification Service Provider shall only accept a Certificate renewal application during the term of the service agreement.

If a previous Certificate of the Subject is revoked, then new Certificate can only be requested in the frame of *Re-key* (see section: 4.7) or new Certificate Application (see section: 4.1).

If any of the Subject data indicated in the Certificate changed, then new Certificate shall be requested within the framework of Certificate modification (see section 4.8).

During the *Certificate renewal*, the Subject or Applicant is informed if the terms and conditions have changed since the previous Certificate issuance.

If the Subject or Applicant is not the same as the Subscriber, then the information aforementioned is also provided to the Subscriber.

The Certificate renewal is performed within the framework of a valid service agreement, there is no need for its modification.

4.6.2 Who May Request Renewal

The Certificate renewal shall be initiated by a person behalf of the Client, who is entitled to submit an application for a new Certificate of the same type at the time of the submission of renewal application.

The applicant shall state in the Certificate renewal application, that the Subject identification data indicated in the Certificate are still valid.

The Certification Service Provider provides the following possibilities for the Clients to submit Certificate renewal application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate of the Subject or Applicant, *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3),]]* sent to the Certification Service Provider's `info@e-szigno.hu` email address.
- on paper signed manually at the customer service of the Certification Service Provider or at the mobile registration associate of the Certification Service Provider, on a date previously agreed. **[[QUA: The personal identification will take place during that time.]]** *[[ADV: In case of Certificates belonging to the III. certification class the personal identification will take place that time.]]*
- on paper signed manually and sent to the customer service of the Certification Service Provider. **[[QUA: (in this case, the personal identification will take place another time)]]** *[[ADV: (then, in case of Certificates belonging to the III. certification class the personal identification will take place another time)]]*

The Certification Service Provider is entitled to initiate the renewal of the Certificate if changes in the internal or external conditions of the provision of the service necessitate it, for example, but not exclusively in the following cases:

- due to changes in external requirements, the Certificate can no longer be used in its current form
- the Certification Service Provider becomes aware that the Certificate does not comply with the referred to Certificate Policy or Certification Practice Statement
- if the Certification Service Provider's signing key used to issue the Certificate shall be replaced urgently.

<not TLS:
[[ADV:
In order to ensure the continuity of the service, the Certification Service Provider is entitled to initiate the renewal of the Certificate during the last month of the Certificate's validity period, if:

- *the service agreement will still be valid on the calendar day following the validity period of the Certificate*
- *Subscriber has agreed in advance to the automatic renewal of the Certificate for the entire term of the service agreement.*

]]
>

4.6.3 Processing Certificate Renewal Requests

During the evaluation of the Certificate renewal application, the Certification Service Provider verifies that:

- the submitted Certificate renewal application is authentic

- the submitter of the Certificate renewal application has the appropriate entitlement and authorization
- the submitter of the Certificate renewal application stated that the data of the Subject to be indicated in the Certificate are unchanged and accurate
- the Certificate renewal application was submitted during the Certificate's validity period
- the Certificate to be renewed is not <not TLS: suspended or> revoked
- based on currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the Certificate to be issued.

The method used for identification and authentication during the Certificate renewal is stated in Section 3.4.

4.6.4 Notification of the Client about the New Certificate Issuance

The Certification Service Provider informs the Subject or Applicant and the Subscriber about the Certificate issuance.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

The renewed Certificate can be received (downloaded) without a personal meeting.

<not TLS: During the Certificate renewal process, there is no key generation, thus there is no need to handover key to the Subject.

If the private key of the Subject is on a personal Qualified Electronic Signature or Seal Creation Device which is physically hold by the Subject, then the Subject installs the Certificate to the device. The easiest way to do this is with a card management application provided by the Certification Service Provider, for which the Certification Service Provider provides written manuals, and if necessary, provides consultation possibility by telephone.

[[QUA:

If the Subject's private key is managed by a Remote Key Management Service Provider, the Certification Service Provider will also send the issued Certificate directly to the trust service provider managing the key.

]]

>

The Subject or Applicant accepts the Certificate by using the Certificate, no separate declaration is required.

4.6.6 Publication of the Renewed Certificate by the CA

The Certification Service Provider discloses the renewed Certificate <TLS: and the corresponding PreCertificate > the same way as the original Certificate.

4.6.7 Notification of Other Entities about the Certificate Issuance

In case of an Organizational Certificate the contact of the Represented Organization is notified by the Certification Service Provider on the Certificate issuance without delay.

4.7 Certificate Re-Key

Re-key means the process when the Certification Service Provider issues a new Certificate to the Subject in a manner that the public key is to be changed.

Further data may be optionally changed in the new Certificate issued during the *Re-key* process, for example validity period, the CRL and OCSP links or the provider key used to sign the Certificate.

4.7.1 Circumstances for Certificate Re-Key

The validity of the previous Certificate is not required for *Re-key*, but the Certification Service Provider shall only accept *Re-key* applications within the scope of the service agreement.

During the Certificate *Re-key*, the Subject or Applicant is informed by the Certification Service Provider if the terms and conditions have changed since the previous Certificate issuance. If the Subject or Applicant is not the same as the Subscriber, then the information aforementioned is also given to the Subscriber.

Certificate *Re-key* is performed within the framework of a valid service agreement, there is no need for its modification.

4.7.2 Who May Request Certification of a New Public Key

The Certificate *Re-key* shall be initiated by a person who would be entitled to submit a new Certificate Application at the time of the submission of the *Re-key* application.

The applicant shall state in the Certificate *Re-key* application, that the Subject identification data indicated in the Certificate are still valid, or they shall give the new data and make a statement of its validity.

The Certification Service Provider ensures the following possibilities for the Clients to submit Certificate re-key application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate of the Subject or Applicant, *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3),]]* sent to the Certification Service Provider's `info@e-szigno.hu` email address.

- on paper signed manually at the customer service of the Certification Service Provider or at the mobile registration associate of the Certification Service Provider, on a date previously agreed. **[[QUA: The personal identification will take place during that time.]]** *[[ADV: In case of Certificates belonging to the III. certification class the personal identification will take place that time.]]*

- on paper signed manually and sent to the customer service of the Certification Service Provider. **[[QUA: (in this case, the personal identification will take place another**

time)]] *[[ADV: (then, in case of Certificates belonging to the III. certification class the personal identification will take place another time)]]*

The Certification Service Provider may also initiate a *Re-key* in the following cases:

- the cryptographic key associated with the Certificate becomes vulnerable for any reason

[[QUA:
<not TLS:

- **the certification status of the Qualified Electronic Signature or Seal Creation Device managing the private key associated with the Certificate changes**

>
]]
In the event of a *Re-key* initiated by the Certification Service Provider, the new Certificate may be issued even without a Certificate Application submitted by the Subject or Applicant.

4.7.3 Processing Certificate Re-Key Requests

During the evaluation of the Certificate *Re-key* application the Certification Service Provider verifies that:

- the submitted application is authentic
- the submitter of the application has the appropriate entitlement and authorization
- the data indicated in the application are accurate
- based on the currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity of the Certificate to be issued.

Before processing the *Re-key* request the identity of the person submitting the Certificate *Re-key* application shall be verified according to section 3.3.

4.7.4 Notification of the Client about the New Certificate Issuance

The Certification Service Provider informs the Subject or Applicant and the Subscriber about the Certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

<TLS:
The Certification Service Provider hands over the Certificate issued for the new public key after the identification of the Subject or Applicant.
>
<not TLS:

If the Qualified Electronic Signature or Seal Creation Device in the possession of the Subject or Applicant still has a usable private key, then it is not necessary to issue a new key or Qualified Electronic Signature or Seal Creation Device, the Certification Service Provider will issue the Certificate for a new key.

If it is necessary to issue a new Qualified Electronic Signature or Seal Creation Device during the re-key process, the Certification Service Provider will personalize the new Qualified Electronic Signature or Seal Creation Device and deliver it to the Subject or Applicant as described in chapter 4.3. The Certification Service Provider issues only the requested Subject or Applicant's Certificates after verifying in a credible manner that the Qualified Electronic Signature or Seal Creation Device is already in the possession of the Subject or Applicant.

[[QUA:

If the Subject's private key is managed by a Remote Key Management Service Provider, the Certification Service Provider will also send the issued Certificate directly to the trust service provider managing the key.

]]

If the new key used during the *Re-key* was provided by the Subject, then there is no need for key and Qualified Electronic Signature or Seal Creation Device handover.

The new Certificate issued as part of the re-key can be received (downloaded) without the need for a face-to-face meeting.

The Subject or Applicant accepts the Certificate by using the Certificate, no separate declaration is required. >

4.7.6 Publication of the Re-Keyed Certificate

The Certification Service Provider discloses the renewed Certificate <TLS: and the corresponding PreCertificate > the same way as the original Certificate.

4.7.7 Notification of Other Entities about the Certificate Issuance

In case of an Organizational Certificate the contact of the Represented Organization is notified by the Certification Service Provider on the Certificate issuance without delay.

4.8 Certificate Modification

Certificate modification means the process when the Certification Service Provider issues a new Certificate for the Subject with changed Subject identity information but with unchanged public key.

The Certificate modification technically means new Certificate issuance. The Certification Service Provider is bound to revoke the previous Certificate, that contains invalid data (see section: 4.9).

Previous data can change in the new Certificate issued during the Certificate modification, such as the validity period, the CRL and OCSP references or the Certification Service Provider key used for Certificate signing.

4.8.1 Circumstances for Certificate Modification

Certificate modification becomes necessary in the following cases:

- change of data indicated in the Subject's Certificate
- in the Certificate issuing system of the Certification Service Provider any data of the Certificate issuer CA indicated in the "Subject DN" is changed, or its public key is changed and as a result of it, its provider Certificate is changed
- the Certificate profile determined by the Certification Service Provider is changed.

Requirements of Certificate modification:

- the Certificate modification application was submitted during the Certificate's validity period
- the Certificate to be modified is not <not TLS: suspended or> revoked
- the private key corresponding to the Certificate is not compromised.

The Certification Service Provider only accepts Certificate modification application in the scope of the Service Agreement.

If the previous Certificate of the Subject is revoked or expired, then the new Certificate can be requested within the framework of *Re-key* (see section: 4.7) or new Certificate Application (see section: 4.1).

During the Certificate modification, the Subject or Applicant is informed if the terms and conditions have changed since the previous Certificate issuance.

If the Subject or Applicant is not the same as the Subscriber, then the information aforementioned is also given to the Subscriber. The Certificate modification is performed within the framework of a valid service agreement, there is no need for its modification.

4.8.2 Who May Request Certificate Modification

The Certificate modification shall be initiated by a person who is entitled to submit a new Certificate Application at the time of the submission of the modification application.

In the Certificate modification request, the applicant shall give the new data and shall make a statement of their accuracy.

The Certification Service Provider initiates the Certificate modification if it becomes aware of that the Subject's data indicated in the Certificate is changed.

The Certification Service Provider ensures the following possibilities for the Clients to submit Certificate modification application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate of the Subject or Applicant, *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3),]]*
  - sent to the Certification Service Provider's `info@e-szigno.hu` email address, or
  - submitted on the Subject or Applicant's e-Szignó Account.

- on paper signed manually at the customer service of the Certification Service Provider or at the mobile registration associate of the Certification Service Provider, on a date previously agreed. **[[QUA: The personal identification will take place during that time.]]** *[[ADV: In case of Certificates belonging to the III. certification class the personal identification will take place that time.]]*
- on paper signed manually and sent to the customer service of the Certification Service Provider. **[[QUA: (in this case, the personal identification will take place another time)]]** *[[ADV: (then, in case of Certificates belonging to the III. certification class the personal identification will take place another time)]]*

The Certification Service Provider may also initiate a Certificate modification if changes in the internal or external circumstances of service provision make this necessary, for example, but not limited to, in the following cases:

- due to changes in external requirements, Certificate can no longer be used in its current form
- the Certification Service Provider becomes aware that the Certificate does not comply with the referenced Certificate Policy or Certification Practice Statement.

In the event of a Certificate modification initiated by the Certification Service Provider, the new Certificate may be issued even without a Certificate Application submitted by the Subject or Applicant.

4.8.3 Processing Certificate Modification Requests

During the evaluation of the submitted Certificate modification application, the Certification Service Provider verifies that:

- the submitted Certificate renewal application is authentic
- the submitter of the Certificate renewal application has the appropriate entitlement and authorization
- the data given in the application are accurate
- the Certificate renewal application was submitted during the Certificate's validity period
- based on the currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the Certificate to be issued.

The Certification Service Provider verifying the validity of the Subject's data proceeds the same as the initial verification performed before a new Certificate issuance.

Before the execution of the Certificate modification application, the applicant shall be identified according to section 3.5.

4.8.4 Notification of the Client about the New Certificate Issuance

The Certification Service Provider informs the Subject or Applicant and the Subscriber about the Certificate issuance.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

During Certificate modification, there is no new key generation, thus there is no need to handover key to the Subject. The modified Certificate can be received (downloadable) without personal encounter.

<not TLS:

If the private key of the Subject is on a personal Electronic Signature or Seal Creation Device which is physically hold by the Subject, then the Subject installs the Certificate to the device. For that purpose, the Certification Service Provider provides written manuals, and if necessary, provides consultation possibility by telephone.

[[QUA:

If the Subject's private key is managed by a Remote Key Management Service Provider, the Certification Service Provider will also send the issued Certificate directly to the trust service provider managing the key.

]]

>

The Subject accepts the Certificate by its usage, and there is no need for further statement.

4.8.6 Publication of the Modified Certificate by the CA

The Certification Service Provider discloses the renewed Certificate <TLS: and the corresponding PreCertificate > the same way as the original Certificate.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

In case of an Organizational Certificate the Organizational Administrator of the Represented Organization is notified by the Certification Service Provider on the Certificate issuance without delay.

4.9 Certificate Revocation and Suspension

The process when the Certification Service Provider terminates the validity of the Certificate before expiration is called Certificate revocation. The Certificate revocation is a permanent and irreversible status change, the revoked certificate will never be valid again.

<TLS:

The Website Authentication Certificate shall not be suspended.

>

<not TLS:

The process when the Certification Service Provider temporarily ceases the validity of the Certificate before expiration is called Certificate suspension. The Certificate suspension is a temporary state; the suspended Certificate can be revoked, or before the end of the validity, with the withdrawal of the suspension it can be made valid again. In case of the withdrawal of suspension the Certificate becomes valid retroactively, as if it has not been suspended.

>

Revocation Reason

The Certification Service Provider may store information on the reason for the revocation in the Certificate revocation status register, which it may disclose in the Certificate revocation status services.

When the Client initiates the revocation, the following revocation reasons may be given:

- key compromise (keyCompromise (1))
- the Certificate is no longer needed (cessationOfOperation (5))

The options available in each revocation service are described in the description of the specific service.

When the Certification Service Provider initiates the revocation, the following revocation reasons may be given:

- unspecified (unspecified (0), which results in no reasonCode extension being provided)
- key compromise (keyCompromise (1))
- Certificate modification (affiliationChanged (3))
- Certificate renewal (superseded (4))
- right of use has been terminated (privilegeWithdrawn (9))

<not TLS:

During the suspension request, the same reasons can be given as in the case of revocation, but the following status is displayed in the revocation status service during the suspension:

- suspended (certificateHold (6))

If the Client requests the final revocation of a suspended Certificate, he can provide the same revocation reason as written above.

If the Certification Service Provider initiates the revocation of the suspended Certificate, it sets the revocation reason as specified during the suspension request.

>

Using the Private Key of a Revoked Certificate

<TLS:
The use of the private key belonging to the revoked Certificate shall be eliminated immediately.
>
<not TLS:
The use of the private key belonging to the revoked or suspended Certificate shall be eliminated or suspended immediately.
>
If possible, the private key belonging to the revoked Certificate shall be destroyed immediately after revocation.
Responsibility regulations related to <not TLS: suspension and> revocation:

- If the Certification Service Provider has already published the revoked status of the Certificate, the Certification Service Provider does not take any responsibility, if the Relying Party considers the Certificate valid.

4.9.1 Circumstances for Revocation

Reasons for Revoking a Subscriber Certificate

Certification Authority revokes the end-user Certificate within 24 hours and uses the corresponding CRLreason if one or more of the following occurs:

- a fully compliant revocation request is submitted to the Certification Service Provider using the web-based revocation service operated by it (see in section 4.9.3)

<TLS:

- a fully compliant revocation request is submitted to the Certification Service Provider using the SMS-based revocation service operated by it
  (see in section 4.9.3)

>
[[QUA:
<not TLS:

- **in case of Email (S/MIME) Certificate, a fully compliant revocation request is submitted to the Certification Service Provider using the SMS-based revocation service operated by it**
  (see in section 4.9.3)

>
]]
<UNI:

- in case of Code Signing Certificate, a fully compliant revocation request is submitted to the Certification Service Provider using the SMS-based revocation service operated by it

  (see in section 4.9.3)

- in case of Email (S/MIME) Certificate, a fully compliant revocation request is submitted to the Certification Service Provider using the SMS-based revocation service operated by it

  (see in section 4.9.3)

>

- the Subject or Applicant or the Subscriber requests the revocation of the Certificate in writing

  (see in section 4.9.3)

- the Subject or Applicant or the Subscriber notifies the Certification Authority that the Certificate Application was not approved and does not retroactively grant authorization

  (privilegeWithdrawn (9))

- the Certification Authority becomes aware that the private key corresponding to the public key in the Certificate has been compromised

  (keyCompromise (1))

<TLS:

- the Certification Authority is made aware of a demonstrated or proven method that can easily compute the Subscriber's private key (such as a Debian weak key, see `http://wiki.debian.org/SSLkeys`)

  (keyCompromise (1))

> <not TLS:

- the Certification Authority is made aware of a demonstrated or proven method that can easily compute the Subscriber's private key (such as a Debian weak key, see `http://wiki.debian.org/SSLkeys`)

  (keyCompromise (1))

>
<TLS:

- the Certification Authority obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name

  [[ADV:

  or IP address

  ]]

  in the Certificate should not be relied upon

  (superseded (4))

>
<UNI:

- in case of Email (S/MIME) Certificate, the Certification Authority obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon

  (superseded (4))

- in case of Code Signing Certificate, the Certification Authority is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, or if there is clear evidence that the specific method used to generate the private key was flawed

  (keyCompromise (1))

- in case of Code Signing Certificate, the Certification Authority has reasonable assurance that the Certificate was used to sign Suspect Code.

  (privilegeWithdrawn (9))

>
Certification Authority revokes the end-user Certificate within 24 hours if it is possible and revokes the end-user Certificate within 5 days and use the corresponding CRLreason if one or more of the following occurs:

- the Certification Authority becomes aware that the public key in the Certificate does not comply with the requirements defined in Section 6.1.5 and 6.1.6

  (superseded (4))

- the Certification Authority becomes aware that the certificate was misused

  (privilegeWithdrawn (9))

- the Certification Service Provider is made aware that a Subscriber has violated one or more of its material obligations under the service agreement or General Terms and Conditions

  (privilegeWithdrawn (9))

<TLS:

- the Certification Authority becomes aware that the usage of the Fully-Qualified Domain Name

  [[ADV:

  or IP address

  ]]

  indicated in the Certificate is no longer legally permitted (e.g court withdraw the right to use the domain, or the owner does not renew the domain registration)

  (cessationOfOperation (5))

[[ADV:

- *the Certification Authority becomes aware that the wildcard certificate was used for deceptive domain name authentication*

  (privilegeWithdrawn (9))

]]

> <UNI:

- in case of Email (S/MIME) Certificate, the Certification Authority becomes aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted

  (privilegeWithdrawn (9))

>

- the Certification Authority is made aware of a material change in the information contained in the Certificate

  (privilegeWithdrawn (9))

- the Certificate modification because of data change referring to the Subject

  (privilegeWithdrawn (9))

- the Certification Authority becomes aware that the Certificate was not issued according to the <TLS: CABF Baseline Requirements or the > related Certificate Policy or the Certification Practice Statement

  (superseded (4))

- the Certification Authority becomes aware that any of the data appearing in the Certificate is inaccurate

  (privilegeWithdrawn (9))

- the Certification Authority is no longer entitled to issue Certificates, unless the Certification Authority made arrangements to continue maintaining the CRL/OCSP Repository

  (unspecified (0), which results in no reasonCode extension being provided)

- the revocation is required by the Certification Authority's Certificate Policy or the Certification Practice Statement for a reason that is not otherwise required to be specified by this section

  (unspecified (0), which results in no reasonCode extension being provided)

<TLS:

- the Certification Authority is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, or if there is clear evidence that the specific method used to generate the private key was flawed

  (keyCompromise (1))

> <UNI:

- in case of Email (S/MIME) Certificate, the Certification Authority is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, or if there is clear evidence that the specific method used to generate the private key was flawed

  (keyCompromise (1))

>

- the Certification Authority issued the Certificate based on a document from a third party, and it withdraws that document in writing

  (privilegeWithdrawn (9))

- the format and technical content of the Certificate presents an unacceptable risk to the Relying Parties (for example, if the used cryptographic algorithm or key size is no longer secure)

  (keyCompromise (1))

- the Certification Authority becomes aware that the private key of the Certificate issuer certification unit might be compromised

  (unspecified (0), which results in no reasonCode extension being provided)

<not TLS:

- a Certification Authority receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted

  (privilegeWithdrawn (9))

- the Certificate was suspended, and was not reinstated during the ensured time period (see section: 4.9.16)

>

- the termination of service agreement

  (privilegeWithdrawn (9))

- the Certification Authority has terminated its activities

  (unspecified (0), which results in no reasonCode extension being provided)

<not UNI:

- the supervisory body enacts it in a legally binding and executable decision

  (unspecified (0), which results in no reasonCode extension being provided)

>

- the law makes revocation mandatory

  (unspecified (0), which results in no reasonCode extension being provided)

Certification Authority may revoke the end-user Certificate and use the corresponding CRLreason if one or more of the following occurs:

- the Certification Authority becomes aware that the Subscriber failed to fulfil any of its financial obligations according to the service agreement

  (privilegeWithdrawn (9))

Reasons for Revoking a Subordinate CA Certificate

Certification Authority is bound to take action on the revocation of the Certificate of the intermediate certification unit in the following cases:

- the CA operating the Subordinate CA requests the revocation of the Certificate in writing
- the Subordinate CA notifies the Certification Service Provider that the original Certificate Application was not authorized and does not retroactively grant authorization
- the Certification Authority becomes aware that it is not in the exclusive possession of the private key
- the Certification Authority becomes aware that the public key in the Certificate does not comply with the requirements defined in Section 6.1.5 and 6.1.6
- the Certification Authority becomes aware that the Certificate was misused
- the Certificate was not issued according to the relevant Certificate Policy and the Certification Practice Statement or the operation of the intermediate certification unit does not comply with the relevant Certificate Policy or Certification Practice Statement
- the Certification Authority determines that any of the information appearing in the Certificate is inaccurate or misleading
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another Certification Authority to provide revocation support for the Certificate
- Certification Authority is no longer entitled to issue Certificates, and maintenance is not provided for the CRL and OCSP services related to the Certificates
- the revocation is required by the Issuing CA's Certificate Policy or the Certification Practice Statement
- Certificate modification because of data change relating to the certification unit or Certification Authority
- the format and technical content of the Certificate presents an unacceptable risk to the Relying Parties (for example, if the used cryptographic algorithm or key size is no longer secure)

- the Certification Authority has terminated its activities
- the law makes the revocation mandatory

The extension of the defined time frames is not possible, if the Certificate was issued under a Root Certificate trusted by any of the Trusted Root Certificate Programs.

4.9.2 Who Can Request Revocation

The revocation of the Certificate may be requested by anyone using the following services operated by the Certification Service Provider, who knows the secret revocation password and the requested identification data:

- web-based revocation service

<TLS:

- SMS-based revocation service
- ACME-based revocation service

>

[[QUA:

<not TLS:

- **in case of Email (S/MIME) Certificate, SMS-based revocation service**

>

]]

<UNI:

- in case of Code Signing Certificate and Email (S/MIME) Certificate, SMS-based revocation service

>

The revocation of the Certificate may be requested in writing by the Clients, namely:

- the Subscriber

<not SEA:

- the Subject or Applicant
- in case of Organizational Certificate, the Organization's authorized representative

>

- the contact person specified in the service agreement

- Organizational Administrator appointed by the Subscriber

[[ADV:
<UNI:

- *the supervisory authority which issued the payment service licence for the Subject, if the Certificate contains the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2]*

>
]]
[[QUA:
<BEL:

- **the supervisory authority which issued the payment service licence for the Subject, if the Certificate contains the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2]**

>
<TLS:

- **the supervisory authority which issued the payment service licence for the Subject, if the Certificate contains the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2]**

>
]]
[[QUA:
<not TLS:

- **in case of remote key management service the Remote Key Management Service Provider**

>
]]

- the Certification Service Provider.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit High Risk Certificate Problem Reports informing the Certification Service Provider of reasonable cause to revoke the Certificate, like fraud, misuse or key compromise.

The Certification Service Provider provides clear instructions on how to report suspected Private Key Compromise, Certificate misuse, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via the following website:

`https://e-szigno.hu/security-events-report`

<TLS: and in section 1.5.2 of the present Certification Practice Statement. >

4.9.3 Procedure for Revocation Request

The Certification Service Provider ensures the following possibilities to submit a revocation request:

- **Via the Website of the Certification Service Provider 24 Hours a Day**

  The revocation request can be submitted via the following website of the Certification Service Provider:

  `https://e-szigno.hu/revocation`

  When revoking via the website of the Certification Service Provider the Client needs to provide the following information:

  - the revocation password as a data certifying the authenticity of the revocation request,
  - the last three parts of the Subject OID in the Certificate (e.g. 2.2.123), or in case of natural person Subject instead of the OID the date of birth of the Subject.

  Revocation requests submitted via the website of the Certification Service Provider are processed without delay by the information system of the Certification Service Provider and it immediately notifies the applicant about the result via its website.

  In case of a successful revocation, the changed revocation status appears in the internal Revocation Status Registry of the Certification Service Provider immediately. The inner processes of the Certification Service Provider ensure that the processing ends within at most 5 minutes from the provision of data, so the changed revocation state is updated from the receipt of the request within maximum that interval.

  When a request submitted via the Certification Service Provider website, the revocation reason is always:

  - key compromise (keyCompromise (1))

  The Certification Service Provider logs every revocation request. In case of a successful revocation, the Certification Service Provider notifies the Subject and the Subscriber about the fact of the revocation by email.

  The Certification Service Provider guarantees availability of revocation service only for revocation requests received from SMS text. If the website of the Certification Service Provider is not available, the Certification Service Provider recommends the Client to request revocation by sending SMS.

<not SIG: <not SEA:

- **By Sending a Fixed-format SMS Text Message 24 Hours a Day**

  <UNI: The service is available only for Code Signing Certificates and Email (S/MIME) Certificates. >

The Clients of the Certification Service Provider may indicate in an SMS text message sent to the Certification Service Provider's revocation phone number if a private key is possessed by an unauthorized person.

The Certification Service Provider immediately begins the processing of the revocation requests arriving in text messages. The Certification Service Provider's system sends an automatically generated reply message to the phone number of the requester about the result of processing and the success of the revocation.

In the request sent in the text message the following data shall be provided separated by a space character:

- date of birth of the Subject in the "YYYY-MM-DD" format, or the last three digits of the OID as indicated in the Certificate
- the revocation password of the Certificate.

Example of formally correct revocation request:

- "2.1.134 pacsirta"

When a request submitted via SMS text message, the revocation reason is always:

- key compromise (keyCompromise (1))

The Certification Service Provider always declines the revocation request arriving in a text message from a hidden phone number regardless of the content of the message.

In order to ensure the availability of the revocation service, the Certification Service Provider also maintains telephone numbers operated by two different mobile service providers. If sending an SMS to one phone number fails (no confirmation is received within a few minutes), please try sending the message to the other phone number.

