MICROSEC

e-Szignó Certification Authority

Unified Certificate Policies

ver. 3.20

Date of effect: 2026-05-13

OID	1.3.6.1.4.1.21528.2.1.1.229
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 policies.
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. **[[QUA:** **<SIG:** **- S/MIME certificates for qualified signature. >** **<SEA:** **- S/MIME certificates for qualified seal. >** **]]**
3.11	2023-12-19	- Revision. <SIG: - Natural person identity validation based on electronic signature. > **[[QUA:** **<not TLS:** **- EKU in S/MIME certificates.** **- S/MIME revocation rules.** > **]]** <UNI: - S/MIME revocation rules. >
3.12	2024-04-03	- Removing SerialNumber extension.
3.14	2024-09-01	- Revision. - Change in Hungarian and EU legal requirements. - Self Audit. - Router and firewall logging. - Initial identity validation. - Reuse of validation materials. - Revocation reasons and deadlines. - Move Certificate fields from 7.1.1 to 7.1.2

Version	Effect date	Description
3.15	2025-03-12	- Global revision. - 2024/2690 Committee order. - Cryptographic requirements. - 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. >
3.17	2025-09-15	- Revision. - Key management. <TLS: - Mass revocation plan and test. - Retire some domain validation methods. - Announced changes in certificate validities. **[[QUA:** **- Increased validity for PSD2 certificates.** **]]** - DNSSEC validation. >

Version	Effect date	Description
3.18	2025-12-22	- Revision. - Improve rules for using revocation reasons. - Correct OCSP nocheck OID. **[[QUA:** **<not TLS: >** **]]** **[[QUA:** **- Conformance to EN 301 549.** **]]**
3.19	2026-04-02	- Revision. - 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 contains the Certificate Policy defined by e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or Certification Service Provider) concerning the issuance of several type of certificates service.

- **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 <SIG: electronic signature certificate> sample in a flowing text ...

or

<SIG:
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 <SEA: electronic seal certificate> sample in a flowing text ...

or

<SEA:
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.

<TLS:
The Certificate Policy complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU **[[QUA: qualified]]** Trust Service.
>
<SIG:
The Certificate Policy complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU **[[QUA: qualified]]** Trust Service.
>
<SEA:
The Certificate Policy 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 according to the requirements of this Certificate Policy can fulfil the requirements of CA/Browser Forum EV (Extended Validation) Certificates [62].
]]
>

1.1 Overview

The Certificate Policy is a "set of rules that specify a Certificate's usability for a community and/or a class of applications with common security requirements". The content and format of this document complies with the requirements of the IETF RFC 3647 [38] framework. It consists of 9 sections that contain the security requirements, processes and the practices defined by the Certification Service Provider to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, section headings where the Certificate Policy does not impose a requirement have the statement "No stipulation".

This document contains the requirements of multiple Certificate Policies. The vast majority of the requirements defined in the document applies to all of the Certificate Policies uniformly and are not otherwise mentioned. In case of requirements to be treated differently it will be clearly defined which Certificate Policies the given requirement refers to.

The Certificates issued in accordance with this document shall indicate the identifier (OID) of the Certificate Policy that they comply to. Relying Parties can ascertain the applicability and reliability of the Certificates based on the identifier regarding a specific application.

The Certificate Policys set out basic requirements related to Certificates in particular for the Certificate issuer Certification Service Provider. The manner how these requirements are met, and a detailed description of the methods mentioned here shall be included in the Certification Practice Statement issued by the Certification Service Provider.

The Certificate Policy is one of several documents issued by the Certification Service Provider that collectively govern conditions of the services provided by the Certification Service Provider. Other important documents include General Terms and Conditions, Certification Practice Statements, and other customer and partner agreements.

Section 1.6 of this document specifies several terms, which are not used or not fully in this sense used in other areas. In this document, terms used in this sence are always capitalized and are written in italics.

1.2 Document Name and Identification

The present document is a Certificate Policy collection, the main identification data of which are:

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

The list and identification information of the Certificate Policies described by the present document can be found in section 1.2.1.