Phone numbers to receive revocation SMS:

"+36 (20) 263-4943"

"+36 (30) 326-2187"

>>
<not TLS: <not UNI:
[[QUA:

- **By Sending a Fixed-format SMS Text Message 24 Hours a Day**

  The service is available only for Email (S/MIME) Certificates.

  The Clients of the Certification Service Provider may indicate in an SMS text message sent to the Certification Service Provider's revocation phone number if a private key is possessed by an unauthorized person.

  The Certification Service Provider immediately begins the processing of the revocation requests arriving in text messages. The Certification Service Provider's system

sends an automatically generated reply message to the phone number of the requester about the result of processing and the success of the revocation.

In the request sent in the text message the following data shall be provided separated by a space character:

- **date of birth of the Subject in the "YYYY-MM-DD" format, or the last three digits of the OID as indicated in the Certificate,**
- **the revocation password of the Certificate.**

Example of formally correct revocation request:

- **"2.1.134 pacsirta"**

When a request submitted via SMS text message, the revocation reason is always:

- **key compromise (keyCompromise (1))**

The Certification Service Provider always declines the revocation request arriving in a text message from a hidden phone number regardless of the content of the message.

In order to ensure the availability of the revocation service, the Certification Service Provider also maintains telephone numbers operated by two different mobile service providers. If sending an SMS to one phone number fails (no confirmation is received within a few minutes), please try sending the message to the other phone number.

Phone numbers to receive revocation SMS:

"+36 (20) 263-4943"

"+36 (30) 326-2187"

]]
>>
<TLS:

- **By using ACME protocol 24 hours a day**

  Within the framework of this service, Website Authentication Certificates managed via the ACME protocol can be revoked using the "revokeCert" command.

  The Certification Service Provider immediately begins processing revocation request received via the ACME protocol. The Certification Service Provider sends an automatically generated response message via the ACME protocol about the processing result and the success of the revocation.

>

- **By Using e-Szignó Account**

  A revocation request can be submitted 24 hours a day using the e-Szignó Account operated by the Certification Service Provider.

  Access address of the e-Szignó Account:

  `https://portal.e-szigno.hu/login`

  On the e-Szignó Account interface, the Client shall select the Certificates to be revoked and then select the reason for revocation from the list below:

  – key compromise (keyCompromise (1))
  – cessation of operation (cessationOfOperation (5))

  Following options are available for authentication of the revocation request to be submitted:

  – **Electronic Signature or Electronic Seal**

    By creating an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3)]]* of the Applicant on the e-Szignó Account interface.

    The submitted revocation requests are processed by the Certification Service Provider during working hours as described in chapter 4.9.5.

    Using this method, a large number of Certificates can be revoked in one application.

  – **Entering the Revocation Password**

    The Client shall enter the revocation password for the Certificate to be revoked via the e-Szignó Account interface.

    Revocation requests submitted this way are processed without delay by the information system of the Certification Service Provider and it immediately notifies the applicant about the result via its website.

    By using this method, those Certificates can be revoked in one request that have the same revocation password.

- **Sent by Email, with an Electronic Signature or Electronic Seal**

  in electronic form with an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3)]]* sent to the Certification Service Provider's `revocation@e-szigno.hu` email address.

  In the submitted application, the applicant must select the revocation reason from the list below:

  – key compromise (keyCompromise (1))
  – the Certificate is no longer needed (cessationOfOperation (5))

- **On Paper, Signed Manually**

  The paper-based, manually signed application can be submitted in person at the Certification Service Provider's Customer Service during service hours or sent by post to the Certification Service Provider's Customer Service address as defined in chapter 1.3.1. In the submitted application, the applicant must select the revocation reason from the list below:

  - key compromise (keyCompromise (1))
  - the Certificate is no longer needed (cessationOfOperation (5))

In case of a Revocation request submitted in writing the Certification Service Provider verifies the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

In case of Revocation request signed with a valid electronic signature, there is no need for further verification of the identity of the applicant and the authenticity of the request.

In case of submitting revocation request on paper, via mail the Certification Service Provider verifies the manual signature on the request.

If the revocation was requested by the Client, and it does not state the reason for revocation, then the Certification Service Provider considers that the reason for revocation is that the Subject does not want to use the Certificate anymore (cessationOfOperation (5)).

If the Client request the revocation due to key compromise, the Certification Service Provider ensures a possibility during the revocation process, to request a new Certificate in the framework of *Re-key* to replace the Certificate to be revoked. The rules for *Re-key* are in section 4.7.

When the revocation is requested in writing, the Certification Service Provider makes possible to ask the revocation in advance for a later date by giving the requested date of the revocation.

The revocation request shall contain the data to identify the Certificate.

The requester shall provide particularly the following information:

- the exact denomination of the Subject

<not TLS:
[[QUA:

- **if the Certificate was issued on a Qualified Electronic Signature or Seal Creation Device, the unique identifier of the Qualified Electronic Signature or Seal Creation Device**

]]
>

- the Certificate's unique identifier
- the requested date of the revocation, if the revocation shall not happen immediately
- identification data of the Client.

In case of invalid or incomplete revocation request the Certification Service Provider rejects the request. The Certification Service Provider notifies the Subject and the Subscriber about the fact and reason of the rejection by email.

In case of complete and valid request the Certification Service Provider makes a decision about the acceptance of the request. Depending on the content of the request the Certification Service Provider revokes the Certificate immediately or sets up the date of revocation according to the request.

In case of a successful revocation the Certification Service Provider notifies the Subject and the Subscriber about the revocation by email.

Further information about the suspension and revocation can be found on the home page of the Certification Service Provider on the following link:

`https://e-szigno.hu/certificate-suspension-and-revocation`

High-Priority Certificate Problem Report

The Certification Service Provider maintains a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report.

The Certification Service Provider is only obliged to process High Priority Certificate Problem Reports submitted in Hungarian or English, the processing of High Priority Certificate Problem Reports submitted in other languages is uncertain, and the Certification Service Provider may reject them without substantive processing.

The Certification Service Provider begins investigating the Certificate Problem Report within 24 hours after receiving and decides whether revocation is appropriate based on the following criteria:

- the nature of the alleged problem
- the consequences of revocation
- the number of Certificate Problem Reports received about a particular Certificate or Subscriber
- the entity making the complaint, and
- relevant legislation.

The Certification Service Provider provides a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the Certification Service Provider works with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which the Certification Service Provider will revoke the Certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frame set forth in Section 4.9.5

If necessary, the Certification Service Provider informs the National Media and Infocommunications Authority about the reported problem.

4.9.4 Revocation Request Grace Period

The Certification Service Provider does not apply grace period during the fulfilment of revocation requests.

4.9.5 Time Within Which CA Must Process the Revocation Request

The Certification Service Provider processes the following revocation requests immediately 24 hours a day:

- revocation requests issued via the website of the Certification Service Provider

<TLS:

- revocation requests issued by sending a fixed-format SMS text message

>
[[QUA:
<ALA:

- **in case of Email (S/MIME) Certificate, revocation requests issued by sending a fixed-format SMS text message**

>
<BEL:

- **in case of Email (S/MIME) Certificate, revocation requests issued by sending a fixed-format SMS text message**

>
]]
<UNI:

- in case of Code Signing Certificate and Email (S/MIME) Certificate, revocation requests issued by sending a fixed-format SMS text message

>
The Certification Service Provider processes the revocation requests issued by any other way within 24 hours following the official arrival time of the request.

The Certification Service Provider determines the date of receipt of the revocation request in the following way:

- In case of revocation requests sent by electronic mail to the dedicated email address `revocation@e-szigno.hu` during office hours of the Customer Service, the official time of arrival is when the email is received on the server of the Certification Service Provider.

- In the case of a request submitted in e-Szignó Account during the opening hours of the Customer Service, the official time of receipt is the actual time of the request submission, recorded by the server.

  Requests submitted outside of Customer Service opening hours are considered received at the beginning of the next Customer Service opening hours.

- In case of applications submitted in person, the time of arrival is when the customer service officer of the Certification Service Provider receives the application.

- In case of applications sent by post, the time of arrival is when the mail arrives to the Certification Service Provider at office hours.

The Certification Service Provider undertakes to meet these requirements only for revocation requests sent to the indicated addresses stated in section 1.3.1. In case of revocation request sent to other addresses – specially directly sent to specific associate of the Certification Service Provider – or via other channels, the Certification Service Provider does not offer any availability.

<not TLS:

If the Client wants to revoke its Certificate and the revocation is urgent, or the Client cannot appear in person at the office of the Certification Service Provider, the Certification Service Provider recommends to the Client to suspend the Certificate until the revocation by using the SMS based suspension service (see section 4.9.13). It is sufficient to take care of the revocation of the suspended certificates later, and the Certification Service Provider automatically revokes the suspended Certificates after the time for restoration elapses (see section: 4.9.16).

>

<TLS:

The Certification Service Provider begins investigation of the Website Authentication Certificate related reported problems and makes decision about further steps within 24 hours.

The Certification Service Provider provides a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

The Certification Service Provider revokes the Website Authentication Certificates within 24 hours after the conditions defined in section 4.9.1 are met.

The Certification Service Provider revokes the Website Authentication Certificate issuer intermediate certification units' Certificates within 7 days after the conditions defined in section 4.9.1 are met.

>

4.9.6 Revocation Checking Requirement for Relying Parties

To maintain the level of security guaranteed by the Certification Service Provider, prior to the adoption and use of the information indicated in the Certificate, it is necessary for Relying Parties to act with proper carefulness. It is particularly recommended for them to verify all of the Certificates located in the Certificate chain according to the relevant technical standards. The verification should cover the verification of the Certificates' validity, the policy requirements and key usage, and the checking of the referenced CRL or OCSP based revocation information.

4.9.7 CRL Issuance Frequency

End user certificates

The Certification Service Provider issues a new Certificate Revocation List for its end user Certificates at least once a day. The validity of these Certificate Revocation Lists is 25 hours.

The Certification Service Provider continues issuing Certificate Revocation Lists until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked
- the corresponding Subordinate CA Private Key is destroyed.

<UNI:

Timestamping Unit Certificates for Codesigning

The Certification Service Provider issues a new Certificate Revocation List for its Timestamping Unit Certificates used for Codesigning monthly, but not later than 15 days before the expiry of the current Certificate Revocation List. The validity of these Certificate Revocation Lists is 65 days.

>

Intermediate certification units

The Certification Service Provider issues a new Certificate Revocation List for its intermediate certification units every day at the same time. The validity of the Certificate Revocation Lists is 25 hours.

4.9.8 Maximum Latency for CRLs

At most 5 minutes elapse between the generation and disclosure of the Certificate Revocation List (CRL).

The size of the Certificate Revocation List file never exceeds 10 MB.

4.9.9 Online Revocation/Status Checking Availability

<UNI: The Certification Service Provider may provide online Certificate revocation status (OCSP) service for Timestamping Certificates used for Codesigning.

The Certification Service Provider provides online Certificate revocation status (OCSP) service for each other type of Certificates. > <not UNI: The Certification Service Provider provides online Certificate revocation status (OCSP) service. >

4.9.10 Online Revocation Checking Requirements

The online Certificate status service complies with the requirements of Section 4.10.

Certification Authority provides OCSP service through GET method.

4.9.11 Other Forms of Revocation Advertisements Available

The Certification Service Provider makes available in its public Certificate Repository – with their status – the revoked <not TLS: and suspended> Certificates. Thus by searching in the Certificate Repository the Clients and the Relying Parties can personally (without the help of an application) verify the revocation status of a Certificate.

See more details in chapter 2.2.

4.9.12 Special Requirements for Key Compromise

Any interested party may submit a key compromise report to the Certification Authority if it becomes aware that the private key of any Certificate issued by the Certification Authority has been compromised.

The fastest way to report is via the following website:

`https://e-szigno.hu/security-events-report`

At the time of report, the reporter must prove that the private key has indeed been compromised. The report must specify:

- the compromised private key itself, or
- the PKCS#10 certificate request signed by the compromised private key and containing the following text in the "CN" field: "Proof of Key Compromise".

In case of any certification unit's private key is compromised, the Certification Service Provider makes every reasonable effort in order to notify the Relying Parties about the incident. It publishes any status change on the provider Certificates via its website.

In case of compromised Certificates issued by the Certification Service Provider, the Certification Service Provider is able to revoke the end-user Certificate belonging to the compromised private key. The revocation reason information (reasonCode) in this case is set to keyCompromise (1) value.

4.9.13 Circumstances for Suspension

<TLS:

The validity of the Website Authentication Certificates shall not be suspended.

>

<not TLS:

When it is possible, the Certification Service Provider ensures a possibility for Clients for the temporary suspension of the Certificate <UNI: in case, that it can be assumed that any of the reasons establishing revocation exists.

[[QUA:

<ALA: The Email (S/MIME) Certificates shall never be suspended.>

<BEL: The Email (S/MIME) Certificates shall never be suspended.>

]]

>

<UNI: The Code Signing Certificates and Email (S/MIME) Certificates never shall be suspended.
>
The Certification Service Provider is entitled for Certificate suspension for the following reasons:

- the Subscriber does not pay until the payment deadline
- if the Certification Service Provider presumes that the data indicated on the Certificate do not comply with reality. If the Certification Service Provider becomes aware of those conditions, it initiates the suspension or revocation of the Certificate
- if the Certification Service Provider presumes that the private key belonging to the Certificate is not in the possession of the Subject, and it is confirmed by substantial evidence. If the Certification Service Provider becomes aware of that the Electronic Signature or Seal Creation Device is possessed by an unauthorized person, the Certification Service Provider suspends every Certificate it contains
- the supervisory body enacts (smth.) in a legally binding and executable decision

The Certification Service Provider does not accept suspension requests related to Certificates not valid, in addition to justify the reason for rejection.
>

4.9.14 Who Can Request Suspension

<TLS: Not applicable. >
<not TLS:
The suspension of a Certificate can be requested by the same persons, who are eligible to initiate the revocation of the Certificate (see section: 4.9.2).
>

4.9.15 Procedure for Suspension Request

<TLS: Not applicable. >
<not TLS:
The Certification Service Provider ensures opportunity for suspension initiation:

- **Suspension via the Website of the Certification Service Provider 24 Hours a Day**

  The suspension request can be submitted via the following website of the Certification Service Provider:

  `https://e-szigno.hu/suspension`

  When suspending via the website of the Certification Service Provider the Client needs to provide the following information:

  - the suspension password as a data certifying the authenticity of the suspension request,

– the last three parts of the Subject OID in the Certificate (e.g. 2.2.123), or in case of natural person Subject instead of the OID the date of birth of the Subject.

Suspension requests submitted via the website of the Certification Service Provider are processed without delay by the information system of the Certification Service Provider and it immediately notifies the applicant about the result via its website.

In case of a successful revocation, the changed revocation status appears in the internal Revocation Status Registry of the Certification Service Provider immediately. The inner processes of the Certification Service Provider ensure that the processing ends within at most 5 minutes from the provision of data, so the changed revocation state is updated from the receipt of the request within maximum that interval.

When a request submitted via the Certification Service Provider website, the revocation reason is always:

– key compromise (keyCompromise (1))

The Certification Service Provider logs every suspension request. In case of a successful suspension, the Certification Service Provider notifies the Subject and the Subscriber about the fact of the suspension by email.

The Certification Service Provider guarantees availability of suspension service only for suspension requests received from SMS text. If the website of the Certification Service Provider is not available, the Certification Service Provider recommends the Client to request suspension by sending SMS.

- **Suspension by Sending a fixed-format SMS Text Message**

[[QUA:

<ALA: Suspension service is not available for Email (S/MIME) Certificates. The Certification Service Provider processes suspension requests received for Email (S/MIME) Certificates as a revocation request. The validity of the Certificates will be irreversibly revoked .

>

<BEL: Suspension service is not available for Email (S/MIME) Certificates. The Certification Service Provider processes suspension requests received for Email (S/MIME) Certificates as a revocation request. The validity of the Certificates will be irreversibly revoked .

>

]]

<UNI: Suspension service is not available for Code Signing Certificates and Email (S/MIME) Certificates. The Certification Service Provider processes suspension requests received for Code Signing Certificates and Email (S/MIME) Certificates as a revocation request. The validity of the Certificates will be irreversibly revoked .

>

The Clients of the Certification Service Provider may indicate in an SMS text message sent to the Certification Service Provider's suspension phone number if a Qualified Electronic Signature or Seal Creation Device or a private key is possessed by an unauthorized person.

The Certification Service Provider immediately begins the processing of the suspension requests arriving in text messages. The Certification Service Provider' s system sends an automatically generated reply message to the phone number of the requester about the result of processing and the success of the suspension.

In the request sent in the text message the following data shall be provided separated by a space character:

- date of birth of the Subject in the "YYYY-MM-DD" format or the last three digits of the OID as indicated in the Certificate,
- the suspension password of the Certificate.

Examples of formally correct suspension request:

- "1976-11-04 a1b2c3d4"
- "2.1.134 pacsirta"

When a request submitted via SMS text message, the revocation reason is always:

- key compromise (keyCompromise (1))

The Certification Service Provider always declines the suspension request arriving in a text message from a hidden phone number regardless of the content of the message.

In order to ensure the availability of the suspension service, the Certification Service Provider also maintains telephone numbers operated by two different mobile service providers. If sending an SMS to one phone number fails (no confirmation is received within a few minutes), please try sending the message to the other phone number.

Phone numbers to receive suspension SMS:

"+36 (20) 263-4943"

"+36 (30) 326-2187"

- **Suspension by Using e-Szignó Account**

A suspension request can be submitted 24 hours a day using the e-Szignó Account operated by The Certification Service Provider.

Access address of the e-Szignó Account:

`https://portal.e-szigno.hu/login`

On the e-Szignó Account interface, the Client shall select the Certificates to be suspended and then select the reason for revocation from the list below:

- key compromise (keyCompromise (1))
- cessation of operation (cessationOfOperation (5))

Following options are available for authentication of the suspension request to be submitted:

– **Electronic Signature or Electronic Seal**

By creating an electronic signature or electronic seal based on a non-pseudonymous **[[QUA: qualified]]** Certificate *[[ADV: with a security classification not lower than the requested Certificate (see section 1.2.3)]]* of the Applicant on the e-Szignó Account interface.

The submitted suspension requests are processed by the Certification Service Provider during working hours as described in chapter 4.9.5.

Using this method, a large number of Certificates can be suspended in one application.

- **Suspension the Same Way as Revocation Request Submission**

The Certification Service Provider enables the submission of the suspension requests the same way, as the revocation requests, according to the requirements of section 4.9.3. From the suspension application, the Certification Service Provider shall be able to determine that exactly which Certificate the applicant asks to the suspend and upon what grounds. The registration staff member sends a notification via email to the Subject and the Subscriber.

At suspension, the reason of suspension shall be given. If the Client requests the suspension, and does not give the reason, the Certification Service Provider assumes that the reason is private key compromise (keyCompromise (1)).

If the Client asks for the suspension because of key compromise, then the Certification Service Provider provides an opportunity for the Client during the suspension process to indicate that if the Certificate is not reinstated within a time frame (and so it becomes revoked), then a new certificate will be requested within the framework of *Re-key*. The rules of *Re-key* are in section 4.7.

>

4.9.16 Limits on Suspension Period

<TLS: Not applicable. >

<not TLS:

If the suspension of the Certificate was requested by the Client, the Client may request the reinstatement of the Certificate within 5 working day after the suspension. If the reinstatement of the Certificate is not requsted within this interval the Certification Service Provider revokes the Certificate.

The reinstatement application can only be submitted to the Certification Service Provider:

- personally in the customer service of the Certification Service Provider
- in an electronic form with an electronic signature based on the non-pseudonymous **[[QUA: qualified]]** Certificate *[[ADV: with a security classification not lower than the suspended Certificate (see section 1.2.3)]]*

In case of a successful Certificate reinstatement, the Certification Service Provider notifies the Subject and the Subscriber by email of the fact.

>

4.10 Certificate Status Services

The Certification Service Provider provides the following possibilities for the Certificate revocation status query:

- OCSP – online Certificate revocation status query service
- CRL – Certificate Revocation Lists.

<UNI:
In case of Code Signing Certificates the Certification Service Provider guaranties the availability of the OCSP based revocation information beyond the Code Signing Certificate's expiration date for at least 10 years.
>

The Certification Service Provider maintains an internal Revocation Status Registry, which contains the current revocation status information of all the Certificates issued by the Certification Service Provider, including the valid, revoked and suspended statuses.

In case of <TLS: revocation> <not TLS: suspension, reinstatement and revocation> the new status of the Certificate – see section: 4.9 – appears immediately in the revocation records of Certification Service Provider after the successful completion of the process.

The Revocation Status Registry contains also the revocation status information of the expired Certificates, which will be available till the expiry date of the issuing CA.

The Certification Service Provider generates the Certificate Revocation List based on the actual information received from the Revocation Status Registry, so any change in the revocation statuses will be published in the first Certificate Revocation List issued after the given change.

The OCSP responses issued by the OCSP responders of the Certification Service Provider are always based on the revocation status information received from the Revocation Status Registry at the time which is indicated in the OCSP response.

OCSP response issued by the Certification Service Provider may contain "good" status information only for the Certificates that were issued by the given certification unit and are stored in the Certification Service Provider's Certificate Repository (positive OCSP).

4.10.1 Operational Characteristics

4.10.1.1 Certificate Revocation List (CRL)

<UNI:

4.10.1.1.1 Timestamping Unit Certificates for Codesigning

These dedicated root and subordinate certification units issues Certificate Revocation List with the frequency below:

- the validity of the Certificate Revocation List is 65 days
- The Certification Service Provider issues a new Certificate Revocation List monthly, but not later than 15 days before the expiry of the current Certificate Revocation List

- These certification units issue Certificate Revocation List within 24 hours after the revocation status change of any Certificate issued by the given certification unit.

4.10.1.1.2 In Case of any Other Type of Certificates

>

Each certification unit of the Certification Service Provider issues Certificate Revocation List with the frequency below:

- The validity period of the Certificate Revocation List is 25 hours.
- Each certification unit issues Certificate Revocation List in at most every 24 hours.
- The productive (subordinate) certification units issue Certificate Revocation List within 60 minutes after the revocation status change of any Certificate issued by the given certification unit.

The all-time current Certificate Revocation Lists for the specific Certificates can be reached at the following address:

`https://e-szigno.hu/ca-certificates`

The effective date of the Certificate Revocation Lists ("thisUpdate") marks also the time when the certification unit assembled and started signing the Certificate Revocation List. After that, in case of long Certificate Revocation Lists the publication of the Certificate Revocation List may even take 1 or 2 minutes. The appearance of the next Certificate Revocation List ("nextUpdate") marks the latest next time, from what the next list is publicly available. Accordingly, the time interval between the date of the Certificate Revocation List entering into force, and the date of publication of the next Certificate Revocation List can be longer than the time intervals above, but this does not affect the time interval between the appearance of the CRLs is at most the interval stated before.

Regarding, that amongst the provided services, the validity of the Certificate can be determined the fastest and the easiest with OCSP, the Certification Authority recommends the use of OCSP to its Clients.

4.10.1.2 Online Certificate Status Protocol (OCSP)

<UNI: When offering OCSP service, the> <not UNI: The> Certification Authority publishes the revocation status of the Certificates with the OCSP service too.

The Certification Authority provides OCSP service according to the IETF RFC 6960 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the Certificates issued by the certification unit (section 1.3.1).

<not TLS:

The Certification Authority provides OCSP services two different ways, below the characteristics of the two versions are shown.

4.10.1.2.1 OCSP Service Provided for Clients

- Only those Clients use of this version of the OCSP service, that have a valid service agreement for the maintenance of that Certificate. The Certification Service Provider can identify the Client by the Certificate or by a username password pair at the query.
- This version of the OCSP service is available for all Certificates, the responses always contain the current information listed in the registry of the Certification Service Provider.
- The issued OCSP response is always made at the time of the query. The "thisUpdate" and "producedAt" time values in the OCSP response match with the time of the query.
- The "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.
- With the help of the OCSP service provided to Clients, an evidence always can be acquired that later verifies towards third parties the revocation status of the Certificate indicated in the registry of the Certification Service Provider for the query date.

4.10.1.2.2 Public and Free OCSP Service >

<TLS:
The main characteristics of the OCSP service:
>

- <not TLS: This version of the> <TLS: The> OCSP service is publicly and freely available, any Relying Party can avail itself of it same as the Certificate Revocation Lists. There is no need for authentication at query.
- <not TLS: This version of the> <TLS: The> OCSP service can be reached through the URLs indicated on the Certificates on the default HTTP port (port 80).

<TLS:

- The OCSP service meets the requirement of the IETF RFC 5019 [46] to support large-scale PKI environments that require a lightweight solution to minimize communication bandwidth and client-side processing.

>
[[QUA:
<not UNI: <not TLS:

- **In case of Email (S/MIME) Certificate, the OCSP service fulfils the requirement of the IETF RFC 5019 [46] to support the large scale PKI environments which require a lightweight solution to minimize communication bandwidth and clientside processing.**

>>
]]
<UNI:

- In case of Email (S/MIME) Certificate, the OCSP service fulfils the requirement of the IETF RFC 5019 [46] to support the large scale PKI environments which require a lightweight solution to minimize communication bandwidth and clientside processing.

>

- Based on the IETF RFC 6960 "Response Pre-production" process, the issued OCSP response can be created before the query and does not necessarily contain the nonce element. The Certification Service Provider can give the same response for multiple queries. The "thisUpdate" and "producedAt" time values are identical, but these can precede the time of the query.

<TLS:

- The "nextUpdate" indicated in the response is always filled and contains a time value not later than the responder certification expiration time.

>
[[QUA:
<not UNI: <not TLS:

- **In case of Email (S/MIME) Certificate, the "nextUpdate" indicated in the response is always filled, and contains a time value not later than the responder certification expiration time.**
- **In case of other Certificate, the "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.**

>>
]]
<UNI:

- In case of Email (S/MIME) Certificate, the "nextUpdate" indicated in the response is always filled, and contains a time value not later than the responder certification expiration time.
- In case of other Certificate, the "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.

>
<not TLS: <not UNI:

- The "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.

>>

- The "thisUpdate" value indicated in the issued OCSP response is never older than 24 hours, because the Certification Service Provider creates a new OCSP response at least in every 24 hours.

<TLS:

- The time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never smaller than 8 hours.

>

[[QUA:

<not UNI: <not TLS:

- **In case of Email (S/MIME) Certificate, the time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never smaller than 8 hours.**

>>

]]

<UNI:

- In case of Email (S/MIME) Certificate, the time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never smaller than 8 hours.

>

- The time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never greater than 10 days.

<TLS:

- The value in the "nextUpdate" field shall be before or equal to the "notAfter" value of all certificates included within the "BasicOCSPResponse.certs" field or, if the certs field is omitted, before or equal to the "notAfter" value of the CA certificate which issued the certificate that the "BasicOCSPResponse" is for.

>

- The OCSP responses always contain the current information listed in the revocation registry of the Certification Service Provider at the "thisUpdate" time of the OCSP response, but if the "thisUpdate" time of the OCSP response is earlier than the time for which the verification is carried out – which is either earlier or coincides with the time of the query –, then the OCSP response is not clear evidence for a third party regarding the revocation status of the Certificate.

<not TLS:
Due to the indicated differences of the aforementioned two versions of the OCSP services, the public and free service can be considered equivalent to the service provided to the Clients in the following cases:

- If there is no need for OCSP response storage, rather it is used for prompt, immediate decision making. In this case, it is acceptable, that the OCSP response does not verify the validity of the Certificate clearly for third parties at a definite time subsequently.
- If the time span between the time of the OCSP query and the time, regarding when the verification is made, is bigger, than the difference of the "nextUpdate" and "thisUpdate" values of the stored OCSP response (which can be at most the validity period of the responser certificate used for signing the OCSP response). In this case, the OCSP responses provided by the public and free service can be accepted as a clear evidence for the third party, because the thisUpdate field in them is guaranteed to be later than the time, regarding when the verification is made.
- If the verifier party does not query the OCSP response itself (but for example uses an OCSP response attached to an archive signature), then it is not necessary to check, which sources the OCSP response came from originally. It is sufficient to verify only that the "thisUpdate" value in the OCSP response is later, than the time regarding which the verification is made.

The Certification Service Provider ensures the aforementioned two versions of the OSCP services with the same availability. >

4.10.2 Service Availability

The Certification Service Provider ensures that the availability of the Certificate Repository and the terms and conditions pertaining to the Certificates issued by the Certification Service Provider is at least 99.9% per year, and the length of downtime shall not exceed at most 3 hours.

The Certification Service Provider ensures that the availability of the revocation status information and the revocation management service is at least 99.9% per year, and the length of downtimes shall not exceed at most 3 hours on any occasion.

The response time of the revocation status service in case of normal operation is less than 10 seconds.

4.10.3 Optional Features

The Certification Service Provider provides various (CRL and two types of OCSP) services according to the descriptions in this section, in the framework of Clients and Relying Parties can verify the revocation status of the Certificates issued by the Certification Service Provider. Besides these, the Certification Service Provider makes available in its public Certificate Repository – with their status indicated – the revoked <not TLS: and suspended> Certificates, so while searching in the Certificate Repository the Clients and Relying Parties can (without the help of an application) verify the revocation status of the Certificate.

4.11 End of Subscription

The Certification Service Provider revokes the end-user Certificates in case of the termination of the contract concluded with the Subscriber.

4.12 Key Escrow and Recovery

<TLS:

The Certification Service Provider does not provide key escrow service for a private key belonging to a Website Authentication Certificate.

>

<ALA:

The Certification Service Provider does not provide key escrow service for a private key belonging to a signatory Certificate.

>

<BEL:

The Certification Service Provider does not provide key escrow service for a private key belonging to a seal Certificate.

>

<UNI:

The Certification Service Provider provides key escrow service only for the private key belonging to the encryption Certificates.

During the key escrow service, the private key for decryption belonging to the Encryption Certificate of the Subject is stored by the Certification Service Provider in an encrypted, unique e-dossier using the AES 256 algorithm, with a unique key for each file, and handed over to the authorized party upon request. According to the decree 24/2016. (VI. 30.) of the Ministry of the Interior and the internal regulations of the e-Szignó Certification Authority, the Certification Service Provider entrusts its employees involved in the provision of trust services with trusted roles. The employee of the e-Szignó Certification Authority in the appropriate trusted role performs the restoration of the deposited decryption keys only at the request of the Client, and only these employees have the means and rights necessary for the restoration of the decryption keys.

>

4.12.1 Key Escrow and Recovery Policy and Practices

<TLS: The private key belonging to the Website Authentication Certificate shall not be escrowed.>

<ALA: The private key belonging to the signing Certificate shall not be escrowed. >

<BEL: The private key belonging to the seal Certificate shall not be escrowed.>

<UNI:

Depositing a Decryption Key

The decryption keys issued on Electronic Signature or Seal Creation Device are automatically deposited by the Certification Service Provider. The Certification Service Provider stores the decryption keys of the Certificates issued in software token in the following cases:

- the Client has requested a Certificate that can be used for electronic administration purposes, and its certification policy requires the deposit of the decryption key
- the Subscriber or the Subject requests the deposit of the key.

In the case of Certificate issued as a software token, after issuing the Certificate, the Client encrypts the decryption key in pfx format with the encryption Certificate provided by the Certification Service Provider for this purpose, then the Client sends it as an encrypted e-dossier to the Certification Service Provider's central customer service e-mail address (`info@e-szigno.hu`). The Client is responsible for the content of the encrypted e-dossier, the Client must ensure that the encrypted file actually contains the appropriate decryption key.

Restore a Deposited Decryption Key

The Client shall request the restoration of the decryption key, the Certification Service Provider does not apply any restrictions regarding the form of the request. The Client's request may be received, for example, by telephone or e-mail inquiry. The key may be collected by the Client, the person authorized to represent the Client or the Subject in person at the Customer Service Office of the Certification Service Provider or on the basis of a separate order within the framework of on-site disembarkation. Before handing over the key, the customer service representative with the appropriate trusted role identifies the recipient and, if necessary, requests the documents proving the right of representation. Identification is based on an official identity card. The Certification Service Provider only accepts identification documents containing a photograph. The Certification Service Provider hands over the deposited key on an optical data carrier (eg CD / DVD) or on a Electronic Signature or Seal Creation Device at the Client's request for an additional fee. >

4.12.2 Symmetric Encryption Key Encapsulation and Recovery Policy and Practices

<TLS:

The private key belonging to the Website Authentication Certificate shall not be escrowed, so regarding that the symmetric encryption keys do not have to be managed.

>

<ALA:

The private key belonging to the signing Certificate shall not be escrowed, so regarding that the symmetric encryption keys do not have to be managed.

>

<BEL:

The private key belonging to the seal Certificate shall not be escrowed, so regarding that the symmetric encryption keys do not have to be managed.

>

<UNI:
The Certification Service Provider does not use symmetric keys to provide the key escrow service.
>
<ALA:
>

5 Facility, Management, and Operational Controls

The Certification Service Provider applies physical, procedural, and personnel security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.

The Certification Service Provider keeps a record of the system units and resources related to the service provision and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.

The Certification Service Provider monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The Certification Service Provider takes care that physical access to critical services is controlled and keeps physical risk of the assets related to critical services at a minimum.

The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the Certification Service Provider's information, and physical zones.

Services that process critical and sensitive information are implemented at secure locations in the system of the Certification Service Provider.

The provided protection is proportional to the identified threats of the risk analysis that the Certification Service Provider has performed.

In order to provide adequate security:

- The Certification Service Provider implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.

- The Customer Service office of the Certification Service Provider was designed, to be able to meet the requirements for registration services under realistic costs.

- The Certification Service Provider constructed its mobile registration units, so that they comply with the requirements imposed on the registration service.

- The Certification Service Provider implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

5.1.1 Site Location and Construction

The IT system of the Certification Service Provider is located and operated within a properly secured Data Centre with physical and logical protection that prevents illegitimate access. Defensive solutions – as for example guarding, security locks, intrusion detection systems, video surveillance system, access control system – are applied over the course of locating and establishing the Data Centre that are built on each other and interdependent and together they provide a powerful protection system for the IT systems participating in service provision, and for the preservation of the confidential data stored by the provider.

5.1.2 Physical Access

The Certification Service Provider protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.

Certification Service Provider ensures that:

- each entry to the Data Centre is registered

[[QUA:

- **entry to the Data Centre may only happen after the simultaneous identification of two authorized staff members with trusted roles – and at least one of the staff members shall be a system administrator**

]]

[[ADV:

- *only authorized staff members with trusted roles with the right permissions can entry to the computer room individually*

]]

- persons without independent authorization can only stay in the Data Centre in justified cases, for the time required and accompanied by personnel with appropriate rights
- the entry logs shall be archived continuously and evaluated weekly.

The activation data (passwords, PIN codes) of the devices shall not be stored openly even in the Data Centre.

In the presence of unauthorized persons:

- data media containing sensitive information are physically out of reach
- the logged-in terminals are not left without supervision
- no work process is carried out during which confidential information may be revealed.

When leaving the computer room the administrator shall verify that:

- every equipment of the Data Centre is in an adequately secure operation state
- there's no terminal left logged-in
- physical storage devices are locked properly
- systems, devices providing physical protection operate properly
- the alarm system has been activated.

There are appointed responsible people to carry out regular physical security assessments. The results of the examinations are recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The Certification Service Provider applies an uninterruptible power supply unit in the Data Centre that:

- has adequate capacity to ensure power supply for the Data Centre's IT and subsidiary facility systems
- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other
- in the event of a permanent power outage, it has its own power generation equipment, which - thanks to the possibility of refueling - can provide the necessary energy for any period.

The air of the outer environment shall not get into the Data Centre directly. The Data Centre air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity is reduced to the level required by the IT systems.

The Certification Service Provider uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4 Water Exposures

The Data Centre of the Certification Service Provider is adequately protected from water intrusion and flooding. The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it.

[[QUA:

The total area of water security zone is monitored by an intrusion detection system.

]]

In the protected computer room, security is further increased by the use of a raised floor.

5.1.5 Fire Prevention and Protection

In the Data Centre of the Certification Service Provider, a fire protection system approved by the competent fire headquarters operates.

[[QUA:

Smoke and fire detectors automatically alert the fire brigade. Water vapor based, automatic fire extinguishing system has been installed in the computer room, which is not hazardous to human life, and does not damage the IT equipment.

]]

There is the type and quantity of manual fire extinguishers in accordance with the relevant regulations at clearly visible locations in each room.

5.1.6 Media Storage

The Certification Service Provider protects its media storages from unauthorized access and accidental damage. All audit and archive data is created in duplicate. The two copies are stored physically separated from each other in fireproof safes, at locations in a safe distance from each other in the operator room of the data centre used for the trust services.

The stored media storages are protected from damaging environmental influences such as low or high temperatures, dirt, moisture, sunlight, strong magnetic fields, strong radiation.

5.1.7 Waste Disposal

The Certification Service Provider ensures the environmental standards compliant disposal of the superfluous assets, and media.

The Certification Service Provider does not use the electronic storage media containing information classified as confidential even for storing data classified as not confidential after deleting their content and devices like that shall not be taken outside of the premises of the Certification Service Provider. The Certification Service Provider physically destroys – according to the rules of disposal – the defective for any other reason unusable, redundant media storages containing confidential classified information:

- chops paper documents up in a shredder machine
- disassembles the hard drives and smashes the critical components
- destroys the optical disc with a suitable shredder machine.

5.1.8 Off-Site Backup

The Certification Service Provider creates a backup weekly from which the whole service could be restored in case of a fatal error. The backups – at least including the last full backup – are stored at an external location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the backup locations is resolved.

Based on the randomly selected backup data a restoration test is made at least yearly. The main circumstances and results of the restoration test is recorded in an audit report.

5.2 Procedural Controls

The Certification Service Provider takes care that its systems are operated securely, according to the rules, and with a minimal risk of defects.

Procedural precautions have the objective of supplementing, and at the same time intensifying the effectiveness of physical safeguards, along with those applicable to personnel, by means of appointing and isolating trusted roles, documenting the responsibilities of various roles, as well as specifying the personnel headcounts and exclusion roles necessary for the various tasks, moreover identification and authentication expected in the various roles.

The Certification Service Provider's internal governance system ensures that its operation complies with legal, as well as its internal regulations. In its system a responsible person shall be clearly assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the Certification Service Provider's system. The auditing activity of the independent system auditor and the Certification Service Provider's internal auditor ensures the system's appropriate operation.

5.2.1 Trusted Roles

The Certification Service Provider creates trusted roles <not UNI: (in the wording of the regulation, scope of activities) > <not UNI: according to the requirements of decree 24/2016. [14] > for the performance of its tasks. The rights and functions are be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

The Certification Service Provider defines the following trusted roles, with the following responsibilities:

Manager with overall responsibility for the IT system of the service provider
: The individual responsible for the IT system.

Security officer
: Senior security associate, the individual with overall responsibility for the security of the service.

System administrator
: Infrastructure administrator. The individual with the task to install, configure and maintain the systems of the Certification Service Provider. Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring the development of technology, and for the detection and proposing of development solutions of the vulnerabilities of each system component.

Operator
: System operator, individual performing the IT system's continuous operation, backup and restore.

Independent system auditor
: Individual who audits the logged, as well as archived dataset of the Certification Service Provider, responsible for verifying the enforcement of control measures the service provider

implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.

Registration officer
Individual responsible for the approval of production, issuance, revocation <not TLS: and suspension> of end-user certificates.

<not TLS:

Official active in the field of personalization
The individual, whose task is to manage and personalize the intelligent cards.

>

For the provision of trusted roles, the manager responsible for the security of the Certification Service Provider formally appoints the Certification Service Provider's employees.

Only those persons may hold a trusted role who are in employment relationship with the Certification Service Provider. Trusted roles shall not be hold in the context of a commission contract.

<UNI:

Up to date records are kept by the Certification Service Provider of the trusted roles.

>

<not UNI:

Up to date records are kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority is notified without delay.

>

5.2.2 Number of Persons Required per Task

The security and operational regulations of the Certification Service Provider define that the following tasks can be only performed in protected environment, with the contemporaneous presence of two employees holding trusted roles:

- the generation of the Certification Service Provider's own service key pair
- the backup of the provider's private key
- the activation of the provider's private key
- the destruction of the provider's private key.

At least one of the persons performing the procedures listed above shall be a system administrator, and the other person shall not be the independent system auditor.

During the implementation of the operations listed, unauthorized person shall not be present in the room.

5.2.3 Identification and Authentication for Each Role

The users managing the IT system of the Certification Service Provider have unique identification data, enabling secure identification and authentication of the users.

The users can only access the IT systems critical from the aspect of the provision of the certification service after identification and authentication.

The identification and authentication data are revoked without delay in case of the cessation of user rights.

Every user of the IT system and every actor in the administrative process is identified individually.

To control physical access, the Certification Service Provider uses an RFID card-based access control system, and for logical access control, it uses VPN Certificates issued on a Secure Signature-Creation Device. Before successful authorization, not even a single security-critical task can be performed. Every employee of the Certification Service Provider has exactly as many access rights, as it is absolutely necessary for the assigned role.

5.2.4 Roles Requiring Separation of Duties

Employees of the Certification Service Provider can hold multiple trusted roles at the same time, but the Certification Service Provider ensures that:

- the security officer and the registration officer shall not hold the independent system auditor role
- the system administrator shall not hold the security officer and the independent system auditor role
- the manager with overall responsibility for the IT system shall not hold the security officer and the independent system auditor role.

In addition to the aforementioned, the Certification Service Provider seeks the complete separation of trusted roles.

5.3 Personnel Controls

The Certification Service Provider takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the Certification Service Provider's operation. The objective of precautions applicable to personnel is to reduce the risk of human errors, theft, fraud and cases of misuse.

The Certification Service Provider addresses personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties – who get in contact with the Certification Service Provider's services – shall sign a non-disclosure agreement.

At the same time, the Certification Service Provider ensures for its employees obtaining as well as further developing of common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

5.3.1 Qualifications, Experience, and Clearance Requirements

As a hiring requirement, the Certification Service Provider requires at least intermediate education degree, but the Certification Service Provider continues to take care that employees receive appropriate training. Immediately after recruitment, the Certification Service Provider grants a training for its new employees, under the course of which they acquire the knowledge necessary to carry out the job. Registration officer can only be an employee, who finished a training course during which, he/she acquired the ability to recognize the ID cards acceptable by the Certification Service Provider (ID card, passport and driver's license). The Certification Service Provider usually supports the professional development of the employees, but it also expects employees to independently develop their skills in their respective fields. Some of the employees of the Certification Service Provider have the role to detect and gather the technical and business innovations and to organize and share this knowledge with their colleagues.

Trusted roles can be held at the Certification Service Provider only by persons, who have no external influence and possess the necessary expertise validated by the Certification Service Provider. All personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the Certification Service Provider's operations.

The manager with overall responsibility for the IT system can only be a person who has:

- specialized degree (mathematics, physics college or university degree or a college/university degree acquired at an engineering department belonging to the technical field of science)
- at least three years of expertise in professional working experience related to information security.

5.3.2 Background Check Procedures

The Certification Service Provider only hires employees for trusted or leading roles, who

- have a clean record and there's no proceeding in progress against them that may affect the impunity
- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

At the time of the appointment, shall the leading role holder Certification Service Provider employee with a statement, a trusted role holder employee with a certificate of good conduct less than 3 months old justify the clean criminal record.

The Certification Service Provider verifies the authenticity of the relevant information given in the applicant's CV during the hiring process, like previous employment, professional references, most relevant educational qualifications.

5.3.3 Training Requirements

The Certification Service Provider trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge

- the specifics and the way of handling the Certification Service Provider's IT system
- the necessary special knowledge for fulfilling their scope of activities
- processes and procedures defined in the public and inner regulations of the Certification Service Provider
- the legal consequences of the individual activities
- the applicable IT security regulations to the extent necessary to the specific scope of activities
- the data protection rules.

The Certification Service Provider trains the employees concerned with registration about the dangers and risks related to the verification of the data to be indicated on the Certificate.

The employees concerned with registration take and pass an exam on the knowledge of the related requirements and procedures for data verification before their appointment, and this fact is documented by the Certification Service Provider.

Only employees having passed the training shall gain access to the he production IT system of the Certification Service Provider.

5.3.4 Retraining Frequency and Requirements

The Certification Service Provider ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.

Further training is held if there's a change within the processes or the IT system of the Certification Service Provider.

The training material is updated at least in every 12 months and contains the new threats and actual security practices.

The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

5.3.5 Job Rotation Frequency and Sequence

The Certification Service Provider does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The Certification Service Provider regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the Certification Service Provider, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability. Upon appointment every trusted role employee as part of the employment documents:

- gets written information about legal liabilities, rights, certification and management standards for the treatment of personal data
- gets a job description that includes the concerning security tasks
- signs a confidentiality agreement in which the related consequences non-compliant with security measures, (criminal sanctions) can be found too.

All of these include the labour legislation or criminal consequences, that sanction the different discipline – job obligations – violation or breaking the law.

5.3.7 Independent Contractor Requirements

The Certification Service Provider only assigns trusted roles to its employees.

The Certification Service Provider chooses persons employed with engagement contract or subcontract to perform the other tasks, chosen if possible, from the list of previously qualified suppliers. The Certification Service Provider concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons, and will not be exploited in any other way. The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the Certification Service Provider does not hold any trainings for them.

5.3.8 Documentation Supplied to Personnel

The Certification Service Provider continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents in writing:

- the organizational security regulations of the Certification Service Provider
- the confidentiality agreement to be signed
- personal job description
- educational materials on the occasion of the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational security regulations.

5.4 Audit Logging Procedures

In order to maintain a secure IT environment, the Certification Service Provider implements and operates an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

The Certification Service Provider logs every security-related event that can provide information on events, changes happened in the IT system or in its physical environment according to the generally accepted information security practice. In case of every log entry, it stores the following data:

- the time of the event
- the type of the event
- the identification of the user or the system who/what triggered the event
- the success or failure of the audited event.

All new audit record is appended to the audit records. The earlier saved audit records can't be modified or deleted.

All of the essential event logs are available to the independent system auditors, who examine the compliance of the Certification Service Provider's operation.

The Certification Service Provider logs the following events at minimum:

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too
  - the loss of synchronization
- LOGGING:
  - the shutdown, restart of the logging system or some of its components
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined
  - the modification or deletion of the stored logging data
  - the activities performed because of the logging system's failure.
- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles
  - in case of password based authentication:
    - the change of the number of permitted unsuccessful attempts
    - reaching the limit of the permitted number of the unsuccessful login attempts in case of user login
    - readmission of the user blocked because of the unsuccessful login attempts
  - changing the authentication technique (for example from password based to PKI based).
- KEY MANAGEMENT:

  - all events for the entire life cycle of service keys (key generation, saving, loading, destruction etc.)

<not TLS:

  - events related to generating, managing the user keys
  - all events related to the management of private keys stored for any purpose by the Certification Service Provider.

>

- CERTIFICATE MANAGEMENT:
  - every event related to the issuance and the status change of the provider Certificates
  - every request including Certificate issuance, re-key, <not TLS: suspension, > key renewal and revocation
  - events related to the request processing

<TLS:

  - all control activities undertaken in relation to the issuance of Certificates, including the time of the telephone conversations related to the verification, the telephone number, the name of the called person and the acquired information

>
<not TLS:

  - every verification activity performed related to the Certificate issuance.

>

  - approval or rejection of the Certificate Applications
  - Certificate issuance or status change.
- DATA FLOWS:
  - any kind of security-critical data manually entered into the system
  - security-relevant data, messages received by the system
- CA CONFIGURATION:
  - re-parameterization, any change of the settings of any component, of the CA
  - user admission, deletion
  - changing the user roles, rights
  - changing the Certificate profile
  - changing the CRL profile
  - generation of a new CRL list
  - generation of an OCSP response

  - Time Stamp generation
  - exceeding the required time accuracy threshold.

- Hardware Security Module:
  - installing Hardware Security Module
  - removing Hardware Security Module
  - disposing, destructing Hardware Security Module
  - delivering Hardware Security Module
  - clearing (resetting) Hardware Security Module
  - uploading keys, certificates to the Hardware Security Module.

- ROUTER AND FIREWALL
  - successful and unsuccessful login attempts
  - administrative actions, including configuration changes, firmware updates and access control modifications
  - changes made to rules, including additions, modifications and deletions
  - system events and errors, including hardware failures, software crashes and system restarts.

- CONFIGURATION CHANGE:
  - hardware
  - software
  - operating system
  - patch
  - installation, update and removal of software on a Certificate System

- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the system components used for providing the trust service
  - access to a system component used for providing the trust service
  - a known or suspected breach of physical security
  - firewall or router traffic.

- OPERATIONAL ANOMALIES:
  - system crash, hardware failure
  - software failures
  - software integrity validation error
  - incorrect or wrongly addressed messages
  - network attacks, attack attempts

  - equipment failure
  - electric power malfunctions
  - uninterruptible power supply error
  - an essential network service access error
  - violation of the Certification Practice Statement
  - deletion of the operating system clock.
- OTHER EVENTS:
  - appointment of a person to a security role
  - operating system installation
  - PKI application installation
  - initiation of a system
  - entry attempt to the PKI application
  - password modification, setting attempt
  - saving the inner database, and restore from a backup
  - file operations (for example creating, renaming, moving)
  - database access.

5.4.2 Frequency of Audit Log Processing

The independent system auditors of the Certification Service Provider evaluates the generated log files every working day.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the Certification Service Provider uses automated evaluation tools too, that are used to monitor the resulting log entries according to preset criteria and, where necessary, alert the operational staff.

The notifications received from the automated evaluation tools are processed and evaluated by the experts of the IT operation within 24 hours.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the online system, the logs are archived and their secure preservation is ensured by the Certification Service Provider for the amount of time defined in Section 5.5.2, but at least 10 years from the date of their creation.

For that time period, the Certification Service Provider ensures the readability of archived data and maintains the software and hardware tools necessary for that.

5.4.4 Protection of Audit Log

The Certification Service Provider protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

- protection against unauthorized disclosure: only authorized persons – primarily the independent system auditors – access the logs
- availability: authorized persons are granted access to the logs
- integrity: any data alteration, deletion in the log files and change in the order of the entries, etc. is prevented.

The Certification Service Provider provides the log records with qualified Time Stamps, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the Certification Service Provider makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The Certification Service Provider verifies the accesses in a secure way. The Certification Service Provider preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

5.4.5 Audit Log Backup Procedures

Daily log files are created from the continuously generated log entries during the operation in each system.

The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups shall be defined in the backup regulations of the Certification Service Provider.

5.4.6 Audit Collection System (Internal vs External)

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas are suspended by the Certification Service Provider until the incident is resolved.

5.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary, the Certification Service Provider involves them in the investigation of the event. The Clients affected by triggering the event has the duty to cooperate with the Certification Service Provider to explore the event.

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the Certification Service Provider monitor the publicly available information about possible vulnerabilities and the new software patches. They analyze the information, classify the vulnerability and if necessary, inform the management about the result and propose an action plan to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat within a period of 48 hours after its discovery, but at least once a year the experts of the Certification Service Provider perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access, and may affect the Certificate issuing process, or allow modification of the data stored in the Certificate.

Based on the results of the analysis the Certification Service Provider

- creates and implements a plan to mitigate the vulnerability or
- documents the factual basis for the decision that the residual risk is accepted and the vulnerability does not require remediation.

At first the new software versions and software patches are installed on the test system of the Certification Service Provider and only after the successfully finished test are installed on the live system which is used to provide the services.

The new software patches are not installed on the live system if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reasons for not applying any security patches are documented.

5.5 Records Archival

5.5.1 Types of Records Archived

The Certification Service Provider is prepared to the proper secure long-term archiving of electronic and paper documents.

The Certification Service Provider archives the following types of information:

- every document related to the accreditation of the Certification Service Provider
- all issued versions of the Certificate Policies
- all issued versions of the Certification Practice Statements
- all issued versions of the General Terms and Conditions
- contracts related to the operation of the Certification Service Provider
- all information related to the registration, including:
  - every document handed in with the Certificate Application
  - the identification data of the document(s) presented during the personal identification

  - service agreement(s)
  - other subscriber disclaimers
  - the ID of the administrator assessing the registration application
  - conditions and the results of the examination of the application
- all information related to the Certificate for the whole life-cycle

<ALA:

- information related to the impersonation of the Electronic Signature or Seal Creation Device

>
<BEL:

- information related to the impersonation of the Electronic Signature or Seal Creation Device

>

- every electronic and paper based log entry.

5.5.2 Retention Period for Archive

The Certification Service Provider preserves the archived data for the time periods below:

- the Certificate Policy for at least 10 years from the date of repeal
- Certification Practice Statement for at least 10 years from the date of repeal
- General Terms and Conditions for at least 10 years from the date of repeal
- in the case of video identification, all communications recorded during the identification for at least 10 years from the date of recording
- All electronic and/or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate

  <ALA:

  - until the completion of the dispute concerning the electronic signature generated with the certificate

  >
  <BEL:

  - until the completion of the dispute concerning the electronic seal generated with the certificate

  >
- all other documents to be archived for at least 10 years from the date of their creation.

5.5.3 Protection of Archive

The Certification Service Provider stores all archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper based copy of the document available.

Each of the two locations fulfils the requirements for archiving security and other requirements.

During the preservation of the archived data, it is ensured that:

- their integrity is preserved
- they are protected against unauthorized access
- they are available
- they preserve authenticity.

The archived electronic data is provided with at least an advanced electronic signature or seal and a qualified Time Stamp.

5.5.4 Archive Backup Procedures

The Certification Service Provider makes an authentic electronic copy of the original paper documents in accordance with the relevant legislation.

Electronic copies are stored according to the same rules as other protected electronic documents.

After archiving the authentic electronic copies the Certification Service Provider may destroy the original paper documents.

5.5.5 Requirements for Time Stamping of Records

Every electronic log entry is provided with a time mark, on which the system provided time is indicated at least to one second precision.

The time value is given by the internal clock of the Certification Service Provider which is synchronized to two separate Stratum-1 UTC time sources:

- one accurate time source uses the satellite-based GNSS (GPS and Galileo) system
- the other accurate time source is based on the longwave time signal service (DCF77).

In order to provide accuracy, the Certification Service Provider synchronizes its own internal time with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization at least 4 times a day.

This way the Certification Service Provider guarantees that the deviation of the time indicated in the time marks from the UTC time base is at most 1 second.

The Certification Service Provider provides the daily log files with a qualified Time Stamp.

During the preservation of the archived data, if necessary (for example algorithm change expiration of the original Time Stamp) the authenticity of the data is ensured.

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the Certification Service Provider's protected computer system, and only the log files that are electronically signed and protected with qualified time stamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the Certification Service Provider in an inner data storage operated by it.

5.5.7 Procedures to Obtain and Verify Archive Information

The Certification Service Provider creates the log files manually or automatically. In case of an automatic logging system, the certified log files are generated daily.

The archived files are protected from unauthorized access.

Controlled access to the archived data is only available to the eligible persons:

- Clients are eligible to see the data stored about them
- in legal litigation in order to provide evidence the necessary data shall be provided.

5.6 CA Key Changeover

The Certification Service Provider ensures that the used Certification Units are continuously possessing a valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it generates a new key pair for the Certification Units and inform its Clients in time. The new provider key is generated and managed according to this regulation.

If the Certification Service Provider changes any of its end-user Certificates issuer provider Certificate keys, it complies with the following requirements:

- it discloses the affected Certificates and public keys in accordance with the requirements defined in section 2.2
- after the provider re-key the end-user Certificates to be issued will only be signed with the new provider keys
- it preserves its old Certificates and public keys, and makes available the <not SEA: seal> <BEL: signature> verification until all of the <ALA: signing Certificate > <BEL: sealing Certificate > with the old provider key validity time expire.