1.2.1 Certificate Policies

All Certificates issued by the Certification Service Provider shall 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

The present document defines 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*

]]

>

<SIG:

[[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*

]]

>

<SEA:

[[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.

<TLS:

Based on these Certificate Policies the Certification Service Provider can issue Certificates used for webserver authentication.

>

<UNI:

Based on these Certificate Policies the Certification Service Provider can issue Certificates for multiple uses (encryption, authentication etc.). (The list of uses that can be specified is described in the Certificate extension section 7.1.2.)

>

[[ADV:

<SIG:

Based on these Certificate Policies the Certification Service Provider can issue 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.

>

<SEA:

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 [65] certification according to CEN SSCD PP [66], at least at level EAL-4**
- **an EAL-4 or higher level Common Criteria [65] certificate according to CEN 419 221-5 [33]**
- **FIPS 140-2, Level 2 (or higher) certification [63]**
- **FIPS 140-3, Level 2 (or higher) certification [64].**

]]

>

<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 [65] certificate according to CEN SSCD PP [66], at least at level EAL-4
- an EAL-4 or higher level Common Criteria [65] certificate according to CEN 419 221-5 [33]
- FIPS 140-2, Level 2 (or higher) certificate [63]
- FIPS 140-3, Level 2 (or higher) certificate [64].

>

[[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 [11] is representing conclusive evidence (in Hungary).

>
]]
Among the present Certificate Policies:
<TLS:
[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [21] standard*
- *each Certificate Policy complies with the [DVCP] Certificate Policy defined in the ETSI EN 319 411-1 [21] 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 [21] 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 [21] 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 [22] standard**
    - **each Certificate issued for PSD2 purposes complies also with the [QCP-w-psd2] Certificate Policy defined in the ETSI TS 119 495 [32] 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 [22] standard**
    - **each Certificate issued for PSD2 purposes complies also with the [QCP-w-psd2] Certificate Policy defined in the ETSI TS 119 495 [32] specification.**

]]
>
<SIG:
[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [21] 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 [22] 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 [21] standard.**

]]
>
<SEA:
[[ADV:

- *each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [21] 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 [22] 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 [21] standard.**

]]
>
<UNI:

- each Certificate Policy complies with the [LCP] Certificate Policy defined in the ETSI EN 319 411-1 [21] 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*	

]]

>

<SIG:

[[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*		

]]

>

<SEA:

[[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

This Certificate Policy collection is in effect from the 2026-05-13 date of entry into force to withdrawal. The effect automatically terminates at the issuance of the newer version of the Certificate Policy.

The present Certificate Policy collection and the Certification Practice Statements based on these policies should be reviewed at least annually and their amendment to the potentially changed requirements and prerequisites shall be ensured.

The effect of the Certificate Policy extends to each of the participants mentioned in section 1.3.

Present Certificate Policy collection include specific requirements for services primarily provided for Hungarian Clients, operating by the Hungarian law in Hungary in Hungarian language. The Certification Service Provider can extend the geographical scope of the service; in this case, it shall use not less stringent requirements than those applicable to Hungarian conditions. The details shall be recorded in the Certification Practice Statement.

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

1.3.1 Certification Authorities

The Certification Service Provider is a Trust Service Provider that issues Certificates within the framework of a Trust Service, and performs the related tasks. For example identifies the applicant person, manages records, accepts the changes related to the Certificates, and publishes the policies related to the Certificate, public keys and information on the current state of the Certificate (in particular about its possible revocation). (This activity is also called Certification service.)

The requirements of the present document apply to every Certification Service Provider who undertake in their the Certification Practice Statement the compliance with any of the Certificate Policy(s) described in the present document.

1.3.2 Registration Authorities

See the definition in section 1.6.

The Registration Authority can operate as a part of the Certification Service Provider, but it can be a separate, independent organization as well. The operation of the Registration Authority shall meet the requirements described in the relevant Certificate Policies, Certification Practice Statements, and other documents. Regardless of the chosen resolution the Certification Service Provider is in all cases fully responsible for the proper operation of the Registration Authority.

In case of an independent Registration Authority, the Certification Service Provider shall contractually oblige the Registration Authority to comply with the relevant requirements.