5.7 Compromise and Disaster Recovery

In case of a disaster, the Certification Service Provider takes all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it takes the necessary amendments, corrective measures to prevent future occurrence of the incident.

<not UNI:

Once the problem resolved, the event is reported to the National Media and Infocommunications Authority, as the supervisory authority.

>

<UNI:

Once the problem resolved, the event is reported – depending on the severity – within 24 hours to every organization, towards which such a requirement exists.

>

5.7.1 Incident and Compromise Handling Procedures

The Certification Service Provider has a business continuity plan.

The Certification Service Provider established and maintains a fully functional backup system, which is at a safe distance from the primary location, geographically located at a different place and is independently capable of supplying the full range of services.

The Certification Service Provider annually tests the changeover to a backup system and reviews its business continuity plans.

The Certification Service Provider has increased security tools and systems in order to minimize the software and hardware failures and data corruptions. The recoverability of services is guaranteed by the underpinning contracts and own backup tools of the Certification Service Provider.

[[QUA:

The Certification Service Provider constructed its IT system providing the trust services in such a way that in case of the dropout of any one device, it is able to continue the provision of its trust services. If multiple units of the Certification Service Provider fail, the Certification Service Provider is able to launch its backup system within at most 3 hours, which is able to provide the services related to the continuously operating services – Certificate storage publication, <not TLS: suspension and> revocation management, publication of revocation status information – of the Certification Service Provider for its Clients.

]]

The internal policies of the Certification Service Provider define in detail the tasks related to the management of security incidents. Any deviation from normal operation is recorded in the internal task management system after detection. Upon detection of a discrepancy, the Certification Service Provider shall immediately begin the investigation of the discrepancy, eliminate the detected discrepancy as soon as possible and, if necessary, take preventive measures to prevent the recurrence of the discrepancy.

In all cases, the Certification Service Provider classifies any discrepancy that may affect the availability, integrity or confidentiality of the services as a security incident and prioritizes it (e.g. service interruption).

According to Commission Implementing Regulation 2024/2690 [5], the Certification Service Provider determines the severity of the incident based on, among other things, the duration of the outage, the nature of the service affected, the number of customers, and the repetition of the error.

<not UNI:

The Certification Service Provider shall officially notify the National Media and Infocommunications Authority of service outages and security incidents deemed serious within 24 hours of the occurrence of the incident.

>

<TLS:

In the event of a security incident, the Certification Service Provider creates an incident report in the Mozilla Bugzilla system in accordance with the requirements of the trusted root certificate programs, in which it describes in detail the circumstances of the security incident, the root causes, the affected Certificates, the immediate measures taken to eliminate the incident and the longer-term measures in order the prevention of further incidents. >

The Certification Service Provider reviews the security incidents of the past period at least once a year and examines whether the measures taken are adequate to prevent the recurrence of the error. The findings of the investigation are recorded in a report.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The IT systems of the Certification Service Provider are built of reliable hardware and software components. The critical functions are implemented using redundant system elements so that in the event of an item failure they are able to operate further.

The Certification Service Provider makes a full daily backup of its databases and the generated log events.

The Certification Service Provider makes full system backups as frequently as necessary to be able to restore the full service in case of a disaster.

The business continuity plan of the Certification Service Provider includes accurate requirements for the tasks to be performed in case of critical system component failure.

Once the problem resolved and the integrity restored, the Certification Service Provider restarts its services as soon as possible.

During the restoration of services, the certificate status information service systems have top priority.

5.7.3 Entity Private Key Compromise Procedures

The Business Continuity Plan of the Certification Service Provider has an action plan in place in case the provider private keys compromise. The action plan reveals the circumstances of the compromise besides the revocation of the provider public key and the Certificate accompanying, arranges the notification of all concerned parties, takes the necessary steps against the recurrence of the compromise and, if necessary, provides new key to the service unit and the compromise affected end users. The Certification Service Provider immediately ceases to use that particular key in case of certification unit key compromise.

In case another certification authority also issued Certificate for the given certification unit - by law, contract or agreement between CAs based - and over or cross certified this certification unit of the Certification Service Provider, the Certification Service Provider promptly informs that other Certification Authority for that given key compromise and initiates the certificate revocation belonging to the key in question. <not TLS:

In case of the key compromise of the intermediate CA issuing Certificates for the public administration this means the notification of the KGYHSZ.

>

The Certification Service Provider publishes a notice about the provider public key revocation according to the section 1.3.1

5.7.4 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster are defined in the Certification Service Provider's business continuity plan.

In the event of disaster, the regulations come into force, the damage control and the restoration of the services begins.

The secondary services site is located at a distance from the primary site such that a probable disaster cannot affect both locations at the same time.

The Certification Service Provider is obliged to notify the affected users as quickly as possible in the event of the disaster.

After the restoration of the services, the Certification Service Provider restores its devices damaged during the disaster and the original service security level as quickly as possible.

<TLS:

5.7.5 Mass Revocation Plan

The Certification Service Provider has a comprehensive Mass Revocation Plan to ensure a well-coordinated, rapid, and effective response to a Mass Revocation Event while maintaining compliance and minimizing disruptions. At least yearly,

- all relevant team members undergoes training on mass revocation response procedures
- testing exercises are conducted to evaluate readiness
- mass revocation plan is reviewed and improved if necessary.

The Mass Revocation Plan itself, and the documented results of the testing exercises are assessed by our independent auditor as part of the normal yearly conformity assessment.

>

5.8 CA or RA Termination

In the event of the planned termination of the service, the Certification Service Provider notifies the end users and the National Media and Infocommunications Authority at least 3 months prior to the termination of the service.

The Certification Service and Certificate Status Service Termination

At the same time with the notification about the service termination, the Certification Service Provider shuts down the following services:

- registration
- Certificate creation
- Certificate issuance
- Certificate renewal
- Certificate modification
- re-key.

The Certification Service Provider at least 20 days before the planned termination, but at least 14 days after the notification of the Clients :

- revokes all valid end-user Certificates
- stop processing the revocation <not TLS: and suspension> requests
- terminates the regular issuance of the Certificate Revocation Lists
- issues a closing Certificate Revocation List, in which the value of the "nextUpdate" field is "99991231235959Z".

At the same time of the termination, the Certification Service Provider shuts down the following services:

- Certificate publishing
- Certificate revocation status publishing
- OCSP service
- technical support
- information provision.

Before a planned termination, the Certification Service Provider engages in negotiations about the taking over of its services with other Trust Service Provider whose rating is identical to its own. Under section 9.3, it will hand over its records, including confidential user data, to such a Trust Service Provider or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.

The Certification Service Provider takes measures concerning the revocation of provider Certificates (and destroying private keys) during the 3 months period – depending on the outcome of the negotiations.

The Certification Service Provider informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The Certification Service Provider is to inform its Clients by electronic mail, and Relying Parties by means of a publication via its website.

The Certification Service Provider will publish an announcement about the shutdown of active root certification units at least 5 days before the termination in accordance with chapter 2.1.

The Certification Service Provider destroys the private keys of the terminated root certification units within 5 working days after the termination in a documented manner.

Upon termination the service, the Certification Service Provider produces a full scope backup of its data contained in its IT system, protected by a qualified Time Stamp.

The Certification Service Provider provides for authorised Relying Parties the possibility to interpret the data appearing in its revoked <not TLS: and suspended> Certificates records if necessary.

In order to make the handing over of its data to another Trust Service Provider possible, the Certification Service Provider places data on media and in a format which the new Trust Service Provider can receive or provides the new Trust Service Provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this.

6 Technical Security Controls

The Certification Service Provider uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The Certification Service Provider manages the provider cryptographic private keys during their whole life-cycle within a Hardware Security Module that has appropriate Certification.

Both the Certification Service Provider and the system supplier and execution contractors have significant experience with deployment of PKI based systems and trust services and they use internationally recognized technology.

The Certification Service Provider continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

6.1 Key Pair Generation and Installation

The Certification Service Provider makes sure that the generation and management of all the private keys generated by it – <not TLS: for the Subjects,> for itself and for some of its departments (for example Certificate Repository, Registration Authority) – is secure and complies with the regulatory requirements in force and with industry standards.

6.1.1 Key Pair Generation

The Certification Service Provider uses key generation algorithms for the key pair generation, which comply with the requirements set out in the following normative:

- ETSI TS 119 312 [30]

<TLS:

- CABF Baseline Requirements recommendation [63]

>

- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2023. Act CIII [13] 96. § (1) b).

Generation of Service Provider's key pairs

The Certification Service Provider in case of the generation of a key pair of its own will ensure:

- The production of provider key pair is performed based on a key generation script.
- In case of a CA key pair generation a Qualified Auditor witness the CA key pair generation process or the Certification Service Provider records a video of the entire CA key pair generation process.
- If the CA key pair is generated for a root CA or a subordinate CA operated by another organization, a qualified auditor will witness the key generation process.

  The Qualified Auditor issues a report opining that the CA followed its key ceremony during its Key generation process and the controls used to ensure the integrity and confidentiality of the key pair.
- The generation of the key pair is (see section 5.1), with at least two trusted role holder (see section 5.2.1) authorized person simultaneously under the principle of split knowledge, excluding the presence of unauthorized persons.
- The creation of the provider key pair is carried out in a device, that:
  - meets the requirements of ISO/IEC 19790 [38], or
  - meets the requirements of FIPS 140-2 [69] level 3 or higher, or
  - meets the requirements of FIPS 140-3 [70] level 3 or higher, or
  - meets the requirements of CEN 419 221-5 [35], or
  - is a reliable system that is evaluated in accordance with ISO/IEC 15408 [37] or equal security criteria valued to level 4 or higher guarantee level. The assessment shall be based on a security system design or on safety appropriations meeting the requirements of this document.
- Detailed log entries are made about the key generation process.
- The Certification Service Provider takes the necessary measures to ensure that the private key has been generated and protected in accordance with the prescribed processes during key generation.
- In case of generating key pairs for Service Provider's root and intermediate Certificate the Certification Service Provider shall make a key generation record demonstrating that the process has been conducted in accordance with the predetermined workflow that ensures the confidentiality and integrity of the generated keys. The record shall be signed by:

  - in case of the generation of the Service Provider's root certification unit's key pair the trusted officer of the Certification Service Provider responsible for key management and a trusted person independent from the operation of the Certification Service Provider, as a witness (eg. qualified auditor), who verifies that the record corresponds to the performed process
  - in case of the generation of the Service Provider's intermediate certification unit's key pair the trusted officer of the Trust Service Provider responsible for key management who verifies that the record corresponds to the performed process.

- the generated keys are recorded in the key registry, where the "SHA-256" fingerprint of the public key is also recorded for unambiguous identification. The key registry will contain and track the entire lifecycle of all keys from their creation, without time limit, including keys for which a certificate has not yet been issued (parking keys).

Generation of Service Provider's infrastructure key pairs

In case of generating the infrastructure keys used in its own IT systems, the Certification Service Provider ensures that:

- the generation of the Certification Service Provider's infrastructure key is carried out in a physically protected environment (see section 5.1) by an authorized person in a role of trust (see section 5.2.1), excluding the presence of other unauthorized persons
- the key generation fully complies with the instructions in the device user documentation.

Subscriber's key pairs

<TLS:
The Certification Service Provider never generates keypairs for the end-user Certificates.
>
<not TLS:
<not UNI:
In case of generating the key pair for the Subjects, the Certification Service Provider ensures that:

- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.

[[QUA:

- **In case of Certificate Policies requiring the use of a Qualified Electronic Signature or Seal Creation Device or a Cryptographic Hardware Device the Certification Service Provider generates the private key on the Subject or Applicant's Qualified Electronic Signature or Seal Creation Device or Cryptographic Hardware Device which makes the disclosure of the private key impossible.**

]]

- The Certification Service Provider never generates keypairs for software based end-user Certificates.
- The Certification Service Provider ensures that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6, and the private key is not one of a known weak key pair.

[[QUA:

- **If the private key is handed over to the Subject, the Qualified Electronic Signature or Seal Creation Device or the Cryptographic Hardware Device is stored in an adequately secure environment by the Certification Service Provider to prevent the key compromise. The generated private keys are stored by the Certification Service Provider until the documented key handover in an adequately secure environment to prevent disclosure.**

]]

> >

<UNI: In case of the generation of the key pair generated for the Subjects by the Certification Service Provider, it ensures that:

- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.
- In case of Certificate Policies requiring the use of a Cryptographic Hardware Device the Certification Service Provider generates the private key on the user's Cryptographic Hardware Device which makes the disclosure of the private key impossible.
- The Certification Service Provider ensures that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6, and the private key is not one of a known weak key pair.
- After the documented handover of the private key to the Subject or Applicant the Certification Service Provider destroys every copy of the handed over private key stored by it – except the encryption keys which will be put to the key escrow service – in such a way that its restoration and usage becomes impossible.

>

In case of an Subject or Applicant generated key pair:

- the production of keys shall be done in a properly secure environment that is under the supervision of the Subject or Applicant
- the Subject or Applicant shall ensure the proper protection of the generated private key
- the Certification Service Provider shall ensure that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6, and the public key is not one of a known weak key pair.

During processing the Certificate Application the Certification Service Provider checks the key pair and rejects the Certificate Application, if one or more of the following conditions are met:

- the key pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6
- there is clear evidence that the specific method used to generate the private key was flawed
- the Certification Service Provider is aware of a demonstrated or proven method that exposes the Subject or Applicant's private key to compromise
- the Certification Service Provider has previously been made aware that the Subject or Applicant's private key has suffered a key compromise, such as through the provisions of Section 4.9.1
- the Certification Service Provider is aware of a demonstrated or proven method to easily compute the Subject or Applicant's private key based on the public key, such as
  - a Debian weak key, see `https://wiki.debian.org/SSLkeys`
  - ROCA vulnerability, see `https://github.com/crocs-muni/roca`
  - Close Primes vulnerability, see `https://fermatattack.secvuln.info/`

6.1.2 Private Key Delivery to Subscriber

<TLS:
The Certification Service Provider never generates keypairs for the end-user Certificates.
>
<not TLS: <not UNI: If the Certification Service Provider generated the Subject's private key, then the following requirements are met:

[[QUA:
If the Private Key is Handed Over to the Subject:

- **Until the key handover, the Certification Service Provider stores the private keys generated by it for the Subjects and the activation data securely to prevent the key disclosure, copy, modification, damage and the usage by unauthorized persons.**
- **The Certification Service Provider shall ensure that the private keys and their activation data can only be taken over by the Subject or Applicant.**
- **The Certification Service Provider shall gain sufficient evidence of the handover of the private key to the Subject or Applicant, and the exact time of the handover.**
- **After the handover of the signer private key to Subject or Applicant, the Certification Service Provider shall not reserve any copy of the signer private key.**

In case of Certificate Policies requiring the use of a Cryptographic Hardware Device (in particular Qualified Electronic Signature or Seal Creation Device) the private key of the Subject together with the Cryptographic Hardware Device providing the secure storage and usage of the private key, is handed over to the Subject or Applicant in person with the closed envelope containing the activation code.

The Certification Service Provider may also provide the Cryptographic Hardware Device to the Subject or Applicant using a third party, in which case it shall ensure that

- **the Cryptographic Hardware Device is in transport mode until handed over to the Subject or Applicant**
- **transmits the device activation code to the Subject or Applicant on a separate channel**
- **the Certificate(s) shall be issued only after the certified handover of the Cryptographic Hardware Device to the Subject or Applicant.**

Following the key generation the Qualified Electronic Signature or Seal Creation Device containing the private key is in transport mode, which ensures that the private key can not be used for electronic signature creation before the activation of the Qualified Electronic Signature or Seal Creation Device.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device or Qualified Electronic Signature or Seal Creation Device in all cases the Client generates the private key, so it does not have to be delivered to the Client.

]]

[[ADV:

When the Certificate is issued for software based keys in all cases the Client generates the private key, so it does not have to be delivered to the Client.

]]

> >

<UNI:

If the Certification Service Provider generated the Subject's private key, then the following requirements are met:

- Until the key handover, the Certification Service Provider stores the private keys generated by it for the Subjects and the activation data securely to prevent the key disclosure, copy, modification, damage and the usage by unauthorized persons.
- The Certification Service Provider shall ensure that the private keys and their activation data can only be taken over by the Subject or Applicant.
- The Certification Service Provider shall gain sufficient evidence of the handover of the private key to the Subject or Applicant, and the exact time of the handover.
- After the handover of the signer private key to Subject or Applicant, the Certification Service Provider shall not reserve any copy of the signer private key.

In case of Certificate Policies requiring the use of a Cryptographic Hardware Device the private key of the Subject together with the Cryptographic Hardware Device providing the secure storage and usage of the private key, is handed over to the Subject or Applicant in person with the closed envelope containing the activation code.

The Certification Service Provider may also provide the Cryptographic Hardware Device to the Subject or Applicant using a third party, in which case it shall ensure that

- the Cryptographic Hardware Device is in transport mode until handed over to the Subject or Applicant
- transmits the device activation code to the Subject or Applicant on a separate channel
- the Certificate(s) shall be issued only after the certified handover of the Cryptographic Hardware Device to the Subject or Applicant.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device, in all cases the Client generates the private key, so it does not have to be delivered to the Client.

>

6.1.3 Public Key Delivery to Certificate Issuer

When the key pair is generated by the Subject or Applicant, the following provisions shall be complied with:

- the public key shall be sent to the Certification Service Provider in a manner that it can be unambiguously assigned to the Subject or Applicant
- the Certificate Application process shall prove that the Subject or Applicant really owns the private key corresponding to the public key.

When the end user keys generated by the Subject or Applicant, the Subject or Applicant sends the Certification Service Provider a PKCS#10 formatted Certificate Application which he or she signs with the private key belonging to the public key to be indicated on the Certificate. The PKCS#10 formatted Certificate Application contains the public key generated by the Subject or Applicant and the Subject data to be indicated on the Certificate, so both requirements are met.

<not TLS:

The Certification Service Provider issues the provider Certificates needed for his trust services himself and generates the provider key pairs himself also, so there is not necessary to deliver the public keys. In case of the provider Certificate issued by another service provider – for example KGYHSZ –, the Certification Service Provider sends to the issuer a PKCS#10 formatted Certificate Application, which is certified with the private key belonging to the public key to be indicated on the Certificate.

>

6.1.4 CA Public Key Delivery to Relying Parties

The Certification Service Provider discloses the status information related to the provider Certificates for the Relying Parties by the following methods:

- The Certification Service Provider publishes the full provider certificate hierarchy containing every root and intermediate provider certificate from which every current provider Certificate is downloadable (see at the Provider certificates point at the

  `https://e-szigno.hu/certification-of-qscd-devices`

  url).

- The denomination of the root and intermediate certification units and the Root Certificates' hash is in the 1.3.1 section of the Certification Practice Statement.
- The Certificates of the intermediate certification units are published on the certified Hungarian Trust Service Provider List [75] maintained and published by the National Media and Infocommunications Authority within the framework of the European common regulations [74]. The list contains every provider certificate (even the expired and revoked ones).
- For the online certificate status response signer responders the Certification Service Provider – according to the best international practice – issues Certificates with very short validity periods, thus eliminating the necessity of checking the revocation status of the Certificates. The current status of the Certificates is continuously available via the website of the Certification Service Provider at the

  `https://e-szigno.hu/ca-certificates`

  address.

The Certification Service Provider discloses for the Relying Parties the status information related to the Certificate of the certification units operated by it, and of the units that take part in the online certificate status service by the following methods:

- The status information related to the Certificate of the root certification units is available via the website of the Certification Service Provider.
- The status change information of the intermediate (not root) certification units' certificates is disclosed on the Certificate Revocation Lists, via its website and within the confines of the online certificate status response service.
- For the responders signing the online certificate status responses the Certification Service Provider – according to the best international practices – issues a Certificate with very short validity period to eliminate the necessity of checking the Certificate revocation status. The Certification Service Provider guarantees that in case of key compromise or other problem no new Certificate will be issued for the old private key signing the OCSP responses . The Certification Service Provider issues the OCSP response Certificates for new, secure private keys.

Regarding the disclosure methods of the status information, also see Section 4.10.

6.1.5 Key Sizes

The Certification Service Provider uses cryptographic algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [30]

<TLS:

- CABF Baseline Requirements recommendation [63]

>

- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2023. Act CIII [13] 96. § (1) b)

The Certification Authority uses at least 2048-bit RSA keys or at least 256-bit ECC keys in every currently active root and intermediate provider Certificate.

The Certification Authority uses at least 3072-bit RSA keys or at least 256-bit ECC keys in the Certificates of the Time Stamping Units and the OCSP responders.

The Certification Authority issues the end-user Certificates

- in case of ECC keys, for at least 256-bit ECC key
- in case of RSA keys, for at least 2048-bit or 3072-bit RSA key, depending on the type of the Certificate

[[ADV:

<not TLS: <not UNI:

The Certification Authority issues the Time Stamping Unit Certificates only for at least 3072-bit RSA keys or at least 256-bit ECC keys.

The Certification Authority issues Time Stamping Unit's Certificates for Code Signing purposes only from subordinate CA units with at least 4096-bit RSA keys or at least 256-bit ECC keys under the "e-Szigno Root CA 2017".

>>

<UNI:

The Certification Authority issues the Code Signing Certificates and the Time Stamping Unit Certificates only for 3072- or 4096-bit RSA keys or at least 256-bit ECC keys.

The Certification Authority issues Code Signing Certificates and Time Stamping Unit's Certificates for Code Signing purposes only from subordinate CA units with 4096-bit RSA keys or at least 256-bit ECC keys under the "e-Szigno Root CA 2017".

>

]]

<BEL:

[[QUA:

The Certification Authority issues the Time Stamping Unit's Certificates only for at least 3072-bit RSA keys or at least 256-bit ECC keys.

The Certification Authority issues Time Stamping Unit's Certificates for Code Signing purposes only from subordinate CA units with at least 4096-bit RSA keys or at least 256-bit ECC keys under the "e-Szigno Root CA 2017".

]]

>

The Certification Service Provider supports only the following RSA keylengths:

- RSA-2048 (2048 bit)
- RSA-3072 (3072 bit)

- RSA-4096 (4096 bit)

The Certification Service Provider supports only the following ECC curves:

- ECC NIST P-256 (256 bit)
- ECC NIST P-384 (384 bit)
- ECC NIST P-521 (521 bit)

The ECC key always represents a valid point on the supported elliptic curve.

6.1.6 Public Key Parameters Generation and Quality Checking

The Certification Service Provider generates the keys according to the description of the section 6.1.1.

Verification of Compliance of Parameters

A Certification Authority verifies the compliance of each service provider's and end-user's key before the Certificate issuance to the following parameters:

1. in case of RSA keys
    - RSA keylength is within the supported values
    - RSA exponent is odd
    - the value of the RSA exponent is at least "(2 exp 16)+1" and at most "(2 exp 256)-1"
    - the modulus is odd, not a prime power and it does not have a divider smaller than 752
2. in case of ECC keys
    - the key is a valid point in a supported curve (ECC Full Public-Key Validation Routine as defined in section 5.6.2.3.3 of NIST Special Publication 800-56A Revision 3 [71])

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The Certification Service Provider root certification unit private key may only be used for the following purposes:

- issuance of the self-signed Certificate of the root certification unit itself
- to sign the intermediate certification units' Certificates
- to sign the OCSP responder Certificate
- to sign CRLs.

The private key of the Certification Service Provider's intermediate certification units – as well as the private key issued to the intermediate certification unit of other organizations – can only be used for the following purposes:

- to sign the intermediate certification units' Certificates
- to sign the end user Certificate
- to sign the Time Stamping Unit Certificate
- to sign the OCSP responder Certificate
- to sign CRLs.

The Certification Service Provider includes the "Key Usage" extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [60] compatible applications technically restrict the usage of the Certificates. The requirements set out for the value of the field are in Section 7.1.2.

<TLS:

The private key of the Applicant belonging to its Certificate may only be used for webserver or - if the Website Authentication Certificate makes it possible - client authentication, and any other usage is not permitted.

>

<ALA:

The signer private key may only be used for electronic signature creation by the creator of the electronic signature or seal, any other uses of the key are specifically prohibited.

>

<BEL:

The seal private key may only be used for electronic seal creation by the creator of the electronic signature or seal, any other uses of the key are specifically prohibited.

[[QUA: The private keys of the Time Stamping Units may only be used for the certification of the Time Stamps.]]

>

<UNI:

The private key of the Subject belonging to its Certificate may only be used according to the key usage in the Certificate, any other usage is not permitted.

>

The private keys of the OSCP Responders may only be used for the certification of the OCSP Responses.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Certification Service Provider ensures the secure management of the private keys held by it and prevents the private key disclosure, copy, deletion, modification and unauthorized usage. The Certification Service Provider may only preserve the private keys as long as the provision of the service definitely requires.

The Certification Service Provider stores and uses the private keys of the Root CAs <UNI: and the Subordinate CAs used for issuing TSU Certificates for codesigning > logically and physically

isolated from normal operations such that only designated trusted personnel have access to the keys for use.

The Certification Service Provider stores the private keys used for Certificate issuance at a physically secure location, in a secure Hardware Security Module.

The Certification Service Provider deletes the signing private keys stored in the decommissioned Hardware Security Modules in the manner specified in the device's user manual, after which it is practically impossible to restore the keys.

<TLS:

The Certification Service Provider doesn't generate keypairs for the Subject or Applicant, eliminating the need to ensure the preservation of the end-user private keys.

>

<not TLS:

The Certification Service Provider the Qualified Electronic Signature or Seal Creation Devices used to create Certificates issued according to Certificate Policies requiring the use of a Qualified Electronic Signature or Seal Creation Device stores at a physically secure location, with special attention in order to prevent the illegal use of private keys after the on-board key generation until handing over to the Subject.

In case of Certificates issued according to Certificate Policies not requiring the use of a Qualified Electronic Signature or Seal Creation Device the Certification Service Provider does not issue private keys to the Subject beforehand, eliminating the need to ensure the preservation of the end-user private keys.

>

6.2.1 Cryptographic Module Standards and Controls

The systems of the Certification Service Provider issuing Certificate, signing OCSP responses and CRL lists store the private keys in such secure hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [38], or
- the requirements of FIPS 140-2 [69] level 3 or higher, or
- the requirements of FIPS 140-3 [70] level 3 or higher, or
- the requirements of CEN 419 221-5 [35], or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to ISO/IEC 15408 [37] or an equivalent security criteria system. The assessment either shall be based on the appropriate security system plan that meets the requirements of the present document, or on security appropriations.

The Certification Service Provider stores the provider private keys outside of the Hardware Security Module only in encrypted form. Only those algorithms and key parameters are used for encoding which fit to the actual algorithmic decision of the National Media and Infocommunications Authority that was issued according to the year 2023. Act CIII [13] 96. § (1) b) and that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The Certification Service Provider provider private keys are stored in a physically secure site even in an encrypted form, in the safe of the Data Centre, where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the Certification Service Provider destroys the coded keys or recodes them again using algorithm and key parameters that ensure higher protection.

6.2.2 Private Key (N out of M) Multi-Person Control

The Certification Service Provider implements the "n out of m" at the activation of the private key related key management functions. The parameters are determined so that the simultaneous presence of at least two trusted role holder employees is needed for the critical operations carried out with its provider private keys.

6.2.3 Private Key Escrow

The Certification Service Provider does not escrow its provider or end-user private keys.

6.2.4 Private Key Backup

The Certification Service Provider makes security copies of its provider private keys, before putting the provider private key into service as described in section 6.2.1 in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 6.2.2.

The Certification Service Provider stores the backup copy in duplicate, and at least one copy of those is stored at a different place from the service provider location.

The same strict security standards are applied to the management and preservation of backups as for the operation of the production system.

The Certification Service Provider does not make any copy of the end-user private keys.

6.2.5 Private Key Archival

The Certification Service Provider does not archive its private keys and the end-user private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the Certification Service Provider are created in a Hardware Security Module that meets the requirements.

The private keys do not exist in an open form outside of the Hardware Security Module.

The Certification Service Provider only exports the private key from the Hardware Security Module for the purpose of making a secure copy.

The export and loading of the provider private keys is performed according to section 6.2.2.

6.2.7 Private Key Storage on Cryptographic Module

The Certification Service Provider keeps its private keys used for service provision in Hardware Security Modules according to section 6.2.1.

Private keys are stored and used in the Hardware Security Module as specified in the certification of the device with full compliance with the related operating instructions.

<UNI:

The Certification Service Provider issues Code Signing Certificate only for Code Signing Services, when the private keys reside in a Cryptographic Hardware Device conforming to the following requirements:

- the requirements of FIPS 140-2 [69] level 3 or higher, or
- the requirements of FIPS 140-3 [70] level 3 or higher, or
- the requirements of CEN 419 221-5 [35]

The Certification Service Provider issues Code Signing Certificate only, when:

- the Certification Service Provider provides the Electronic Signature or Seal Creation Device with keys, which are pre-generated onboard by the Certification Service Provider
- within the framework of the remote key management service operated by the Certification Service Provider, for keys generated on Hardware Security Module
- the Certification Service Provider relies on a report provided by the Applicant that is signed by an auditor, who is approved by the Certification Service Provider and who has accreditation for eIDAS and ETSI audits, witnesses the Key Pair creation in a suitable Cryptographic Hardware Device solution

>

6.2.8 Method of Activating Private Key

The Certification Service Provider keeps its provider private keys in a secure Hardware Security Module and complies with its user guide and the requirements outlined in the certification documents. The Hardware Security Module can only be activated by the corresponding operator cards and the private keys within the Hardware Security Module can not be used before activating the module. The Certification Service Provider keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the Certification Service Provider.

The Certification Service Provider ensures that signatures can only be created with the private key of the root unit certificate in case of commands issued directly by the trust official duly authorized to do so.

<not TLS:

In case of the end-user private keys generated by the Certification Service Provider it ensures that the private keys and the private key activation data are generated and managed in a properly secure way that excludes the possibility of the unauthorized usage of the private key.

[[QUA:

The Qualified Electronic Signature or Seal Creation Devices or Cryptographic Hardware Devices prepared for the Subject and configured and handed over by the Certification Service Provider to the Subject or Applicant so that:

- **it can be clearly established that the device has not been used <ALA: for electronic signature creation> before the handover**
- **before the use of the private key the Subject or Applicant shall authenticate itself towards the device.**

]]

[[ADV:

<UNI:

In case of the private keys handled over by the Certification Service Provider to the Subject or Applicant on a Cryptographic Hardware Device (like intelligent card or token): and configured and handed over by the Certification Service Provider to the Subject or Applicant so that:

- *it can be clearly established that the device has not been used before the handover*
- *before the use of the private key the Subject or Applicant shall identify itself towards the Cryptographic Hardware Device.*

>

]]

>

In case of Subject or Applicant generated private key the protection of the private key is the Subject or Applicant's full responsibility.

6.2.9 Method of Deactivating Private Key

Provider Private Keys

The private key used by the Certification Service Provider, and managed by the cryptographic devices becomes deactivated if (in a regular or irregular way) the device is removed from active status. This can happen in the following cases:

- the user deactivates the key
- the power supply of the device is interrupted (switched off or power supply problem)
- the device enters an error state.

The private key deactivated like this can not be used until the module is in active state again.

End-User Private Keys

<TLS:

The proper usage of the private keys is the responsibility of the Subject or Applicant.

>

<not TLS:

[[QUA:

In case of Certificate Policies requiring the use of Cryptographic Hardware Device the private keys shall be used in accordance with the requirements defined in the used cryptographic module's user guide and in the certification documents.

The Cryptographic Hardware Device handled over to the Subject ensures that the private keys become deactivated in the following cases:

- **the power supply of the device ceases for any reason**
- **the Subject or Applicant exits the application using the device containing the private key**
- **the Subject or Applicant gives a deactivation (exit) instruction from the application to the device.**

The deactivated key and the Qualified Electronic Signature or Seal Creation Device may only be used <ALA: for electronic signature creation > <BEL: for electronic seal creation > after the re-authentication of the Subject or Applicant.

In case of Certificate Policies not requiring the use of a Qualified Electronic Signature or Seal Creation Device or Cryptographic Hardware Device the proper usage of the private keys is the responsibility of the Subject or Applicant.

]]

<not UNI:

[[ADV:

The proper usage of the softweare based private keys is the responsibility of the Subject or Applicant.

]]

> >

<UNI:

In case of Certificate Policies requiring the use of Cryptographic Hardware Device the private keys shall be used in accordance with the requirements defined in the used cryptographic module's user guide and in the certification documents.

The Cryptographic Hardware Device handed over to the Subject ensures that the private keys become deactivated in the following cases:

- the power supply of the device ceases for any reason
- the Subject or Applicant exits the application that uses the private key

- the Subject or Applicant gives a deactivation (exit) instruction from the application to the device.

The deactivated key and the Cryptographic Hardware Device may only be used after the re-authentication of the Subject or Applicant.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device the proper usage of the private keys is the responsibility of the Subject or Applicant.

>

6.2.10 Method of Destroying Private Key

Provider Private Keys

The discarded, expired or compromised Certification Service Provider's private keys are destroyed in a way that makes further use of the private keys impossible.

The Certification Service Provider destroys the provider private keys stored in the secure Hardware Security Module of the certification organization according to the procedures, requirements defined in the user guide and in the certification documents of the used Hardware Security Module, in the simultaneous presence of two Certification Service Provider employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

The Certification Service Provider destroys each backup copy of the private key in a documented way in such a way that its restoration and usage becomes impossible.

End-User Private Keys

<TLS:

The discarded website authentication private keys of the end-users are recommended to be destroyed.

>

<not TLS:

[[QUA:

The destruction of the discarded signer private keys issued on a Qualified Electronic Signature or Seal Creation Device is possible by the physical destruction of the Qualified Electronic Signature or Seal Creation Device, which is the responsibility of the Subject or Applicant.

For the request of the Client in its presence the Certification Service Provider destroys the Qualified Electronic Signature or Seal Creation Device presented by the Client personally free of charge.

In case of Certificate Policies requiring the use of a Qualified Electronic Signature or Seal Creation Device the obsolete private keys shall be destroyed in accordance with the requirements defined in the used cryptographic module user guide and the certification documents. The compliant destruction of the private keys is the responsibility of the Subject or Applicant.

In case of Certificate Policies requiring the use of a Cryptographic Hardware Device the obsolete private keys shall be destroyed in accordance with the requirements defined in

the used cryptographic module user guide and the certification documents. The compliant destruction of the private keys is the responsibility of the Subject or Applicant.

]]

>

<ALA:

The discarded signer private keys of the end-users are recommended to be destroyed.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device the proper destruction of the private keys is the responsibility of the Subject or Applicant.

>

<BEL:

The discarded seal private keys of the end-users are recommended to be destroyed.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device the proper destruction of the private keys is the responsibility of the Subject or Applicant.

>

<UNI:

In case of Certificate Policies requiring the use of a Cryptographic Hardware Device the obsolete private keys shall be destroyed in accordance with the requirements defined in the used cryptographic module user guide and the certification documents. The compliant destruction of the private keys is the responsibility of the Subject or Applicant.

In case of Certificate Policies not requiring the use of a Cryptographic Hardware Device the proper destruction of the private keys is the responsibility of the Subject or Applicant.

Discarded authentication private keys of the end users are recommended to be disposed however, the encryption private keys are recommended to be preserved so that the previously encrypted documents can be decrypted later.

>

6.2.11 Cryptographic Module Rating

According to the requirements of Section 6.2.1 every provider private key of the Certification Service Provider is stored in a cryptographic module that

- has a certificate according to ISO/IEC 19790 [38], or
- has a certificate according to FIPS 140-2 Level 3 [69], or
- has a certificate according to FIPS 140-3 Level 3 [70], or
- has an at least EAL-4 level Common Criteria [72] based certificate attesting compliance with the requirements of the CEN 419 221-5 [35], or
- has a certificate issued for this purpose by an independent certification body eligible for evaluating electronic signature products, registered by the National Media and Infocommunications Authority, or in a member state of the European Union

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Certification Service Provider archives every issued Certificate for ten years after the end of the validity period or until the completion of the incurred dispute related to the Certificate<ALA: (or to the electronic signature based on the Certificate)><BEL: (or to the electronic seal based on the Certificate)>.

For the same time period, the Certification Service Provider preserves devices, with which the content of the Certificate can be established.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Keys and Certificates of the Root Certification Units

The validity period of the Certification Service Provider root certification unit certificates and the private keys belonging to them shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority.

The validity period of the Certification Service Provider root certification unit certificates and the private keys:

- the key of the "Microsec e-Szigno Root CA" root certification unit was valid until 2017-04-06
- the key of the "e-Szigno OCSP CA" root certification unit was valid until 2017-04-26
- the key of the "Microsec e-Szigno Root CA 2009" root certification unit is valid until 2029-12-30

  Due to the planned phase out of the use of 2048-bit RSA keys - 2028-12-31 according to the currently valid cryptographic requirements - the entire hierarchy will be shut down on schedule before the expiry of the Certificate.
- the key of the "e-Szigno Root CA 2017" root certification unit is valid until 2042-08-22

<TLS:

- the key of the "e-Szigno TLS Root CA 2023" root certification unit is valid until 2038-07-17
- the key of the "e-Szigno TLS Root CA 2024" root certification unit is valid until 2039-07-14
- the key of the "e-Szigno RSA TLS Root CA 2025" root certification unit is valid until 2040-07-29
- The validity period of root certificates created after 2023-09-15 shall be
  - minimum 2.922 days (≙8 years)
  - maximum 9.132 days (≙25 years)

>
<TLS:

- the key of the "e-Szigno Root CA 2024" root certification unit is valid until 2049-07-14

>
<ALA:

- the key of the "e-Szigno SMIME Root CA 2024" root certification unit is valid until 2042-07-14

>
<BEL:

- the key of the "e-Szigno SMIME Root CA 2024" root certification unit is valid until 2042-07-14

>
<UNI:

- the key of the "e-Szigno CodeSigning Root CA 2024" root certification unit is valid until 2039-07-14
- the key of the "e-Szigno TSA Root CA 2024" root certification unit is valid until 2039-07-14
- the key of the "e-Szigno ECC TSA Root CA 2024" root certification unit is valid until 2039-07-14

>

- az "e-Szigno RSA Root CA 2025" root certification unit is valid until 2050-09-05

The Keys and Certificates of the Intermediate Certification Units

The validity period of the Certification Service Provider intermediate certification unit certificates and the private keys belonging to them:

- shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority
- shall not exceed the validity period of the issuer root or intermediate provider Certificate that issued the intermediate provider Certificate.

The intermediate (not root) certification unit keys of the Certification Service Provider are valid until the expiration time of the Certificates belonging to them.

End-User Certificates

The validity period of the end user Certificates issued by the Certification Service Provider
<TLS:

- in case of Certificates used also for public website authentication
  maximum 200 days from the date of issuance

[[QUA:

- **In case of EV Certificate**
  recommended validity is not more than 12 months
- **in case of qualified Certificate**
  maximum 3 years from the date of issuance

]]
>
<not TLS:
[[QUA:

- **is maximum**
  - **825 days (≙27 months) from the date of issuance in case of Email (S/MIME) Certificates**
  - **3 years from the date of issuance in case of other Certificates**

]]
>
<not TLS: <not UNI:
[[ADV:

- *is maximum*
  - *10 years from the date of issuance in case of any Certificates*

]]
> >
<UNI:

- – in case of Code Signing Certificates, maximum 460 days from the date of issuance
  – in case of Email (S/MIME) Certificates, maximum 825 days (≙27 months) from the date of issuance
  – in case of other Certificates, maximum 10 years from the date of issuance

>

- shall not exceed the date until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority
- shall not exceed the expiration date of the provider Certificate that issued the Certificate.

Taking into account the above aspects, the Certification Service Provider issues end-user Certificates with the following validity periods by default:

<TLS:

[[QUA:

- **In case of EV Certificates:**
  365 days (≙12 months) from the date of issuance
- **In case of special purpose qualified Certificates, like PSD2:**
  1095 days (≙3 years) from the date of issuance

]]

[[ADV:

- *198 days from the date of issuance*

]]

>

<not TLS:

[[QUA:

- **– in case of Email (S/MIME) Certificate 824 days (≙27 months) from the date of issuance**
  – in case of other Certificates 1.095 days (≙3 years) from the date of issuance

]]

>

<not TLS: <not UNI:

[[ADV:

1.095 days (≙3 years) from the date of issuance

]]

>>

<UNI:

- – in case of Email (S/MIME) Certificate 824 days (≙27 months) from the date of issuance

- in case of encryption Certificates 2.922 days (≐8 years) from the date of issuance
- in case of client authentication Certificates 2.922 days (≐8 years) from the date of issuance
- in case of other Certificates 1.095 days (≐3 years) from the date of issuance

>

If the Certification Service Provider deviates from the specified values, it will inform the Clients in advance.

<TLS: We would like to draw our customers' attention to the fact that, in accordance with the requirements of the CA/Browser Forum [63], the maximum validity period of newly issued Website Authentication Certificates will be radically reduced in several steps over the coming years, as follows:

- from 2027-03-15, maximum 100 days
- from 2029-03-15, maximum 47 days

Other requirements may necessitate faster implementation or even shorter validities.

The shorter validity period necessitates more frequent certificate replacement, which, due to the increased administrative and operational tasks, justifies a review of certificate management processes, where automation can be introduced.

The Certification Service Provider recommends using standard ACME-based solutions that it also provides.

>

During the Certificate renewal and Certificate modification the Certification Service Provider may issue the new Certificate for the same end-user private key.

<BEL:

Certificates of the Time Stamping Units

The Certification Service Provider may issue special time stamping service provider Certificates based on the request of Time Stamping Service Providers.

The validity period of the Certificates of the Time Stamping Units issued by the Certification Service Provider

- in case of Certificate issued for a qualified Time Stamping Service Provider at most 4.476 days (≐12 years 3 months) from the date of issuance
- in case of Certificate issued for a non qualified Time Stamping Service Provider at most 135 months from the date of issuance
- shall not exceed the end of the implemented cryptographic algorithms and key parameters' validity period
- shall not exceed the expiration date of the provider Certificate that issued the Certificate.

Taking into account the above aspects, the Certification Service Provider issues Certificates for Time Stamping Units with the following validity periods:

- in case of Certificate issued for a qualified Time Stamp Provider 4.475 days (≐12 years 3 months) from the date of issuance
- in case of Certificate issued for a non qualified Time Stamp Provider 4.106 days (≐135 months) from the date of issuance

Life-Cycle of the Time Stamping Keys

The following requirements are met for the private keys used for Time Stamp certification:

- The Time Stamping Service Provider specifies the end of the validity period of the private keys used in the Time Stamping Units at the Certificate request
- the end of the key usage period shall not be a later time than the end of the Certificate validity period
- the end of the validity period is not a later date than the end of the implemented cryptographic algorithms and key parameters' validity period
- the validity period of the Time Stamping Units' is given by setting the "PrivateKeyUsagePeriod" value of the Certificate (see section 7.1.2)

>

Certificates of the OCSP Responder Units

The validity period of the OCSP Responder Certificates issued by the Certification Service Provider

- shall not exceed the end of the implemented cryptographic algorithms and key parameters' validity period
- shall not exceed the time until which the implemented cryptographic algorithms can be used securely according to the decision of the National Media and Infocommunications Authority
- shall not exceed the expiration date of the provider Certificate that issued the Certificate.

For responders signing online certificate status responses, the Certification Authority issues Certificates with an extremely short validity period, in accordance with international best practice, thus eliminating the need to check the Certificate's revocation status. The validity period of the OCSP responder Certificate is <TLS: 24 hours.> <not TLS: 10 minutes.>

The Certification Service Provider automatically renews the Certificate for the same key pair before the Certificate expires.

In the event of key compromise or any other problem, a new Certificate will not be issued for the old private key. The Certification Service Provider then issues OCSP responder Certificates for a new, secure private key.

<not TLS: Exclusively in the case of an intermediate certification unit that issues special Certificates exclusively for Time Stamping Units, in the event of the intermediate certification unit being shut down, the Certification Authority may also issue a long-lived, non-revocable final OCSP responder Certificate, provided that

- the given intermediate certification unit will definitely not issue Time Stamping Unit Certificates in the future
- none of the Time Stamping Unit Certificates previously issued by the given intermediate certification unit can be used to issue a new Time Stamp
- no Time Stamping Unit Certificate is in a suspended or revoked state
- there may be no need to suspend or revoke the Certificates of Time Stamping Units in the future.

The validity of the final OCSP responder Certificate is the same as the validity of the issuing intermediate certification entity Certificate. Until the end of the validity period of the intermediate certification entity Certificate, the OCSP responder entity uses the final OCSP responder Certificate to authenticate OCSP responses. >

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.

If this happens, the Certification Service Provider revokes the related Certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Certification Service Provider's private keys are protected in accordance with the procedures, requirements defined in the used Hardware Security Module user guide and the certification documents.

In case of password based activation data usage, the passwords are sufficiently complex in order to ensure the required level of protection.

<not TLS:

[[QUA:

In case of Qualified Electronic Signature or Seal Creation Devices and Cryptographic Hardware Devices provided by the Certification Service Provider for the Subject or Applicant, the Certification Service Provider provides:

- **the activation data is created and installed to the Qualified Electronic Signature or Seal Creation Devices or to the Cryptographic Hardware Device is generated in a physically secure environment, with an adequate quality random number generator**
- **the activation data to be handed over to the Subject or Applicant using a safe method.**

]]

>

<UNI:

In case of Cryptographic Hardware Devices provided by the Certification Service Provider for the Subject or Applicant, the Certification Service Provider provides:

- the activation data is created and installed to the Cryptographic Hardware Device is generated in a physically secure environment, with an adequate quality random number generator
- the activation data to be handed over to the Subject or Applicant using a safe method.

>

The Certification Service Provider never generates software based private keys for the end user Certificates.

The creation and installation of the activation data of the Subject or Applicant created private keys is the duty of the Subject or Applicant.

6.4.2 Activation Data Protection

The employees of the Certification Service Provider manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

<not TLS:

[[QUA:

In case of Qualified Electronic Signature or Seal Creation Devices or Cryptographic Hardware Devices issued for Subjects or Applicants by the Certification Service Provider:

- **the Certification Service Provider only records the activation data for the purpose of delivering them to the Subject or Applicant**
- **the Certification Service Provider distributes the activation data to the Subjects or Applicants using a secure method.**

]]

>

<UNI:

In case of Cryptographic Hardware Devices issued for Subjects or Applicants by the Certification Service Provider:

- the Certification Service Provider only records the activation data for the purpose of delivering them to the Subject or Applicant
- the Certification Service Provider distributes the activation data to the Subjects or Applicants using a secure method.

>

The protection of the activation data of the private keys created by the Subject or Applicant, is the duty and responsibility of the Subject or Applicant.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the Certification Service Provider ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles
- a log entry is created for every transaction, and the log entries are archived
- for the security-critical processes it is ensured that the internal network domains of the Certification Service Provider are sufficiently protected from unauthorized access
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

6.5.2 Computer Security Rating

Microsec highlights the importance of Client experience. In order to maintain a high level of services, Microsec has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002.

Microsec assigns high priority to the security of the systems it operates and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003.

The scope of both the quality control system and the information security management system covers the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly.

Based on the results of the risk assessment the Certification Service Provider

- sets up new measures to eliminate the vulnerabilities, or/and
- accepts the identified residual risks by stating the reason of the decision.

See:

`https://www.microsec.hu/en/quality-assurance-and-audit`

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Certification Service Provider only uses applications and devices in its production IT system that are:

- commercial boxed software, designed and developed by a documented design methodology, or
- custom hardware and software solutions developed by the Certification Service Provider itself during which design structured development methods and controlled development environment were used, or
- custom hardware and software solutions developed by a reliable party for the Certification Service Provider during which design structured development methods and controlled development environment were used, or
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

Procurement of IT tools is performed in a way that excludes changes to the hardware and software components using reliable, regularly qualified suppliers.

The hardware and software components applied for the provision of services are not used for other purposes by the Certification Service Provider.

The Certification Service Provider prevents the malicious software from entering into the devices used for certification services with appropriate security measures.

The hardware and software components are checked regularly for malicious software prior the first usage, and subsequently.

The Certification Service Provider acts with the same carefulness in case of program update purchases as at the acquisition of the first version.

The Certification Service Provider employs reliable, adequately trained staff over the course of installing software and hardware.

The Certification Service Provider only installs software to its service provider IT equipment necessary for the purpose of service provision.

The Certification Service Provider has a version control system where every change of the IT system is documented.

The Certification Service Provider operates automatic monitoring system to record all unauthorized changes, which records all changes in every file and in case of changes in the monitored files it generates a log entry or sends an alert to the system operators.

6.6.2 Security Management Controls

The Certification Service Provider implements processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system detects any kind of unauthorized changes, data entry that affects the system, the firewall, the routers, programs and other components used in the

service. Installing the program used in the service the Certification Service Provider ensures that the program to be installed is the proper version and that it is free from any unauthorized modification. The Certification Service Provider regularly checks the integrity of the software in its system used in the service.

Each Hardware Security Module applied by the Certification Service Provider has been verified, tested and evaluated. The Certification Service Provider verifies the integrity of the modules:

- following the acquisition of the devices during the takeover
- immediately before the first usage
- regularly during operation.

The Certification Service Provider deletes the provider keys from the Hardware Security Modules permanently or temporarily withdrawn from use.

The Certification Service Provider stores the unused Hardware Security Modules at a physically protected location.

6.6.3 Life Cycle Security Controls

The Certification Service Provider ensures the protection of the used Hardware Security Modules during their whole life cycle.

During the operation of the IT equipment and systems used for the provision of the services, the Certification Service Provider takes into account the security aspects related to the life cycle of the equipment, according to which:

- it uses properly certified Hardware Security Modules in its systems
- ensure, upon receipt of the Hardware Security Modules, that the quality control ensures that that the protection of the Hardware Security Modules against tampering was ensured during transportation
- it stores the Hardware Security Modules in a safe place, and ensure the protection of the Hardware Security Modules against tampering during storage
- continuously complies with the requirements set out in the Hardware Security Module's security target, instructions for use and certification report during operation
- deletes the private keys stored in their decommissioned Hardware Security Modules in such a way that it becomes practically impossible to restore the keys
- handle and dispose of decommissioned Hardware Security Modules in accordance with the requirements of its security target, instructions for use and certification report.

6.7 Network Security Controls

The Certification Service Provider follows industry best practices for securing their networks. It conforms to the CA/B Forum's Network and Certificate System Security Requirements [66].

The Certification Service Provider keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too.

The Certification Service Provider implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system.

The Certification Service Provider checks the authenticity and integrity of every software component at their first loading.

The Certification Service Provider applies proper network security measures for example:

- divides its IT system into well separated security zones
- separates dedicated network for administration of IT systems and the Certification Service Provider's operational network
- separates the production systems for the TSP services from systems used in development and testing
- establishes communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure
- operates the IT systems used for the live operational network in secure network zones
- restricts access and communications between zones to those necessary for the operation of the service
- disables the not used protocols and user accounts
- disables unused network ports and services
- only runs network applications unconditionally necessary for the proper operation of the IT system.
- reviews the established rule set on a regular basis.

The Certification Service Provider undergoes or performs a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum
- after any system or network changes that the CA determines are significant
- at least every three (3) months.

The Certification Service Provider checks the compliance of the local network components (e.g. routers) configuration with the requirements specified by the Certification Service Provider at least every three months.

The Certification Service Provider orders a penetration test from an external independent expert who has the necessary skills, tools, proficiency and code of ethics to provide a reliable report yearly and in case of a significant change in the IT network.

6.8 Time stamping

For the protection of the integrity of the log files and other electronic files to be archived the Certification Service Provider uses qualified electronic Time Stamps issued by the e-Szignó Certification Authority.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The end-user Certificates issued by the Certification Service Provider and all the provider's root and intermediate Certificates which are in the Certificate Chain used to issue the Certificates comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [60]

[[QUA:

- **IETF RFC 3739 [41]**

]]

- IETF RFC 5280 [48]
- IETF RFC 6818 [51]

<TLS:

- IETF RFC 6962 [54]

>

- ETSI EN 319 412-1 [25]

<ALA:

- ETSI EN 319 412-2 [26]

>
<UNI:

- ETSI EN 319 412-2 [26] in case of Certificates issued to natural persons

>
<BEL:

- ETSI EN 319 412-3 [27]

>
<UNI:

- ETSI EN 319 412-3 [27] in case of Certificates issued to legal persons

>
<TLS:

- ETSI EN 319 412-4 [28]

>
[[QUA:

- **ETSI EN 319 412-5 [29]**

]]
<TLS:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [63]

[[QUA:

- **Guidelines for the Issuance and Management of Extended Validation Certificates [65]**

]]
>
[[QUA:
<not TLS: <not UNI:

- **CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [62] in case of Email (S/MIME) Certificate**

>>
]]
<UNI:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates [64] in case of Code Signing Certificate
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [62] in case of Email (S/MIME) Certificate

>

7.1.1 Version Number(s)

The provider certification unit (root and intermediate) Certificates used by the Certification Service Provider and the end-user Certificates issued by the Certification Service Provider are "v3" Certificates according to the X.509 specification [60].

7.1.2 Certificate Content and Extensions

The Certificates have the following basic fields:

- Version
  The Certificate complies with "v3" Certificates according to the X.509 specification, so the value "2" is in this field. [48]
- Serial Number
  The unique identifier generated by the Certificate issuer certification unit.

  In case of the end-user Certificates the "Serial Number" field contains a random number generated by a CSPRNG conformant Hardware Security Module, with at least 8 bytes (64 bits) entropy.
- Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for digitally signing the Certificate.

  The Certification Authority uses the cryptographic algorithm sets listed in chapter 7.1.3 to digitally sign the issued Certificates.
- Signature
  Electronic seal made by the Certification Authority certifying the Certificate, that has been created with an Algorithm set defined in the "Algorithm Identifier" field.
- Issuer
  The unique name of the Certificate issuer Certification Unit according to the ITU X.501 [59] name format (see in section 3.1).
- Validity (notBefore & notAfter)
  The beginning and the end of the validity period of the Certificate.

  The beginning of the validity period of the Certificate shall be

  - in case of provider's certificates
    - earliest the real issuance time of the Certificate minus 24 hours
    - latest the real issuance time of the Certificate
  - in case of subscriber's certificates
    <TLS:
    - earliest the real issuance time of the Certificate minus 48 hours
    - latest the real issuance time of the Certificate plus 48 hours

    >
    <not TLS:

    * earliest the real issuance time of the Certificate minus 48 hours

  >

  The Certification Service Provider never backdates Certificates.

  The time is recorded according to UTC and compliant with IETF RFC 5280 encoding.

- Subject
  The unique name of the Subject according to the ITU X.501 [59] name format (see in section 3.1).

  Always filled out.

- Subject Public Key Algorithm Identifier

  The Certification Service Provider supports the RSA and the ECDSA algorithms in the end-user Certificates.

  The values to be included in this field:

  – RSA algorithm
    * algorithm name: "rsaEncryption"
    * algorithm identifier: 1.2.840.113549.1.1.1
    * parameters must be present and must be an explicit NULL
    * encoded value: `30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00`

  – ECDSA algorithm
    * algorithm name: "ecPublicKey"
    * algorithm identifier: (1.2.840.10045.2.1)
    * parameters must use the namedCurve encoding
      · for P-256 keys:
      namedCurve: secp256r1 (OID: 1.2.840.10045.3.1.7)
      encoded value: `30 13 06 07 2a 86 48 ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01 07`
      · for P-384 keys:
      namedCurve: secp384r1 (OID: 1.3.132.0.34)
      encoded value: `30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 22`
      · for P-521 keys:
      namedCurve: secp521r1 (OID: 1.3.132.0.35)
      encoded value: `30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 23`

- Subject Public Key Value
  The public key of the Subject.