<TLS:

The Certification Service Provider shall not delegate the validation of the FQDN *[[ADV: and IP address]]* according to the section 3.2.2 to an independent Registration Authority. The validation shall be done by the internal Registration Authority of the Certification Service Provider.

>

1.3.3 Subscribers

Subscribers define the scope of Subject or Applicants using the service, and Subscribers also cover the service fees related to the usage of these services.

<TLS: The Applicant is that natural person, who acts during the application for Website Authentication Certificate.>

<SIG: The Subject is that natural person, whose data is indicated on the Certificate.>

<SEA: The Subject is that legal person, whose data is indicated on the Certificate.>

<UNI: The Subject is that natural or legal person, whose data is indicated on the Certificate.>

<not TLS: <not UNI:

In case of a Certificate for electronic signature or seal purposes, the Subject is the creator of the electronic signature or seal.

>>

1.3.4 Relying Parties

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

1.3.5 Other Participants

The independent auditor who makes the conformity assessment audit.

The supervisory authority.

1.4 Certificate Usage

The Certificate usability area is essentially determined by the Certificate attribute values set by the Certification Service Provider beside which the Certificate Policy and the Certification Practice Statement may also contain additional restrictions.

1.4.1 Appropriate Certificate Uses

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

<SIG: 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. > <SEA: 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.). >

[[QUA:

<not TLS:

In case of Certificate Policies requiring Qualified Electronic Signature or Seal Creation Device usage <SIG: ([MATBN]) > <SEA: ([MBJBN])> the private key belonging to the qualified Certificate is protected by the Qualified Electronic Signature or Seal Creation Device that was issued within the confines of the electronic signature or seal qualified certificate issuance service. Certificates issued according to these polices are suitable for qualified electronic signature or seal generation.

If a Certificate Policy does not require the usage of a Qualified Electronic Signature or Seal Creation Device, then the electronic signature or seal based on a certificate issued according that policy can be considered a qualified certificate based advanced electronic <SIG: signature.> <SEA: seal.> >

<SIG:

A document, with a qualified electronic signature or a qualified certificate based advanced electronic signature under the paragraph 325 of Act CXXX of 2016 on Civil Procedure [11] is a notarial or private document representing conclusive evidence.

>

<SEA:

A document, with a qualified electronic seal under the paragraph 99. of Act CCXXII. [10] of 2015. on general rules about electronic administration and trust services shall be considered a document representing conclusive evidence.

>

]]

[[ADV:

<SIG:

The Certificate issued according to the present Certificate Policies is suitable for advanced electronic signature creation. The document certified by an advanced electronic signature meets the requirements for phrasing according to Hungarian legislation.

>

<SEA:

The Certificate issued according to the present Certificate Policies is suitable for advanced electronic seal creation. The document certified by an advanced electronic seal meets the requirements for phrasing according to Hungarian legislation.

>

]]

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 Certificate Policy 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 Certificate Policy 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 shall maintain a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report. The Certification Practice Statement shall contain the way how to issue the report.

>

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

The provider that issued the Certification Practice Statement is responsible for its compliance with the Certificate Policy referenced in it and for the provision of the service in harmony with the regulations contained therein.

<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

The Certification Service Provider shall describe the acceptance procedure of the Certification Practice Statement that announces its conformity with the present Certificate Policy in the given Certification Practice Statement.

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]]* . > <SIG: 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. > <SEA: 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. >
<SIG: 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.
> <SEA: 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 [51], which stores the issued Certificates and the corresponding PreCertificates.
>	
<SIG:	

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).
>	
<SEA:	
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.
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 [51], 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:
<SIG:

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.**

>
<SEA:

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. > <SIG: Recipient of the electronic document, who acts relying on the electronic signature based on a given certificate. > <SEA: 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.
<SIG: 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.
> <SEA: 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<SIG: , 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.

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. [12] 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. > <SIG: In case of electronic signatures the creator of the electronic signature or seal generates the signature with the help of the private key. > <SEA: 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.**
]]	
<SIG:	
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).