- Issuer Unique Identifier
  Not filled out.

- Subject Unique Identifier
  Not filled out.

The Certification Service Provider only uses the following certificate extensions according to the X.509 specification [60]:

Certificate of the Root Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field is not indicated.
- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.

  The field value: the SHA-1 hash of the provider public key.

  In case of the self-signed root certification unit certificate the value is identical with the value of the Subject key identifier field.
- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the Subject public key. The field value: the SHA-1 hash of the public key.

  Always filled in.
- Subject Alternative Names – not critical
  OID: 2.5.29.17

  It is filled in according to section 3.1.1.
- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" field is not present in the root Certificate.
- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The used values are:

  – "keyCertSign",
  – "cRLSign".

- Extended Key Usage – not critical
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  It is not present.

The above fields are always filled in. There are no more Certificate extensions.

Certificate of the Intermediate Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32

  This field may limit the Certificate Policies which can be used in the end-user Certificate. The intermediate CAs below this CA may issue only that type of end-user Certificates which fit to at least one of the Certificate Policies listed here.

  It is always filled.

  In case of Certificates issued to the intermediate certification units of the Certification Service Provider, the "anyPolicy" Identifier may be present in this field.

  The reference to the related Certification Practice Statement can be given in this field.

  In case of certification unit Certificates issued to other Certification Authority, only that identifier can be in this field, which relates to a Certificate Policy which complies to the Certificate Policy implemented by the issuer Certification Authority, and there can be no "anyPolicy" Identifier.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.

  It is always filled.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the Subject public key.
  The field value: the SHA-1 hash of the public key.

  It is always filled.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  It is filled in according to section 3.1.1.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" is not present in the Certificate.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The field contains the following values:

  – "keyCertSign",
  – "cRLSign".

- Extended Key Usage – not critical
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  <TLS:

  The Intermediate Certification Unit Certificates issued after 2019-01-01 for issuing Website Authentication Certificates

  – contains the following EKU value:
    * Server Authentication (1.3.6.1.5.5.7.3.1)
  – may contain the following EKU value:
    * Client Authentication (1.3.6.1.5.5.7.3.2)

  >

  <ALA:

  [[QUA:

  The Intermediate Certification Unit Certificates issued after 2019-01-01 contains the following "Extended Key Usage" values:

  The Intermediate Certification Unit Certificates for issuing Certificates exclusively for the creation of qualified electronic signatures:

  – **Document Signing (1.3.6.1.4.1.311.10.3.12)**

  The Intermediate Certification Unit Certificates for issuing Email (S/MIME) Certificates booth for protecting emails (S/MIME) and for the creation of qualified electronic signatures:

  – **emailProtection (1.3.6.1.5.5.7.3.4)**

  ]]

  >

  <BEL:

  [[QUA:

  The Intermediate Certification Unit Certificates issued after 2019-01-01 contains at least one "Extended Key Usage" value as detailed below:

  The Intermediate Certification Unit Certificates for issuing Certificates exclusively for the creation of qualified electronic seals:

– **Document Signing (1.3.6.1.4.1.311.10.3.12)**

The Intermediate Certification Unit Certificates for issuing Email (S/MIME) Certificates booth for protecting emails (S/MIME) and for the creation of qualified electronic seals:

– **emailProtection (1.3.6.1.5.5.7.3.4)**

The Intermediate Certification Unit Certificates for issuing Certificates for the Time Stamping Units:

– **Time stamping (1.3.6.1.5.5.7.3.8)**

]]

>

<not TLS: <not UNI:

[[ADV:

The Intermediate Certification Unit Certificates issued after 2019-01-01 contains at least one "Extended Key Usage" value as detailed below:

The Intermediate Certification Unit Certificates for issuing Certificates for the creation of electronic electronic signature or seals:

– *Document Signing (1.3.6.1.4.1.311.10.3.12)*

]]

>>

<UNI:

The Intermediate Certification Unit Certificates issued after 2019-01-01 contains at least one "Extended Key Usage" value as detailed below:

Each intermediate Certification Unit's Certificate contains all the extended key usage bit values which are included in the end-user Certificates isseued or can be issued by that Certification Unit according to Table 7.1.2.

>

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL accessibility through http protocol.
  It is always filled.

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the Certificate provided by the Certification Service Provider.

  Mandatory, and the field contains the following data:

- For the purpose of the fast and reliable verification of the current Certificate revocation status, the Certification Service Provider provides online certificate status service. The availability of this service is indicated here.
- To facilitate the certificate chain building the Certification Service Provider gives the access path through http protocol of the Certificate of the Certificate issuer certification unit.

The above fields are always filled in. There are no more Certificate extensions.

End-User Certificate

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field contains the denomination of the valid certification policy (see Section 1.2.1) at the time of the Certificate issuance and other information on the other uses of the Certificate.

  In case of end-user certificates, the Certification Service Provider fills in this field in all cases by providing the following data:

  <TLS:

  - CA/Browser Forum Certificate Policy:
    [[QUA:
    - **When the issued qualified Certificate can also be used to authenticate websites:**
      EVCP: Extended Validation Certificate Policy
      OID 2.23.140.1.1.
    - **When the issued qualified Certificate can not be used to authenticate websites:**
      No policy included

    ]]
    [[ADV:
    - *in case of DVCP Certificate OID 2.23.140.1.2.1*
    - *in case of OVCP Certificate OID 2.23.140.1.2.2*

    ]]

  >

  [[QUA:

  <not TLS: <not UNI:

  - **In case of Email (S/MIME) Certificate Certificate Policy defined by the CA/Browser Forum:**
    - **in case of Organization-validated Certificate OID 2.23.140.1.5.2.3**
    - **in case of Sponsor-validated Certificate OID 2.23.140.1.5.3.3**

>>
]]
<UNI:

- In case of Code Signing Certificate Certificate Policy defined by the CA/Browser Forum:
  - OID 2.23.140.1.4.1.
- In case of Email (S/MIME) Certificate Certificate Policy defined by the CA/Browser Forum:
  - in case of Organization-validated Certificate OID 2.23.140.1.5.2.3
  - in case of Sponsor-validated Certificate OID 2.23.140.1.5.3.3

>
<not TLS: <not UNI:

- In case of Time Stamping Certificate used for Code Signing purposes Certificate Policy defined by the CA/Browser Forum:
  - OID 2.23.140.1.4.2.

>>

- ETSI Certificate Policies
  [[QUA:
  the identifier (OID) of the certification policy specified by the ETSI EN 319 411-2 [24]
  <TLS:
  - **When the issued Certificate can also be used to authenticate websites:**
    QEVCP-w: Policy for EU qualified Certificate for website authentication, linking the given website to the given person
    OID: 0.4.0.194112.1.4.
  - **When the issued Certificate can not be used to authenticate websites:**
    QNCP-w-gen: Policy for EU qualified Certificate for webserver authentication, linking the given webserver to the given person
    OID: 0.4.0.194112.1.6.
  - **In case of PSD2 Certificate:**
    QCP-w-psd2: certificate policy for PSD2 qualified website authentication certificates
    OID: 0.4.0.19495.3.1.

  >
  <ALA:
  - **QCP-n: Policy for EU qualified Certificate issued to a natural person**
    OID: 0.4.0.194112.1.0

* **QCP-n-qscd: Policy for EU qualified Certificate issued to a natural person where the private key and the related Certificate reside on a Qualified Electronic Signature or Seal Creation Device OID: 0.4.0.194112.1.2.**

>

<**BEL:**

* **QCP-l: Policy for EU qualified Certificate issued to a legal person OID: 0.4.0.194112.1.1**
* **QCP-l-qscd: Policy for EU qualified Certificate issued to a legal person where the private key and the related Certificate reside on a Qualified Electronic Signature or Seal Creation Device OID: 0.4.0.194112.1.3.**

>

]]

[[ADV:

<TLS: the identifier specified by ETSI EN 319 411-1 [23] the policy which the Certificate complies with as follows:

* *in case of DVCP Certificate OID 0.4.0.2042.1.6,*
* *in case of OVCP Certificate OID 0.4.0.2042.1.7,*

>

<not TLS:

* *The identifier specified by ETSI EN 319 411-1 [23] the policy which the Certificate complies with as follows:*
  - *in case of LCP Certificate OID 0.4.0.2042.1.3,*
  - *in case of NCP Certificate OID 0.4.0.2042.1.1,*
  - *in case of NCP+ Certificate OID 0.4.0.2042.1.2.*

>

]]

– the identifier of the Microsec Certificate Policy (OID according to section 1.2.1)

– <TLS: optionally,> the availability of the Certification Practice Statement

<not TLS:

– the textual warning in English and Hungarian from which it can be established that **[[QUA:**

* **the Certificate is qualified**
* **the private key related to the Certificate is protected by a Qualified Electronic Signature or Seal Creation Device (exclusively in case of policies requiring the usage of Qualified Electronic Signature or Seal Creation Device)**
* **the preservation time of the data related to the Certificate.**

<not TLS:

- **the name of the tariff package associated with the Certificate, as specified in the "Certificate type" field of the table in section 9.8**

>

]]

[[ADV:

- *it is a II. or III. certification class certificate, namely personal appearance did or did not happen at the registration*
- *the Subject of the Certificate is a natural person*
- *the private key belonging to the Certificate is protected by a Electronic Signature or Seal Creation Device (this information can be seen also based on the OID identifier of the Certificate Policy)*

]]

>

The end-user Certificates that do not contain the "Certificate Policies" field shall be considered test certificates. The test Certificate can only be used for testing purposes, and they shall be declined in case of real transactions.

The reference to the related Certification Practice Statement may be given in this field.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.

  It is always filled in.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the Subject public key. The field value: the SHA-1 hash of the public key.

  It is always filled in.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  See section: 3.1.1.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the end-user Certificates.

  The "pathLenConstraint" field is not present in the end-user Certificates.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  <TLS:

  In the Website Authentication Certificates the mandatory and exclusively admissible values:

  - mandatory value is:
    - "digitalSignature"
  - optional values are:
    - in case of RSA key "keyEncipherment"
    - in case of ECC key "keyAgreement"

  [[ADV:

  The same key usage values are used in the Server Authentication Certificates, like the CISCO VPN Server, the Domain Controller or the VPN Server Authentication Certificate.

  ]]

  >

  <not TLS: <not UNI:

  In end-user Certificates the value is exclusively set to the following:

  [[QUA:

  - **in case of Email (S/MIME) Certificate**
    - **"nonRepudiation"**
    - **"digitalSignature"**
  - **any other types of Certificate**
    - **"nonRepudiation"**

  ]]

  [[ADV:

  - *"nonRepudiation"*
  - *"digitalSignature"*

  ]]

  >>

  <UNI:

  In case of the different usage purpose Certificates the following key usage bits are set (other value is not present):

Certificate type	keyUsage (critical)	ExtKeyUsage
Authentication	digitalSignature, keyAgreement (ECC)	clientAuth (1.3.6.1.5.5.7.3.2)
Cisco VPN client	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
Code Signing	digitalSignature	Code Signing (1.3.6.1.5.5.7.3.3)
Email encryption (S/MIME)	keyAgreement (ECC), keyEncipherment (RSA)	emailProtection (1.3.6.1.5.5.7.3.4)
Email protection (S/MIME)	digitalSignature	emailProtection (1.3.6.1.5.5.7.3.4)
Encryption	keyAgreement (ECC), keyEncipherment (RSA)	Document Encryption (1.3.6.1.4.1.311.80.1)
SCEP server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2)
Smartcardlogon	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), smartcardLogon (1.3.6.1.4.1.311.20.2.2)
national WRPAC	digitalSignature	WRPAC (1.3.6.1.4.1.21528.2.6.1)

Table 7.1.2.
Key Usage Bits and Extended Key Usage Bits

>

- Extended Key Usage – not critical
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  <TLS: In the Website Authentication Certificates the following value is always set:

  – "serverAuth (1.3.6.1.5.5.7.3.1)"

  In the Website Authentication Certificates the following further value is not included by default, but it may be added in case of the request of the Applicant:

  – "clientAuth (1.3.6.1.5.5.7.3.2)"

  [[ADV:

  In the Server Authentication Certificates the following extended key usage bits are indicated:

Certificate Type	*ExtKeyUsage*
Cisco VPN Server	*serverAuth (1.3.6.1.5.5.7.3.1), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)*
DomainController	*clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)*
RDP Gateway	*serverAuth (1.3.6.1.5.5.7.3.1)*

]]

>

<not TLS: <not UNI:

[[QUA:

<ALA: Mandatory to set, and the value in the qualified end user Certificates used exclusively for creation of electronic signatures is:

- **"Document Signing (1.3.6.1.4.1.311.10.3.12)"**

The value in the end user Email (S/MIME) Certificates booth for protecting emails (S/MIME) and for the creation of qualified electronic signatures is:

- **emailProtection (1.3.6.1.5.5.7.3.4)**

>

<BEL: Mandatory to set, and the value in the qualified end user Certificates used exclusively for creation of electronic seals is:

- **"Document Signing (1.3.6.1.4.1.311.10.3.12)"**

The value in the end user Email (S/MIME) Certificates booth for protecting emails (S/MIME) and for the creation of qualified electronic seals is:

- **emailProtection (1.3.6.1.5.5.7.3.4)**

>

]]

[[ADV:

In the non-qualified signing end user Certificates the set values are:

- *"Document Signing (1.3.6.1.4.1.311.10.3.12)"*

]]

>>

<UNI:

In case of the different usage purpose end-user Certificates the key usage bits of the above table are set (other value is not present).

>

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL availability relevant to the Certificate through http protocol. The CRL availability related to the Certificate is present here (URL).

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the Certificate provided by the Certification Service Provider.

  In case of end-user certificates the field contains the following data:

  – For the purpose of the fast and reliable verification of the current Certificate revocation status, the Certification Service Provider provides online certificate status service on the default HTTP port (port 80). The availability of this service is indicated here.
  – To facilitate the certificate chain building the Certification Service Provider gives the access path through http protocol of the Certificate of the Certificate issuer certification unit.

  The Certification Service Provider may give in this field the data of more than one service and Certificate of the Certificate issuer certification unit.

- Qualified Certificate Statements – not critical
  OID: 1.3.6.1.5.5.7.1.3
  The field is intended for the indication of statements related to the qualified Certificates, but it has a field, that can be used in case of a non-qualified Certificate too.

  [[QUA:

  The following statements are present in every end-user qualified Certificate:

  – **the Certificate is an EU qualified Certificate – 'id-etsi-qcs 1' (0.4.0.1862.1.1)**
  – **the transactional limit related to the Certificate – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2)**
  - optional
  – **that statement that the Certification Service Provider retains the registration data related to the Certificate for 10 years after the expiration of the Certificate – 'id-etsi-qcs 3' (0.4.0.1862.1.3)**

  <not TLS:

  – **that statement that the private key related to the Certificate resides inside a Qualified Electronic Signature or Seal Creation Device – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – only in the case of certification policies requiring the use of a Qualified Electronic Signature or Seal Creation Device**

  >

  – **the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the end-user Certificate – 'id-etsi-qcs 5' (0.4.0.1862.1.5)**

  <TLS:

  – **that indication that the Certificate was issued for website authentication purposes – 'id-etsi-qct-web' (0.4.0.1862.1.6.3)**

>

<ALA:

- **that indication that the Certificate was issued for signing purposes – 'id-etsi-qct-esign' (0.4.0.1862.1.6.1)**

>

<BEL:

- **that indication that the Certificate was issued for sealing – 'id-etsi-qct-eseal' (0.4.0.1862.1.6.2)**

>

<TLS: Based on the request of the Client the end-user Certificate may contain the optional statement describing the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] (OID: 0.4.0.19495.2). If this data is present, its value is a data structure containing the service type of the Subject's financial service and the name and the abbreviation of the supervisory authority supervising the Subject's financial service. >

<BEL:

Based on the request of the Client the end-user Certificate may contain the optional statement describing the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] (OID: 0.4.0.19495.2). If this data is present, its value is a data structure containing the service type of the Subject's financial service and the name and the abbreviation of the supervisory authority supervising the Subject's financial service.

>

]]

<not UNI:

[[ADV:

The QCType field may be filled according to the usage purpose.

<ALA:

It is indicated in the field that the Certificate was issued for signing purposes (the value of the field is 'id-etsi-qct-esign').

>

<BEL:

It is indicated in the field that the Certificate was issued for sealing purposes (the value of the field is'id-etsi-qct-eseal').

>

]]

>

<UNI:

Based on the request of the Client the end-user Certificate may contain the optional statement describing the Subject's data regarding the Open Banking requirements, or the Payment Services EU Directive (PSD2) [2] (OID: 0.4.0.19495.2). If this data is present, its value is a data structure containing the service type of the Subject's financial service and the name and the abbreviation of the supervisory authority supervising the Subject's financial service.

In any other case the field is not present.

>

<TLS:

- Precertificate Poison - critical
  OID: 1.3.6.1.4.1.11129.2.4.3
  Filling out is optional.

  The field indicates that this is a PreCertificate, which can not be used by correctly working applications in live systems.

  The Certification Service Provider adds this extension to each PreCertificate.

  The live Website Authentication Certificate never contains this extension.

- List of embedded Signed Certificate Timestamps (SCT) - not critical
  OID: 1.3.6.1.4.1.11129.2.4.2
  The field contains the SCTS signed by the Certificate Transparency log servers.

  This extension shall never be included in PreCertificates, but it may be included if Website Authentication Certificates.

  Filling out in the Website Authentication Certificate is optional and depends on the approval given by the Applicant.

>
<TLS:
The above fields are always filled out according to the given rules, except the List of embedded Signed Certificate Timestamps (SCT).
>
<not TLS:
The above fields are always filled out according to the given rules.
>
Other certificate extensions will not be filled out.
<BEL:
[[QUA:

Certificate issued for Time Stamping Unit

- **Certificate Policies – not critical**
  OID: 2.5.29.32

This field contains the identifier of the valid certification policy at the time of the Time Stamping Unit Certificate issuance and usage, and other information on the other uses of the Certificate.

Filling in is mandatory for this field, and it shall not be critical.

The reference to the related Certification Practice Statement can be given in this field.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the Time Stamping Unit public key. The field value: the SHA-1 hash of the public key.

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  The central email address of the Time Stamping Service Provider can be in this field in the Certificate of the Time Stamping Unit.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the Certificate issued for the Time Stamping Unit.

  The "pathLenConstraint" field is not present in the Certificate issued for the Time Stamping Unit.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  In the Certificates issued to the Time Stamping Unit only the following values are present:

  - nonRepudiation
  - digitalSignature

- Private Key Usage Period – not critical
  OID: 2.5.29.16
  Determination of the permitted private key usage period.

  In the Certificates issued to the Time Stamping Unit the Certification Authority restricts the private key usage time by setting the "notBefore" and "notAfter" values.

- **Extended Key Usage – critical**
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  In the Certificates issued to the Time Stamping Unit only the following values are present:

  - **timeStamping (1.3.6.1.5.5.7.3.8)**

- **CRL Distribution Points – not critical**
  OID: 2.5.29.31
  The field contains the CRL availability through http protocol.
  Mandatory to fill.

- **Authority Information Access – not critical**
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the time stamping unit Certificate provided by Certification Authority.

  Mandatory, and the field contains the following data:

  - **For the purpose of the fast and reliable verification of the current Certificate revocation status, the Certification Authority provides online certificate status service. The availability of this service is indicated here.**
  - **To facilitate the certificate chain building the Certification Authority gives the access path through http protocol of the Certificate of the Certificate issuer certification unit.**

[[QUA:

- **Qualified Certificate Statements – not critical**
  OID: 1.3.6.1.5.5.7.1.3
  The field is intended for the indication of statements related to the qualified Certificates.

  The following statements are present in the Certificate of the time stamping unit:

  - **the Certificate is an EU qualified Certificate – 'id-etsi-qcs 1' (0.4.0.1862.1.1)**
  - **the transactional limit related to the Certificate – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2)**
    - optional
  - **that statement, that the Certification Service Provider retains the registration data related to the Certificate for 10 years after the expiration of the Certificate – 'id-etsi-qcs 3' (0.4.0.1862.1.3)**
  - **that statement, that the private key related to the Certificate resides inside a Qualified Electronic Signature or Seal Creation Device – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – only in the case of certification policies requiring the use of a Qualified Electronic Signature or Seal Creation Device**

- **the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the Time Stamping Unit Certificate – 'id-etsi-qcs 5' (0.4.0.1862.1.5)**
- **that indication, that the Certificate was issued for sealing – 'id-etsi-qcs 6' (0.4.0.1862.1.6) (the value of the field is 'id-etsi-qct-eseal' (2))**

]]

The above fields are always filled in according to the given rules. There are no more Certificate extensions.

]]

[[ADV:

Certificate of the Time Stamping Unit

- *Certificate Policies – not critical*
  OID: 2.5.29.32
  This field contains the identifier of the valid certification policy at the time of the Time Stamping Unit Certificate issuance and usage, and other information on the other uses of the Certificate.

  Filling in is mandatory for this field, and it shall not be critical.

  The reference to the related Certification Practice Statement can be given in this field.

- *Authority Key Identifier – not critical*
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.

  The field value: the SHA-1 hash of the provider public key.

- *Subject Key Identifier – not critical*
  OID: 2.5.29.14
  The 40 character long unique identifier of the Time Stamping Unit public key. The field value: the SHA-1 hash of the public key.

- *Subject Alternative Names – not critical*
  OID: 2.5.29.17

  The central email address of the Time Stamping Service Provider can be in this field in the Certificate of the Time Stamping Unit.

- *Basic Constraints – critical*
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the Certificate issued for the Time Stamping Unit.

  The "pathLenConstraint" field is not present in the Certificate issued for the Time Stamping Unit.

- *Key Usage – critical*
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  In the Certificates issued to the Time Stamping Unit only the following values are present:

  - *nonRepudiation*
  - *digitalSignature*

- *Private Key Usage Period – not critical*
  OID: 2.5.29.16
  Determination of the permitted private key usage period.

  In the Certificates issued to the Time Stamping Unit the Certification Authority restricts the private key usage time by setting the "notBefore" and "notAfter" values.

- *Extended Key Usage – critical*
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  In the Certificates issued to the Time Stamping Unit only the following values are present:

  - *timeStamping (1.3.6.1.5.5.7.3.8)*

- *CRL Distribution Points – not critical*
  OID: 2.5.29.31
  The field contains the CRL availability through http protocol.
  Mandatory to fill.

- *Authority Information Access – not critical*
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the time stamping unit Certificate provided by Certification Authority.

  Mandatory, and the field contains the following data:

  - *For the purpose of the fast and reliable verification of the current Certificate revocation status, the Certification Authority provides online certificate status service. The availability of this service is indicated here.*
  - *To facilitate the certificate chain building the Certification Authority gives the access path through http protocol of the Certificate of the Certificate issuer certification unit.*

[[QUA:

- ***Qualified Certificate Statements – not critical***
  OID: 1.3.6.1.5.5.7.1.3
  The field is intended for the indication of statements related to the qualified Certificates.

  The following statements are present in the Certificate of the time stamping unit:

  - ***the Certificate is an EU qualified Certificate – 'id-etsi-qcs 1' (0.4.0.1862.1.1)***

- ***the transactional limit related to the Certificate – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2) - optional***
- ***that statement, that the Certification Service Provider retains the registration data related to the Certificate for 10 years after the expiration of the Certificate – 'id-etsi-qcs 3' (0.4.0.1862.1.3)***
- ***that statement, that the private key related to the Certificate resides inside a Qualified Electronic Signature or Seal Creation Device – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – only in the case of certification policies requiring the use of a Qualified Electronic Signature or Seal Creation Device***
- ***the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the Time Stamping Unit Certificate – 'id-etsi-qcs 5' (0.4.0.1862.1.5)***
- ***that indication, that the Certificate was issued for sealing – 'id-etsi-qcs 6' (0.4.0.1862.1.6) (the value of the field is 'id-etsi-qct-eseal' (2))***

]]

The above fields are always filled in according to the given rules. There are no more Certificate extensions.

]]

>

Certificate issued for OCSP Responder

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field contains the identifier of the valid certification policy (see section 1.2.1) at the time of the OCSP Responder Certificate issuance and usage, and other information on the other uses of the Certificate.

  Filling in is optional for this field, and it shall not be critical.

  The reference to the related Certification Practice Statement can be given in this field.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the Certificate.
  The field value: the SHA-1 hash of the provider public key.

  Always filled in.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the OCSP Responder public key.
  The field value: the SHA-1 hash of the public key.

  Always filled in.

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  It is never filled out.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the Certificate has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the Certificate issued for the OCSP Responder.

  The "pathLenConstraint" field is not present in the Certificate issued for the OCSP Responder.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  In the Certificates issued to the OCSP Responder only the following values are present:

  - digitalSignature

- Private Key Usage Period – not critical
  OID: 2.5.29.16
  Determination of the permitted private key usage period.
  It is not filled out.

- Extended Key Usage – not critical
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  In the Certificates issued to the OCSP Responder only the following values are present:

  - OCSP Signing (1.3.6.1.5.5.7.3.9)

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field is not included in the Certificate because revocation is not needed due to the short Certificate lifetime.

- nocheck

  OID: 1.3.6.1.5.5.7.48.1.5

  Indication that the Certification Service Provider doesn't offer revocation service for the Certificate, so the revocation status shall not be checked. It is always filled in.

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  Access information related to the use of the OCSP responder unit Certificate provided by Certification Authority.

  Optional, and the field may contain the following data:

  - To facilitate the construction of the certificate chain, Certification Authority can give here the address of the Certification Unit's Certificate, issuing the OCSP Certificate, via the http protocol.

The above fields are always filled in according to the given rules. There are no more Certificate extensions.

7.1.3 Algorithm Object Identifiers

The denomination of the cryptographic algorithm that has been used to certify the Certificate.

The Certification Authority uses the following cryptographic algorithm sets to digitally sign the issued Certificates, OCSP responses and Certificate Revocation Lists:

- RSA algorithm
  - in case of sha256 hashing:
    algorithm name: "sha256WithRSAEncryption"
    algorithm OID: (1.2.840.113549.1.1.11)
    encoded value: `30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00`
  - in case of sha384 hashing:
    algorithm name: "sha384WithRSAEncryption"
    algorithm OID: (1.2.840.113549.1.1.12)
    encoded value: `30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00`
  - in case of sha512 hashing:
    algorithm name: "sha512WithRSAEncryption"
    algorithm OID: (1.2.840.113549.1.1.13)
    encoded value: `30 0d 06 09 2a 86 48 86 f7 0d 01 01 0d 05 00`
- ECDSA algorithm
  - in case of P-256 key:
    algorithm name: "ecdsaWithSHA256"
    algorithm OID: (1.2.840.10045.4.3.2)
    encoded value: `30 0a 06 08 2a 86 48 ce 3d 04 03 02`
  - in case of P-384 key:
    algorithm name: "ecdsaWithSHA384"
    algorithm OID: (1.2.840.10045.4.3.3)
    encoded value: `30 0a 06 08 2a 86 48 ce 3d 04 03 03`
  - in case of P-521 key:
    algorithm name: "ecdsaWithSHA512"
    algorithm OID: (1.2.840.10045.4.3.4)
    encoded value: `30 0a 06 08 2a 86 48 ce 3d 04 03 04`

7.1.4 Name Forms

The Certification Service Provider uses a distinguished name – composed of attributes defined in the standards IETF RFC 5280 [48], ETSI EN 319 412-2 [26], ETSI EN 319 412-3 [27] and

ETSI EN 319 412-4 [28] – for the Subject identification in the Certificates issued based on this Certification Practice Statement.

The Certificate contains the globally unique identifier of the Subject (OID), filled out as defined in Section 3.1.1.

The value in the "Issuer DN" field of the Certificate is identical to the value in the "Subject DN" field of the issuer Certificate.

7.1.5 Name Constraints

The Certification Service Provider does not use name constraints with the use of the "nameConstraints" field.

7.1.6 Certificate Policy Object Identifier

The Certification Service Provider includes the not critical (Certificate Policy) extension in the Certificates according to the requirements of the Section 7.1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The Certification Service Provider can put short information related to the Certificate usage into the Certificate Policy extension Policy Qualifier field.

The field contains the online availability of the Certification Practice Statement (URI).

7.1.9 Processing Semantics for Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

The Certification Authority always issues full CRL whose scope includes all Certificates issued by the CA.

7.2.1 Version Number(s)

The Certification Authority issues version "v2" Certificate Revocation Lists according to the IETF RFC 5280 [48] specification.

7.2.2 CRL and CRL Entry Extensions

The Certificate Revocation Lists issued by the Certification Authority contain the following fields:

1. tbsCertList
   This field contains issuer information, validity, and other information, as well as a list of revoked Certificates.
   The entire field is signed with the Certification Service Provider's private key.

   (a) Version
   For the Certificate Revocation List version "v2" according to the IETF RFC 5280 [48] specification, the value of this field is mandatory "1".

   (b) Signature
   Identifier of the signing algorithm used by the Certification Unit during the issuance of the Certificate. Same as the algorithm ID used to sign the Certificate Revocation List (see signatureAlgorithm).

   (c) Issuer Name
   Unique name of the Certification Unit issuing the Certificate Revocation List (value of the "DN" field in the issuing Certification Unit Certificate byte-for-byte).

   (d) Effect from (thisUpdate)
   Start of entry into force of the Certificate Revocation List. UTC value with "UTCTime" encoding according to IETF RFC 5280 [48]. In the case of Certificate Revocation Lists issued by the Certification Authority, this is the same as the time of issue.

   (e) Next issuance (nextUpdate)
   Date of issuance of the next Certificate Revocation List (see Chapter 4.10). UTC value with "UTCTime" encoding according to IETF RFC 5280 [48].

   (f) Revoked Certificates
   The list of <not TLS: suspended or> revoked Certificates is sorted in ascending order by the Certificate Serial Number. If there is no <not TLS: suspended or> revoked Certificate, this field is not included in the Certificate Revocation List.

   Required fields for all entries:

   - Certificate Serial Number (CertificateSerialNumber)
     A unique identifier generated by the Certification Authority that issued the Certificate, which is an integer.
   - Revocation Date (revocationDate)
     UTC value with "UTCTime" encoding according to IETF RFC 5280 [48].

   Optional Certificate Revocation List Entry Extensions (crlEntryExtensions) that can be used by the Certification Authority:

   - Revocation Reason (reasonCode) – not critical
     OID: 2.5.29.21
     The reason for revocation is entered in this field.
     Mandatory field in case of subordinate CA Certificates, including a meaningful reason code.
     <not TLS:

Mandatory field in suspended Certificates, the value is:
"certificateHold (6)".
>

- Invalidity Date (InvalidityDate) – not critical
  OID: 2.5.29.24
  This field can contain the time the private key became untrusted.
  This field is not necessarily filled by the Certification Authority.
  When it is filled, the time value is equal to the time encoded in the "revocationDate" field of the CRL entry.
- Guide to Suspended Certificates (holdInstruction) – not critical
  OID: 2.5.29.23
  This field may contain the guide for managing the suspended Certificate.
  This field is not <not TLS: necessarily> filled by the Certification Authority.

(g) CRL Extensions

- Provider Key Identifier (AuthorityKeyIdentifier)
  OID: 2.5.29.35
  The ID of the public key which belongs to the private key used to authenticate the Certificate Revocation List in the form of an "SHA1" hash.
- CRL Serial Number (cRLNumber) – not critical
  OID: 2.5.29.20
  This field contains the monotonically increasing serial numbers of the Certificate Revocation Lists.

Certificate Revocation List Extension conditionally used by the Certification Authority:

- Expired Certificates on the CRL (expiredCertsOnCRL) – not critical
  OID: 2.5.29.60
  The Certification Authority indicates with this standard field according to the X.509 specification that it does not remove expired Certificates from the CRL. (See: chapter 4.10.)

2. Signing Algorithm ID (signatureAlgorithm)
   The cryptographic algorithm set identifier (OID) used to digitally sign the Certificate Revocation List.

   The Certification Authority uses the cryptographic algorithm sets listed in chapter 7.1.3 to digitally sign the issued Certificate Revocation Lists.

3. Signature (signatureValue)
   The electronic seal of the Certification Authority certifying the Certificate Revocation List.

   The Certificate Revocation List is authenticated by the Certification Authority using the same key as used to seal the issued Certificate.

The Certification Authority is not obliged to fill out the extensions.

7.3 OCSP Profile

The Certification Service Provider operates an online certificate status service according to the IETF RFC 6960 [53] and IETF RFC 9654 [58] standard.

The OCSP responses issued by Certification Authority contain the following fields:

- Algorithm identifier (signatureAlgorithm)
  The identifier of the cryptographic algorithm used for signing the OCSP response (OID).

  The Certification Authority uses the cryptographic algorithm sets listed in chapter 7.1.3 to digitally sign the issued OCSP responses.

- (Signature)
  The electronic signature or seal of the Certification Service Provider.

- Identifier of the Responder (responderID)
  The unique identifier of the OCSP Responder which issues the OCSP Response.

- Produced At (producedAt)
  The time when the OCSP Response was created.
  Value according to UTC with encoding according to IETF RFC 5280 [48].

  The OCSP Response is always based on the current revocation status information, so the value of the field is always the same as the value of the "thisUpdate" field.

- This Update (thisUpdate)
  The date of the entry into force of the OCSP Response.
  Value according to UTC with encoding according to IETF RFC 5280 [48].

- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response.
  Value according to UTC with encoding according to IETF RFC 5280 [48].

  <TLS: Mandatory, the value is equal to the time of the issuance + 12 hours. >

  <not TLS: Optional.

  If it is not filled, it means that there is no "grace period", the Certification Service Provider will give a newly generated OCSP response to an incoming OCSP request at any time, where the creation time is not earlier than the query time.

  >

- Certificate Status Response (SingleResponse)
  The field contains the ID of the Certificate (CertID) and the revocation status of the Certificate (CertStatus).

  The Certification Service Provider issues positive OCSP response according to the requirements of the CABF BR. The Response contains the "good" value only if the Certificate is included in the Certificate Repository of the Certification Service Provider and its revocation status is not <not TLS: suspended or> revoked.

7.3.1 Version Number(s)

The Certification Service Provider supports the online certificate status requests and responses conforming to the "v1" version according to the standard IETF RFC 6960 [53] The default value of the (Version) field is "v1", so this field is not included in the OCSP response.

7.3.2 OCSP Extensions

The Certification Service Provider may optionally include the following OCSP extension:

- ArchiveCutoff – not critical
  The Certification Authority may indicate with a standard notation according to the IETF RFC 6960 [53] specification that it retains revocation information beyond the Certificate's expiration. (See Section 4.10.)

The Certification Service Provider may include the following OCSP registration extension:

- Reason Code – not critical
  The reason of the revocation is in this field.

  Mandatory field in case of subordinate CA Certificates, including a meaningful reason code.

  <not TLS:

  In case of suspended certificates it is a mandatory field, its value shall be: "certificateHold (6)".

  >

8 Compliance Audit and Other Assessments

[[QUA:

The operation of the Certification Service Provider is supervised by the National Media and Infocommunications Authority in line with European Union regulations. The National Media and Infocommunications Authority holds site inspections on at least yearly basis at the Certification Service Provider location. Before the site inspection, the Certification Service Provider has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the Certification Service Provider meets the requirements of the eIDAS Regulation [1] and the related Hungarian legislation and the requirements of the applied Certificate Policy(s) and the corresponding Certification Practice Statement(s).

The subject and methodology of the screening complies with the following normative documents:

- **REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1]**
- **ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers [22]**

- **ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [21]**
- **ETSI EN 301 549 Harmonised European Standard; Accessibility requirements for ICT products and services [20]**
- **ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [23]**
- **ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [24]**

<TLS:

- **ETSI TS 119 411-5 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Implementation of qualified certificates for website authentication as in amended Regulation 910/2014 [31]**

>
<not TLS: <not UNI:

- **ETSI TR 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates [32]**

>>

- **ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [33]**

]]

[[ADV:

The Certification Service Provider has its operation periodically examined by independent external auditor. During the audit it is examined that the operation of the Certification Service Provider complies with the following normative documents:

- *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1]*
- *ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [21]*

- *ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [23]*

<UNI:

- *ETSI TR 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates; [32]*

>

- *ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [33]*

]]

The result of the screening is a confidential document accessible only to authorized persons.

The conformity certificate issued in accordance with the conformity assessment report is published via the website of the Certification Service Provider.

The Certification Service Provider applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

[[QUA:

<not TLS: <not UNI:

Distributed QSCD devices

The Certification Service Provider provides the following Qualified Electronic Signature or Seal Creation Devices for the Subjects:

- **IDPrime MD 940 (contact mode only) and IDPrime MD 3940 (contact and non-contact mode) smartcard which consist of M7892 G12 (Infineon) security controller, MultiApp v4.0.1 Java Card platform and IAS Classic v.4.4.2 electronic signature application with MOC server v1.1.**
  (Supplier: THALES)

- **IDPrime MD 940 C (contact mode only) and IDPrime MD 3940 C (contact and non-contact mode) smartcard which consist of SLC37 (Infineon) security controller, MultiApp v5.0 Java Card platform and IAS Classic v.5.2 electronic signature application with MOC server v3.1**
  (Supplier: THALES)

Supported QSCD devices

The Certification Service Provider doesn't have these devices on stock so there will be no Certificate issuance on new Qualified Electronic Signature or Seal Creation Device and there will be no new key generation on these type of devices.

The Certification Service Provider may issue Certificates for the Qualified Electronic Signature or Seal Creation Devices which were issued earlier and are still in use during the normal Certificate renewal or modification process.

The Certification Service Provider provides ongoing technical support and the software components required for the operation of the devices.

- **Currently, there is no such QSCD device.**

SSCD devices being phased out

The following Qualified Electronic Signature or Seal Creation Devices will be phased out due to the expiration of the validity of the card certificates on the one hand, and the usable cryptographic algorithm change on the other. The Certification Service Provider no longer has devices of this type that can be issued and no longer issues new Certificates for previously issued and still in use Qualified Electronic Signature or Seal Creation Devices, but it will continue to provide the software components and support necessary for the use of the devices until the devices are completely phased out.

- **Currently, there is no such SSCD device.**

Phased out SSCD devices

The following Qualified Electronic Signature or Seal Creation Devices have already been fully deprecated due to the expiration of the validity of the SSCD certificates.

The Certification Service Provider has already revoked the Certificates suitable for creating qualified electronic signatures or seals and no longer provides the software components and support required to use the devices.

- **IDPrime MD 840 (contact mode only) and IDPrime MD 3840 (contact and non-contact mode) smartcard which consist of M7820 A11 security controller, MultiApp v3 Java Card platform and IAS v.4 electronic signature application.**
  (Supplier: Gemalto)

- **IDClassic 340 smartcard which consist of P5CC081V1A microchip, MultiApp ID v2.1 Java Card platform and IAS Classic v.3 electronic signature application (version: MPH117 V2.2 filter).**
  (Supplier: Gemalto)

- **MultiApp ID Citizen 72k smartcard which consist of S3CC91C microchip, MultiApp v1.1 Java Card platform and IAS Classic v.3.0 electronic signature application.**
  (Supplier: Gemalto)

- **Smartcard which consist of ST19WR66I microchip and Touch & Sign2048 V1.00 signature creation application.**
  (Supplier: ST Incard)

In case of remote key management service

- **Product: Trident version 3.1.3**
  (Supplier: I4P.informatikai Kft. (I4P Ltd.))
- **Product: Trident version 3.2.3**
  (Supplier: I4P.informatikai Kft. (I4P Ltd.))
- **Entrust Signature Activation Module, version 1.1.1**
  (Supplier: Entrust)
  - **on nShield Solo XC v.12.60.15 HSM, or**
  - **nShield 5s v13.5.1 HSM**

Before using Qualified Electronic Signature or Seal Creation Device, the Certification Service Provider makes sure that it has a valid device certificate that meets the current requirements.

The Certification Service Provider manages the Qualified Electronic Signature or Seal Creation Device throughout its life cycle in accordance with the requirements in the appendix to the device certificate.

The Certification Service Provider monitors the certification status of the used Qualified Electronic Signature or Seal Creation Devices at least until the end of the validity period of the last Certificate issued on them and takes appropriate measures in case of modification of this status.

In case of the revocation of the Qualified Electronic Signature or Seal Creation Device's certificate the Certification Service Provider revokes all the valid Certificates issued on that Qualified Electronic Signature or Seal Creation Device in which Certificates the "id-etsi-qcs 4" statement was set (see in chapter 7.1.2).

The actual list of the Qualified Electronic Signature or Seal Creation Devices used by the Certification Service Provider and the information related to its certification can be found on the web page of the Certification Service Provider on the following link:

`https://e-szigno.hu/certification-of-qscd-devices`

The informativ full list of the certified Qualified Electronic Signature or Seal Creation Devices can be found on the web page of the European Commission:

European Commission eIDAS Dashboard

Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices [7]

>>

[7] https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

]]

The Certification Service Provider has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The Certification Service Provider keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

The Certification Service Provider has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation (see section: 1.3.1)

8.1 Frequency or Circumstances of Assessment

The Certification Service Provider has the conformance assessment carried out annually on its IT system performing the provision of the services.

<TLS:

An audit period never exceeds one year in duration. The successive period-of-time audits cover the entire lifetime of each trusted Certification Unit, continuously (without gaps) from cradle to grave. The audit covers service provider key pairs generated during the audit period, including keys for which a Certificate has not yet been issued (parking keys). The generated keys are identified by the public key "SHA-256" value in the issued audit reports (AAL). >

8.2 Identity/Qualifications of Assessor

The eIDAS and ETSI conformity assessment is performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

8.3 Assessor's Relationship to Assessed Entity

External audit is performed by a person who:

- is independent from the owners, management and operations of the examined Certification Service Provider
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the Certification Service Provider
- remuneration is not dependent on the findings of the activities carried out during the audit

8.4 Topics Covered by Assessment

The review covers the following areas:

- compliance with the legislation currently in force
- compliance with technical standards

- compliance with the Certification Policy and the Certification Practice Statement
- adequacy of the employed processes
- documentation
- physical security
- adequacy of the personnel
- IT security
- compliance with the data protection rules

<TLS:
The scope of the audit covers all active intermediate Certification Units in the audited CA hierarchy, under which there is a valid Certificate or suitable for issuing a new Certificate.
>
If the Certification Service Provider issued a subordinate Certificate for the certification unit of another organization then the listed areas are examined at these external organizations as well.

8.5 Actions Taken as a Result of Deficiency

The independent auditor summarizes the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them are recorded in a separate chapter of the report.
The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

- modification suggestions to be optionally taken into consideration
- derogations to be averted mandatorily.

[[QUA:
The independent auditor shall report the revealed serious derogations without delay to the National Media and Infocommunications Authority that is authorized to take the necessary measures. The Certification Service Provider shall answer the problems stated by the independent auditor in writing, and to report the measures taken to avert them at the occasion of the next authority review. The independent auditor shall send the assessment report in each case to the National Media and Infocommunications Authority.
]]

8.6 Communication of Results

- The Certification Service Provider publishes the summary report of the assessment on its web page on the following URL:

  `https://e-szigno.hu/en/eidas/`

  The Certification Service Provider doesn't publish the details of the findings, they are treated as confidential information.

[[QUA:

- **The certificates of the conformity assessment audit can be found on the official site of the auditor [8], and they are published also on the site of the Certification Service Provider on the following link:**

  `https://e-szigno.hu/en/eidas/`

- **The availabilities of the Hungarian National Trusted List are:**
  - **human readable PDF format:** `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
  - **machine-processable XML format:** `http://www.nmhh.hu/tl/pub/HU_TL.xml`

  The register of the National Media and Infocommunications Authority on trust services is available on the following link:

  `https://esign.nmhh.hu/bszny/setLanguageAction.do?lang=en`

]]

<TLS:

- The Certification Service Provider discloses the audit report (AAL) in the CCADB within three months of the point-in-time date or the end date of the latest audited period.
- The Certification Service Provider also discloses in the CCADB all intermediate CA certificates they issue that chain up to a root CA Certificate trusted by any of Apple's, Google Chrome's, Microsoft's or Mozilla's Root Program, including those CA certificates that share the same key pair whether they are self-signed, doppelganger, reissued, cross-signed, or other roots.

  The Certification Service Provider discloses such CA certificate within one week of certificate creation, and before any such CA is allowed to issue certificates.

>

8.7 Self-Audits

In addition to the external audit, the Certification Service Provider also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The Certification Service Provider ensures regular monitoring of its internal processes, the details of which is specified in the Certification Practice Statement and in its inner regulations.

It checks the compliance of the operation during a comprehensive internal audit at least once per every year in accordance with applicable CA/B Forum Guidelines.

The Certification Service Provider shall perform an annual self-assessment evaluating the conformance of this Certification Practice Statement against CA/B Forum Baseline Requirements and the applicable Root Program Policies.

[8] `https://www.hunguard.hu/en/ugyfeleinknek/tanusitott-termekek-rendszerek/eidas-rendelet-szerinti-bizalmi-s`

Completed self-assessments shall be submitted to the CCADB within 90 days from the "BR Audit Period End Date" field specified in the root CA's "CA Owner/Certificate" CCADB record (i.e. End Date of the Audit Period).

<TLS:

A random check is performed by the Certification Service Provider quarterly on at least 3% of the Website Authentication Certificate issued since the previous inspection, whether they comply with the related Certificate Policies and Certification Practice Statement.

The technical accuracy of the selected sample Website Authentication Certificates will be validated again by using automated test tools (linters).

>

<UNI:

A random check is performed by the Certification Service Provider quarterly on at least 3% of the Code Signing Certificate issued since the previous inspection, whether they comply with the related Certificate Policies and Certification Practice Statement. >

<not TLS:

A random check is performed by the Certification Service Provider quarterly on at least 3%, but not less than 30 of the Email (S/MIME) Certificate issued since the previous inspection, whether they comply with the related Certificate Policies and Certification Practice Statement.

The technical accuracy of the selected sample Email (S/MIME) Certificates will be validated again by using automated test tools (linters).

The Certification Service Provider performs the testing of different types of Email (S/MIME) Certificates in a common test which covers each type of Email (S/MIME) Certificates. >

In case of a provider Certificate issued to a certification unit operated by another organization, the operation of the external certification unit is audited annually.

The Certification Service Provider performs the internal audits with the help of its employees who hold the independent system auditor role.

9 Other Business and Legal Matters

9.1 Fees

The Certification Service Provider publishes fees and prices via its website and makes them available for reading at its customer service.

Price list availability:

- `https://e-szigno.hu/en/price-list`

The Certification Service Provider may unilaterally change the price list. The Certification Service Provider publishes any modification to the price list 30 days before it comes into force.

Changes that are favorable to the Client may take effect in less than 30 days.

Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service agreement and its annexes – the General Terms and Conditions in particular.

9.1.1 Certificate Issuance or Renewal Fees

See section: 9.1.

9.1.2 Certificate Access Fees

The Certification Service Provider grants free of charge online access to its Certificate Repository for the Relying Parties.

9.1.3 Revocation or Status Information Access Fees

The Certification Service Provider provides free of charge online CRL and OCSP service for the Relying Parties on the status of all end-user and intermediate Certificates it issued.

9.1.4 Fees for Other Services

See section: 9.1.

9.1.5 Refund Policy

See section: 9.1.

9.2 Financial Responsibility

<TLS:

In order to facilitate trust the Certification Service Provider takes financial responsibility to fulfil all its obligations defined in the present Certification Practice Statement, the related Certificate Policy and the service agreement concluded with the Client.

>

<not TLS: <not UNI:

In order to facilitate trust the Certification Service Provider complies with the financial and liability requirements below.

>>

<UNI:

In order to facilitate trust the Certification Service Provider takes financial responsibility to fulfil all its obligations defined in the present Certification Practice Statement, the related Certificate Policy and the service agreement concluded with the Client.

>

9.2.1 Insurance Coverage

The Certification Service Provider has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

<not UNI:

- The Certification Service Provider has liability insurance to ensure reliability.
  - The liability insurance covers the following damages caused by the Certification Service Provider in connection with the provision of services:
    - damages caused by the breach of the service agreement to the trust service Clients
    - damages caused out of contract to the trust service Clients or third parties
    - damages caused to the National Media and Infocommunications Authority by the Certification Service Provider terminating the provision of the trust service
    - under the eIDAS Regulation [1] 17. article (4) e) point, the legal costs of conformity assessment bodies to perform a conformity assessment by the request of the National Media and Infocommunications Authority if it enforces the costs as legal costs.
  - The liability insurance policy shall cover at least for 3.000.000 Hungarian forints. Coincidental damages occurred for the same reason constitute a single insurance event.
  - The liability insurance provides coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the Certification Service Provider regardless of whether the damage was caused by breach of contract or outside the contract.
  - If the valid claim of several entitled parties related to an insurance event exceeds the liability limit defined for an insurance event in the liability insurance, then the compensation of the claims takes place in the proportion of the liability limit to the total sum of the claims.

>
<TLS:
[[QUA:

- **The Certification Service Provider maintains liability insurance for EV Certificates according to section 8.4 of CABF EVG [65]:**
  - **Commercial General Liability insurance with policy limits of two million US dollars in coverage**
  - **Professional Liability/Errors and Omissions insurance, with policy limits of five million US dollars in coverage, and including coverage for:**
    - **claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates,**

* **claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.**

]]

>

<UNI:

The Certification Service Provider does not have liability insurance. The Certification Service Provider indemnification is described in section 9.6.1.

>

9.3 Confidentiality of Business Information

The Certification Service Provider manages clients' data according to legal regulations. The Certification Service Provider has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

By applying for a Certificate, and signing the service agreement, Clients consent to the Certification Service Provider retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the Certification Service Provider's services go offline; moreover to forwarding such information to the Certification Service Provider's subcontractors – solely for the purpose of performing tasks associated with providing the service.

Subject or Applicants shall make a declaration whether they consent to the disclosure of a Certificate on the Certificate Application form that is linked to the service agreement.

The Certification Service Provider uses clients' data solely in connection with the provision of its services.

The Certification Service Provider discloses Subjects' <not SEA: and Represented Organizations' > data appearing in a Certificate together with the Certificate. The Certification Service Provider stores their data that are not entered in a Certificate in a secured manner, for the purpose of providing evidence about the Subjects' <not SEA: identity, Represented Organizations'> organisational identity, and that of its miscellaneous data provision related obligations. The Certification Service Provider retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the Certification Service Provider sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The Certification Service Provider provides for the confidentiality and intactness of information that is not public during the forwarding of Clients' data.

9.3.1 Scope of Confidential Information

The Certification Service Provider treats as confidential:

- all Client data, with the exception of those that qualify as information not considered confidential in section 9.3.2

- besides the Client data:
  - private keys and activation codes
  - Certificate Applications and Service Contracts
  - transaction related data and log data
  - non-public regulations
  - all data whose public disclosure would have an adverse effect on the security of the service.

9.3.2 Information Not Within the Scope of Confidential Information

The Certification Service Provider considers all data public that can be obtained from a public source, or to the disclosure of which the Subscriber gave its consent in writing beforehand.

The Certification Service Provider treats all of the data it indicates in a Certificate as non-confidential information. Such data appear in the Certificate Application form linked to the service agreement in a clearly marked way.

The Certification Service Provider manages the revocation <not TLS: and suspension> status of the end-user and intermediate provider Certificates as public information and makes it available without restriction to the Relying Parties by publishing a Certificate Revocation List (CRL) and by providing online Certificate Status Protocol (OCSP) service. The disclosed information contains the serial number of the Certificate, the time of the revocation and optionally the reason for revocation. For more information, see section 7.2 and 7.3.

9.3.3 Responsibility to Protect Confidential Information

The Certification Service Provider is responsible for the protection of the confidential data it manages.

The Certification Service Provider obliges its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

<not UNI:

The Certification Service Provider processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following case:

>

<UNI:

The Certification Service Provider processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information.

>

<not UNI:

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the Certification Service Provider – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the Certification Service Provider to investigating authorities and national security services free of charge.

  The Certification Service Provider records the fact of data transfers, but does not inform involved clients about it.

- **Provision of information in the scope of litigation**

  In the course of litigation and non-litigious actions under common law, the Certification Service Provider may hand over – in case their being affected is certified – Subject identity information and the information verified by the Certification Service Provider, to an adverse party or its representative, as well as it may disclose them to the inquiring court.

  The Certification Service Provider records the fact of data transfers and informs impacted clients about it.

>

- **Disclosure upon owner's request**

  Upon a Client's personal request to do so or on the basis of its authorisation granted officially, in writing, the Certification Service Provider reveals confidential user information pertaining to the Client to third parties.

<not UNI:

- **Miscellaneous circumstances resulting in the disclosure of information**

  Upon termination of its activity the Certification Service Provider is bound to hand over its records subject to the access obligations together with confidential user data to the trusted service provider that takes it over.

>

9.4 Privacy of Personal Information

The Certification Service Provider takes care of the protection of the personal data it manages, the operation and regulations of the Certification Service Provider comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [9] and the 2016/679 EU General Data Protection Regulation [3].

The Certification Service Provider:

- preserves
- upon expiry of the obligation to retain – unless the Client otherwise indicates – deletes from the client database

the registered personal data and information on the Client in accordance with the legal requirements.

The Certification Service Provider stores identification data, data about the Subject appearing in the Certificate, data about the Subscriber associated with contact details and data connected to the provision of the service in its records.

The Certification Service Provider hands over Client data to third parties solely in cases where this is stipulated by a legal regulation or if the Client has granted its consent to this in writing.

9.4.1 Privacy Plan

The Certification Service Provider has a Privacy Policy and a Privacy Notice document, which contain detailed regulations on the handling of personal data.

The Privacy Policy is published via the website of the e-Szignó Certification Authority on the following URL:

`https://e-szigno.hu/all-documents`

The Privacy Notice is published via the website of the e-Szignó Certification Authority on the following URL:

`https://e-szigno.hu/privacynotice`

9.4.2 Information Treated as Private

The Certification Service Provider protects all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from the Certificate or other public data source.

9.4.3 Information Not Deemed Private

The Certification Service Provider may disclose the data of the Subjects indicated in the Certificate based on the written consent of the Subject or Applicant.

The Certification Service Provider may indicate the unique provider identifier assigned to the Subject in the Certificate.

9.4.4 Responsibility to Protect Private Information

The Certification Service Provider stores securely and protects the personal data related to the Certificate issuance and not indicated in the Certificate. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

9.4.5 Notice and Consent to Use Private Information

The Certification Service Provider only discloses personal data indicated in the Certificates with the written consent of the Client.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the <ALA: 94. § of the Digital Citizenship Act [13] > <not SIG: relevant legislation> the Certification Service Provider may disclose the stored personal data about the Client without notifying the Client.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

During its business operation, the Certification Service Provider shall not harm any intellectual property rights of a third person.

The owner of the private and public key issued by the Certification Service Provider to clients is the Subscriber and the full user is the Subject or Applicant regardless of the physical media that contains and protects the keys.

The owner of the Certificate issued by the Certification Service Provider to its clients is the Certification Service Provider and its full user is the <not TLS: Subject or Applicant.> <TLS: Subscriber.>

The Certification Service Provider may publish, reproduce, revoke and manage the issued end-user Certificates, with the public key contained in them in the manner described in the terms and conditions.

The certificate revocation status information is the property of the Certification Service Provider which is disclosed as defined in sections 7.2. and 7.3.

The unique provider identifier issued to the Clients by the Certification Service Provider is the property of the Certification Service Provider which

is disclosed as a part of the Certificate by the Certification Service Provider in the Certificate Repository.

The <not TLS: named Subject and the> Client is entitled to the use of the identification in the certificate (which identifies the Certificate subject).

The present Certification Practice Statement is the exclusive property of the Certification Service Provider. The Clients and other Relying Parties are only entitled to use the document according to the requirements of the present Certification Practice Statement and any other use for commercial or other purposes is strictly prohibited.

The present Certification Practice Statement may be freely distributed in unchanged form, in full length and with the indication of origin.

The rules of the application of the software provided for the use of the service by the Certification Service Provider is accessible in the description of the software and it is included in the user's guide referenced in the description.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the Certification Service Provider is in the Certification Practice Statement, the related Certificate Policies, and the service agreement with the Client and its attachments.
<TLS:

- The Certification Service Provider assumes responsibility that it validated that the Applicant either had the right to use, or had control of, the Domain Name(s) *[[ADV: and IP address(es)]]* listed in the Certificate.

>

- The Certification Service Provider assumes responsibility for compliance with the procedures described in Certificate Policies it supports.
- The Certification Service Provider assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors.
- The Certification Service Provider is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [10] in relation to the Clients which are in a contractual relationship with it.
- The Certification Service Provider is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [10] in relation to third parties (such as the Relying Party) that are not in a contractual relationship with it.
- The Certification Service Provider will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The Certification Service Provider is not responsible:

- for the Subject activities related to the private key

<not TLS:

- for the Subject activities related to the Electronic Signature or Seal Creation Device

>

- for the certificate verification and usage activities of the Relying Parties
- for the regulations issued by the Relying Parties or others.

Certification Authority Obligations

[[QUA:
The Certification Service Provider shall fulfil the requirements defined in section (2) of article 24. of the eIDAS regulation [1].
]]

The Certification Service Provider's basic obligations is that it shall provide the service in line with the Certificate Policy, this Certification Practice Statement, the General Terms and Conditions, furthermore corporate and security related internal regulations. These basic obligations are as follows:

- to establish the legal, regulatory, material, contractual, etc. framework appropriate for the service
- to provide high standard and secure services in accordance with the applicable regulations
- to continuously operate and audit organisations associated with the services (certification body, customer service etc.)
- to abide by the procedures prescribed in the regulations, and to avoid or eliminate any potentially occurring incorrect operation
- to ensure the Services to every applicant who accepts the terms and conditions specified in the regulations
- to maintain public and proprietary records, as well as to make them continuously available to anybody over the internet.

Certification Organization Obligations

The certification organization has the task of setting up and operating the certification units (see section: 1.3.1), as well as units necessary for the online certificate status service, to take care of the certificate repository and revocation status related information <not TLS: to manage and make available smart cards, > moreover to manage regulations.

The Certification Service Provider's internal, operative regulations specify how a certification organization shall be operated. Certification Authority's certificates issued by certification units are managed (for registration staff members, on-call duty staff, etc.) in accordance with the stipulations of operative regulations. This statement only includes stipulations in connection with the public provider and end-user certificates.

Tasks to be performed in the scope of managing regulations:

- the specification, approval, and maintenance of certificate types that are used
- preparing the public regulations of the services and internal (not public) stipulations, their reconciliation with legal regulations and internal (not public) regulations, furthermore, carrying out any updates
- the recording of observations associated with regulations applicable to the services, and to evaluate recommendations.

The e-Szignó Certification Authority is responsible:

- for the authenticity and accuracy of the Certificates it issued
- for the regulations it has issued, and for their conformity and compliance with statutory regulations
- for the compliance of the key pairs it generated, and for the relationship between the private-public key and the Certificate

<not TLS:

- for the relationship of the Electronic Signature or Seal Creation Device activation code and the keys uploaded to the device

>

- in general, for the compliance with its obligations.

9.6.2 RA Representations and Warranties

The customer service has the task of representing the Certification Service Provider at end-users in connection with the services. It performs the following tasks in the scope thereof:

- participates in selling the services
- performs the registration of Subjects
- receives requests pertaining to various certificate operations (revocation, <not TLS: suspension, reinstation,> certificate replacement)
- receives and handles data modification related filings
- participates in revocation status publication
- offers information provision activity to Clients and Relying Parties in connection with its activities associated with the services provided by the Certification Service Provider

The Registration Authority is responsible:

- for establishing the personal identity of <BEL: the person authorized to represent the> Subject or Applicants

<not SEA:

- for establishing the organisational identity of Represented Organizations, and in this latter case for establishing the right of representation of an individual acting in the name of a Represented Organization

>

- for the genuineness of recorded registration data
- for providing information to those using the services as to the contents and availability of the Certificate Policy and the Certification Practice Statement, as well as the terms and conditions of using the service prior to concluding the service agreement
- in general, to fully comply with its obligations.

9.6.3 Subscriber Representations and Warranties

Subscriber Responsibility

The responsibility of the Subscriber is set by the service agreement and its attachments (including the terms and conditions).

Subscriber Obligations

The responsibility of the Subscriber is to act in accordance with the contractual terms and regulations of the Certification Service Provider while using the service including requesting and applying the Certificates and private keys.

The obligations of the Subscriber are determined by this Certification Practice Statement, the service agreement, the General Terms and Conditions, as well as the relevant Certificate Policy.

When the Subscriber is informed about any actual or suspected misuse or compromise of the private key associated with the public key included in a Certificate belonging to the Subscriber, the Subscriber is obliged to

- promptly report this fact to the Certification Service Provider,
- promptly request the revocation <not TLS: or suspension> of the Certificate,
- promptly cease using the Certificate and its associated private key.

<TLS:
The Subscriber may install the Certificate and its associated private key only on servers that are accessible at one of the domains *[[ADV: or IP addresses]]* listed in the subjectAltName(s) field in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the service agreement and the General Terms and Conditions.
>

Subscriber Rights

- Subscribers have the right to use the services in accordance with this Certification Practice Statement.
- Subscribers are entitled to specify which Subjects should be allowed to receive Certificates, in writing, and Subscribers have the right to request the <not TLS: suspension and> revocation of such Certificates.
- Subscribers have the right to request the <not TLS: suspension and> revocation of Certificates.
- Subscribers are entitled to appoint Organizational Administrators.

Subject or Applicant Responsibility

The Subject or Applicant is responsible for:

- the authentication, accuracy and validity of the data provided during registration
- the verification of the data indicated <not TLS: in the Certificate > <TLS: in the requested Certificate >
- to provide immediate information on the changes of its data <TLS: and the data indicated in the Certificate >
- using its <not TLS: <not UNI: Electronic Signature or Seal Creation Device, >> private key and Certificate according to the regulations
- the secure management of its private key and activation code

<ALA:

- the secure management of the Electronic Signature or Seal Creation Device

>

- for the immediate notification and for full information of the Certification Service Provider in cases of dispute
- to generally comply with its obligations.

Subject or Applicant obligations

The Subject or Applicant shall:

- read carefully this Certification Practice Statement before using the service
- completely provide the data required by the Certification Service Provider necessary for using the service, and to provide truthful data
- if the Subject or Applicant becomes aware of the fact that the necessary data supplied for using the service – especially data indicated in the certificate – have changed, it is obliged to immediately:
  - notify the Certification Service Provider in writing,
  - request the <not TLS: suspension or> revocation of the Certificate and
  - terminate the usage of the Certificate

<not UNI:

- immediately terminate the usage of the private key belonging to the Certificate, if the Subject or Applicant becomes aware of the fact that the subject's Certificate has been revoked, or that the issuing CA has been compromised

>

- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents

<TLS:

- install the Website Authentication Certificate only to that servers which are accessible on the domain name *[[ADV: or IP address]]* in the Certificate

>

- ensure that no unauthorized individuals have access to data and tools (passwords, secret codes, signature-creation devices) necessary for using the service
- notify the Certification Service Provider in writing and without delay in case a legal dispute starts in connection with <ALA: any of the electronic signatues or> <BEL: any of the electronic seals or> the Certificates associated with the service
- cooperate with the Certification Service Provider in order to validate the data necessary for issuing certificates, and to do everything they can to allow the soonest possible completion of such verification

<ALA:

- report this fact to the Certification Service Provider promptly and in writing, in case a Subject's private key, Electronic Signature or Seal Creation Device or the secret codes necessary for activating the device end up in unauthorized hands or are destroyed, and will also be obliged to initiate the revocation and/or suspension of the Certificates and terminating the usage of the Certificate

>

- answer to the requests of the Certification Service Provider within the period of time determined by the Certification Service Provider in case of key compromise or the suspicion of illegal use arises
- acknowledge that the Subscribers entitled to request the revocation <not TLS: and/or suspension> of the Certificate
- acknowledge that the Certification Service Provider issues Certificates in the manner specified in the Certification Practice Statement, upon the completion of the validation steps described therein
- acknowledge that the Certification Service Provider only displays data that are corresponding to reality in issued Certificates. Accordingly, the Certification Service Provider validates data to be entered in Certificates according to the Certification Practice Statement

<not SEA:

- acknowledge that in case of requesting an Organizational Certificate, the Certification Service Provider will issue the Certificate solely in the case of the consent of the Represented Organization
- acknowledge that in case of requesting an Organizational Certificate, the Represented Organization has the right to request the revocation of the Certificate

>

- acknowledge and accept that the Certification Service Provider is entitled to <not TLS: suspend and/or> revoke the issued Certificate within the timeframe specified in section 4.9.1 of this Certification Practice Statement, if
  - the Certification Service Provider becomes aware that the data indicated in the Certificate do not correspond to the reality or the private key is not in the sole possession or usage of the Subject or Applicant and in this case, the Subject or Applicant is bound to terminate the usage of the Certificate
  - the Subscriber violates the terms of service agreement or General Terms and Conditions
  - the revocation is required by <TLS: the CABF Baseline Requirements,> the Certification Service Provider's Certificate Policy or Certification Practice Statement
  - the Certification Service Provider becomes aware that the Certificate was used for an illegal activity <TLS: (for example phishing, fraud, malware spreading)> <CSI: (for example phishing, fraud, malware spreading)>
  - the Subscriber fails to pay the fees of the services by the deadline.

Subject or Applicant Rights

- Subject or Applicants have the right to apply for Certificates in accordance with the Certification Practice Statement.
- In case this is allowed by the applicable Certificate Policy, Subject or Applicants are entitled to request <not TLS: the suspension and> the revocation of their Certificates, according to this Certification Practice Statement.

9.6.4 Relying Party Representations and Warranties

The Relying Parties decide based on their discretion and/or their policies about the way of accepting and using the Certificates. During the verification of the validity for keeping the security level guaranteed by the Certification Service Provider it is necessary for the Relying Party to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the present Certificate Policy and the corresponding Certification Practice Statement
- use reliable IT environment and applications

- verify the revocation status of the Certificate based on the current CRL or OCSP response
- take into consideration every restriction in relation to the Certificate usage which is included in the Certificate, in the Certification Practice Statement and in the corresponding Certificate Policy.

9.6.5 Representations and Warranties of Other Participants

<BEL: No stipulation.>
<not SEA:

Represented Organisation responsibility

The Represented Organization is solely responsible for the documents it issues. In particular for document in which it attests that a Subject or Applicant is a staff member of the Certification Service Provider, moreover, is entitled to appear in the Represented Organization's Certificate. In case the information appearing in any certification made out by the Represented Organization is changed, reporting this to the Certification Service Provider without delay is the Represented Organization's responsibility.

Represented Organisation rights

- The Certification Service Provider only issues Certificates in which the Represented Organization's name is indicated in possession of the Represented Organization's consent.
- The Represented Organization is entitled to <not TLS: suspend and> revoke Certificates in which the Represented Organization's name was also indicated.

>

9.7 Disclaimers of Warranties

The Certification Service Provider excludes its liability if:

- the Subjects or Applicants do not follow the requirements related to the management of the <ALA: Electronic Signature or Seal Creation Device and of the > private key
- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it
- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by <not UNI: the National Media and Infocommunications Authority algorithmic decree.> <UNI: international standard recommendations.>

9.8 Limitations of Liability

<TLS: Conditions of liability of the Certification Service Provider:>
<UNI: Conditions of liability of the Certification Service Provider:>

- The Certification Service Provider is not responsible for damages that arise from the Relying Party failing to proceed as recommended according to effective legal regulations and the Certification Service Provider's regulations in the course of validating and using certificates, moreover its failing to proceed as may be expected in the situation.
- The Certification Service Provider shall only be liable for contractual and non-contractual damages connected to its services in relation to third parties with respect to provable damages that occur solely on account of the chargeable violation of its obligations.
- The Certification Service Provider is not liable for damages that result from its inability to tend to its information provision and other communication related obligations due to the operational malfunction of the Internet or one of its components because of some kind of external incident beyond its control.
- If The Certification Service Provider engages data comparison with an authentic database before the issuance of the Subject's Certificate, it relays on the data received from the authentic database. The Certification Service Provider will not assume any liability for damages arising out of the inaccuracy of information provided by such authentic databases.
- The Certification Service Provider assumes liability solely for providing the services in accordance with the provisions of this Certification Practice Statement, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

Administrative Processes

The Certification Service Provider logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

Financial Liability

[[QUA:
The Certification Service Provider has appropriate deposit according to the relevant legal requirements for its financial liability and to guarantee costs related to its termination and for reliability.
]]

The Certification Service Provider has liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

[[QUA:

<TLS: The Certification Service Provider limits the obligation for compensation related to services, this limit is 6.000.000,-HUF per Subscriber or Relying Party per EV Certificate.

>

<not TLS: <not UNI:

The Certification Service Provider does not limit the highest level of the obligation undertaken at the same time.

In connection with the services provided as a qualified provider, the Certification Service Provider defines tariff packages, which differ from each other in the financial liability of the Certification Service Provider as stated below.

Certificate type	Limitation of the provider liability [M HUF]
basic	0,02
bronze	1
silver	5
gold	20
platinum	200

>>

]]

[[ADV:

<TLS: The Certification Service Provider limits the obligation for compensation related to services, the extent of this limitation is 4.000.000,-HUF per damage event.

If the valid claim of several entitled parties related to a damage event exceeds the limitation defined for a damage event, then the compensation of the claims takes place in a relative ratio to the limitation. >

<not TLS: <not UNI:

The Certification Service Provider does not limit the highest level of the obligation undertaken at the same time. The Certification Service Provider limits its compensation obligation related to its services, the rate of this limitation is:

- *related to Certificates belonging to the III. certification class, 100.000,-HUF per insurance incident*
- *related to Certificates belonging to the II. certification class, 100.000,-HUF per insurance incident*

>>

<UNI:

The Certification Service Provider limits the obligation for compensation related to services, the extent of this limitation is 100.000,-HUF per damage event.

>

]]

<not TLS:

If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

>

9.9 Indemnities

9.9.1 Indemnification by the Certification Service Provider

The detailed rules of the indemnities of the Certification Service Provider are specified in this regulation (see section: 9.8), the service agreement and the contracts concluded with the Clients.

9.9.2 Indemnification by Subscribers

The Subscriber and the Subject are liable for damages to the Certification Service Provider for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3 Indemnification by Relying Parties

See section: 9.8.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific Certification Practice Statement is specified on the cover of the document.

9.10.2 Termination

The Certification Practice Statement is valid without a time limit until withdrawal or the issuance of the newer version of the Certification Practice Statement.

Section 9 of the Certification Practice Statement shall remain effective even after the termination of the Certification Practice Statement's effect (regardless of the manner in which effectiveness is terminated) in connection with any and all Certificates which the Certification Service Provider will have issued while the Certification Practice Statement was effective.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the Certification Practice Statement the Certification Service Provider publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal via its website.

The Certification Service Provider guarantees that in case of a the Certification Practice Statement withdrawal, requirements for the protection of the confidential data remain in effect.

9.11 Individual Notices and Communications with Participants

The Certification Service Provider maintains a customer service in order to contact with its Clients.

Unless otherwise provided for in the GTC or in an individual contract, Clients may make their legal declarations to the Certification Service Provider in writing and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

Issued Certificates may also be <not TLS: suspended> <TLS: revoked> by sending an SMS. Notifications of other nature may also be given in writing, in the form of electronic mail or fax.

The e-Szignó Certification Authority informs its Clients by means of publication via its website or in electronic mail.

9.12 Amendments

The Certification Service Provider reserves the right to change the Certification Practice Statement in a controlled way in case of the change of normative rules, security requirements, market conditions or other circumstances.

9.12.1 Procedure for Amendment

The Certification Service Provider only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The Certification Service Provider has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 8.4 audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the Certification Service Provider's organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certification Authority.

The team produces internal, non-public working copies of the regulations as it collects changes, and these undergo internal review before being published. The Certification Service Provider strives to only issue new regulations at the least frequent intervals possible.

The Certification Service Provider reviews the Certification Practice Statement annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change – or in case of the annual review even if no changes are made to the document – and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document **[[QUA: will be sent for review to the National Media and Infocommunications Authority 30 days prior to the planned entry into force date, and it]]** will be published via the website of the Certification Service Provider.

[[QUA:

The Certification Service Provider will accept remarks connected to new regulations published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

In case of observations that require substantive changes, the document will be amended.

The Certification Service Provider will close and publish the version of the regulation as amended with remarks on the 7th day prior to its becoming effective.

]]

9.12.2 Notification Mechanism and Period

The Certification Service Provider notifies the Relying Parties of new document version issuances as described in Section 9.12.1.

9.12.3 Circumstances Under Which OID Must Be Changed

The Certification Service Provider issues the new version with a new version number even in the case of the smallest change to the Certification Practice Statement, in which either the main version number or the sub-version number changes depending on the extent of the change.

In versions 1.x and 2.x, the version number of the Certification Practice Statement appeared in the 2 tags at the end of the OID of the document identifier, so two Certification Practice Statement with different contents - brought into force - could not have the same OID identifier.

Starting with Certification Practice Statement version 3.1, the version number does not appear at the end of the OID, so the Certification Practice Statement OID identifier has the same value in all released versions. Individual Certification Practice Statement can be identified by using the document OID and version number together.

9.13 Dispute Resolution Provisions

The Certification Service Provider aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The Certification Service Provider and the Client mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The Client in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the Certification Service Provider or the use of issued Certificates shall be addressed to the customer care centre office in written form. The Certification Service Provider notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The Certification Service Provider is obliged to issue a written response to the submitter within the specified time limit. The Certification Service Provider may request the provision of information required for giving a response from the submitter. The Certification Service Provider investigates complaints within 30 days and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the Certification Service Provider involved, the submitter may initiate consultation with the Certification Service Provider and the Relying Parties. All participants

of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof, and the submission, the Certification Service Provider's response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The Relying Parties shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

9.14 Governing Law

The Certification Service Provider at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the Certification Service Provider contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

9.15 Compliance with Applicable Law

The applicable regulations:

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1]
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [9]
- (Hungarian) Act V of 2013. on the Civil Code [10]
- (Hungarian) Act CIII of 2023 on the digital state and certain rules for the provision of digital services [13]

<not UNI:

- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [14]
- (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates [15]
- (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body [17]

> <not TLS: <not UNI:

- (Hungarian) Government Decree 137/2016. (VI. 13.) on the requirements for the use of electronic signatures and seales related to the provision of electronic administration services [16]

>>

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

The providers operating according to this Certification Practice Statement may only assign their rights and obligations to a third party with the prior written consent of Certification Service Provider.

9.16.3 Severability

Should some of the provisions of the present Certification Practice Statement become invalid for any reason, the remaining provisions will remain in effect unchanged.

<TLS:

In case of a conflict between national or EU legislation and the mandatory requirements of the **[[QUA: CABF EV Guidelines [65] or the]]** CABF BR [63], the Certification Service Provider notifies the CAB Forum of the facts, circumstances, and law(s) involved prior to the issuance of conflicting certificates.

>

[[QUA:

<not TLS: <not UNI:

In case of a conflict between national or EU legislation and the mandatory requirements of the CABF S/MIME BR [62], the Certification Service Provider notifies the CAB Forum of the facts, circumstances, and law(s) involved prior to the issuance of conflicting certificates.

>>

]]

<UNI:

In case of a conflict between national or EU legislation and the mandatory requirements of the CABF S/MIME BR [62], the Certification Service Provider notifies the CAB Forum of the facts, circumstances, and law(s) involved prior to the issuance of conflicting certificates.

>

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The Certification Service Provider is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the Certification Service Provider does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present Certification Practice Statement, it would waive the enforcement of claims for damages.

9.16.5 Force Majeure

The Certification Service Provider is not responsible for the defective or delayed performance of the requirements set out in the Certificate Policy and the Certification Practice Statement if the reason for failure or delay was a condition that is outside the control of the Certification Service Provider.

9.17 Other Provisions

No stipulation.

A Interpretation of the short policy names

For the simpler handling of the Certificate Policies the Certification Service Provider defines a five characters long short name (identifier) for each Certificate Policy, where each character is meaningful and defines some basic features of the given policy according to the following rules:

- First character [?....]
  - M: Certificate Policy for qualified Certificates

  <UNI:
  - N: Certificate Policy for non-qualified Certificates

  > <not UNI:
  - N: Certificate Policy for non-qualified Certificates

  >
  - H: Certificate Policy for non-qualified, III. certificate class Certificates
  - K: Certificate Policy for non-qualified, II. certificate class Certificates
  - A: Certificate Policy for non-qualified, automatic issuance Certificates
  - x: no stipulation
- Second character [.?...]
  - A: Certificate Policy for Signature Creation Certificates
  - B: Certificate Policy for Seal Creation Certificates
  - W: Certificate Policy for Website Authentication Certificates
  - P: Certificate Policy for PSD2 Website Authentication Certificates
  - K: Certificate Policy for Code Signing Certificates
  - S: Certificate Policy for Email (S/MIME) Certificates

  <UNI:
  - Z: Certificate Policy for Wallet RPA Certificates

  > <not UNI:
  - Z: Certificate Policy for Wallet RPA Certificates

  >
  - E: Certificate Policy for other purpose Certificates
- Third character [..?..]
  - T: Certificate Policy for Certificates issued to a natural person
  - J: Certificate Policy for Certificates issued to a legal person

  - x: no stipulation, can be issued to any type of Subject

- Fourth character [...?.]
  - B: Certificate Policy for Certificates issued on Qualified Electronic Signature or Seal Creation Device
  - H: Certificate Policy for Certificates issued on Cryptographic Hardware Device
  - S: Certificate Policy for Certificates issued as a software token
  - x: no stipulation, it can be issued on any platforms
- Fifth character [....?]
  - A: Certificate Policy for pseudonymous Certificates
  - N: Certificate Policy for non-pseudonymous Certificates

B REFERENCES

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC .

[2] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC .

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

[4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework .

[5] 2024/2690 (18.10.2024) COMMISSION IMPLEMENTING REGULATION (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers .

[6] (Hungarian) Act LXVI of 1992 on the registration of citizens' personal data and address .

[7] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

[8] (Hungarian) Act II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[9] (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information .

[10] (Hungarian) Act V of 2013. on the Civil Code .

[11] (Hungarian) Act CCXXII of 2015 on the general rules of electronic administration and trust services .

[12] (Hungarian) Act CXXX of 2016 on Civil Procedure .

[13] (Hungarian) Act CXIII of 2023 on the digital state and certain rules for the provision of digital services .

[14] (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services .

[15] (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates .

[16] (Hungarian) Government Decree 137/2016. (VI. 13.) on the requirements for the use of electronic signatures and stamps related to the provision of electronic administration services .

[17] (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body .

[18] (Hungarian) Government Decree 541/2020. (XII. 2.) on Other Methods of Identification Recognized at National Level as Providing Trust Equivalent to Personal Presence in the Case of Trust Services.

[19] A Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) hitelesítési rendje, http://www.kgyhsz.gov.hu/KGYHSZ_HR_v1.0.pdf, 1.0.

[20] ETSI EN 301 549 V3.2.1 (2021-03); Harmonised European Standard; Accessibility requirements for ICT products and services.

[21] ETSI EN 319 401 V3.2.1 (2026-01); Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[22] ETSI EN 319 403-1 V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

[23] ETSI EN 319 411-1 V1.5.1 (2025-04); Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[24] ETSI EN 319 411-2 V2.6.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[25] ETSI EN 319 412-1 V1.6.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[26] ETSI EN 319 412-2 V2.4.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

[27] ETSI EN 319 412-3 V1.3.1 (2023-09); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[28] ETSI EN 319 412-4 V1.4.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

[29] ETSI EN 319 412-5 V2.5.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[30] ETSI TS 119 312 V1.5.1 (2024-12); Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites.

[31] ETSI TS 119 411-5 V2.1.1 (2025-02); Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Implementation of qualified certificates for website authentication as in amended Regulation 910/2014.

[32] ETSI TS 119 411-6 V1.1.1 (2023-08); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

[33] ETSI TS 119 461 V2.1.1 (2025-02) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.

[34] ETSI TS 119 495 V1.7.1 (2024-07); Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

[35] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[36] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

[37] ISO/IEC 15408 (parts 1 to 3) Information technology - Security techniques - Evaluation criteria for IT security.

[38] ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.

[39] IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.

[40] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

[41] IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.

[42] IETF RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, January 2005.

[43] IETF RFC 4035: Protocol Modifications for the DNS Security Extensions, March 2005.

[44] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.

[45] IETF RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs), May 2006.

[46] IETF RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environment, September 2007.

[47] IETF RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, March 2008.

[48] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[49] IETF RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC, October 2009.

[50] IETF RFC 5952: A Recommendation for IPv6 Address Text Representation, August 2010.

[51] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

[52] IETF RFC 6840: Clarifications and Implementation Notes for DNS Security (DNSSEC), February 2013.

[53] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.

[54] IETF RFC 6962: Certificate Transparency, June 2013.

[55] IETF RFC 8555: Automatic Certificate Management Environment (ACME), March 2019.

[56] IETF RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019.

[57] IETF RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses, October 2023.

[58] IETF RFC 9654: Online Certificate Status Protocol (OCSP) Nonce Extension, August 2024.

[59] ITU X.501 Information technology - Open Systems Interconnection - The Directory: Models.

[60] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[61] ITU X.520 Information technology - Open Systems Interconnection - The Directory: Selected attribute types.

[62] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates, v.1.0.13. CA/Browser Forum, `https://cabforum.org/baseline-requirements-documents/`, 2026.

[63] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, v.2.2.6. CA/Browser Forum, `https://cabforum.org/baseline-requirements-documents/`, 2026.

[64] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, v.3.10.0. CA/Browser Forum, `https://cabforum.org/baseline-requirements-code-signing/`, 2025.

[65] Guidelines for the Issuance and Management of Extended Validation Certificates, v.2.0.1. CA/Browser Forum, `https://cabforum.org/extended-validation/`, 2024.

[66] CA/Browser Forum Network and Certificate System Security Requirements, v.2.0.5. CA/Browser Forum, https://cabforum.org/network-security-requirements/, 2025.

[67] Common CA Database Policy, v.2.0,. https://www.ccadb.org/policy, 2025.

[68] Chrome Root Program Policy, v.1.8,. https://googlechrome.github.io/chromerootprogram/, 2026.

[69] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[70] FIPS PUB 140-3 (2019 March 22): Security Requirements for Cryptographic Modules.

[71] NIST Special Publication 800-56A Revision 3 (April 2018): Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

[72] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.

[73] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.

[74] EU/EEA Trusted List Browser, (https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/t

[75] Magyarország (Hungary): Trusted List (http://www.nmhh.hu/tl/pub/HU_TL.pdf).

[76] PRADO - Public Register of Authentic identity and travel Documents Online, https://www.consilium.europa.eu/prado/en/prado-start-page.html .

[77] e-Szignó Certification Authority - eIDAS conform Unified Certificate Policies.

[78] e-Szignó Certification Authority - Qualified Signing Certificate Policies .

[79] e-Szignó Certification Authority - General Terms and Conditions. .

[80] Microsec ltd. - Information on online video identification terms .