>
<SEA:

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. > <SIG: 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). > <SEA: 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. <SEA: 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 <SIG: (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: >
]]

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 shall disclose the contractual conditions and policies electronically via its website.

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

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

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

After concluding the contract, the Certification Service Provider shall make the individual Service Agreement, 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 on a durable medium, or in a way that can be downloaded to the Client.

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

2.2 Publication of Certification Information

The Certification Service Provider shall disclose via its website

- its provider Certificates
- all Cross Certificates that identify the Certification Service Provider as the Subject, provided that the Certification Service Provider arranged for or accepted the establishment of the trust relationship
- the end user Certificates in case of the Subject or Applicant's prior consent.

Service Provider Certificates

With the following methods the Certification Authority shall disclose 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 shall be available via the website of the Certification Authority.
- The status change of Certificates of intermediate (non-root) certification units shall be 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 – shall issue a Certificate with extremely short period of validity thereby eliminating the need for Certificate revocation status verification.

  Each OCSP responder Certificate shall contain 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 shall disclose 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 shall be 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. For status information disclosing methods, see Section 4.10.

The Certification Service Provider shall guarantee, 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% annually, while service downtimes may not exceed 3 hours in each case.

<TLS:
The Certification Service Provider shall publish through known Certificate Transparency Log providers those PreCertificates, the publication of which is consented by the Applicant.
>

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 [68] 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, shall follow the practices below:

- the Certificates of the root certification units operated by it shall be disclosed before commencing the service
- the Certificates of the intermediate certification units operated by it shall be disclosed within 5 workdays after issuance

<TLS:

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

>

- the Certification Service Provider shall disclose 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 shall be available immediately within the confines of the online certificate status service.

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

2.4 Access Controls on Repositories

The provided information shall be 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 shall prevent the unauthorized changes to the information with various protection mechanisms.

<TLS:

2.5 Websites for testing

The Certification Service Provider shall operate special test websites to test and demonstrate the operation and usability of the valid, expired and revoked Website Authentication Certificates.

>

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 present Certificate Policies.

The indicated Issuer ID and the Subject ID amongst the basic fields of the Certificate shall comply with the ITU X.520 standard [58], the RCF 5280 [45] and IETF RFC 6818 [48] recommendations name-specific format requirements, in addition the Certification Service Provider shall support the "Subject Alternative Names" and "Issuer Alternative Names" fields located amongst the extension.

3.1.1 Types of Names

Denomination of the Subject

The present Certificate Policy requires the following related to the Certificate's subject id (Subject field):

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

  <TLS:

  If present, this field shall contain 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 [40], 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 [47], Section 4. pg. 81

  ]]

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

  Usage is optional.

  The Website Authentication Certificate shall not be pseudonymous.

  >

  <SIG:

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

  >

  <SEA:

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

  >

  <UNI:

  In case of natural persons, the name of the natural person Subject shall be 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 shall be in this field in the same form as verified by the Certification Service Provider according to the section 3.2.2.

>

<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).

Filling is required.

>

<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 shall not be filled.

]]

[[ADV:

It shall not be filled.

]]

>

<SIG:

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

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

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

>

<SEA:

It shall not be filled.

>

<UNI:

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

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

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

>

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

  <TLS:

  [[QUA:

  It shall not be filled.

  ]]

  [[ADV:

  It shall not be filled.

  ]]

  >

  <SIG:

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

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

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

  >

  <SEA:

  It shall not be filled.

  >

  <UNI:

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

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

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

  >

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

  <TLS:

It shall not be filled.

>

<SIG:

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 shall not be filled out.

]]

>

<SEA:

It shall not be 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 shall not be filled.

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

>

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

<TLS:

It shall not be filled.

>

<SIG:

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 shall not be filled out.

]]

>

<SEA:

It shall not be 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 shall not be filled.

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

>

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

  It may be filled only in case of a pseudonymous Certificate.

  <UNI:

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

  >

- 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 compulsory, 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 [42] 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 shall contain one filled out "Serial Number" field.

]]

[[ADV:

The Certificate shall not contain the "Serial Number" field.

]]

>

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

<TLS:

[[ADV:

In case of DVCP Certificate it shall not be filled.

]]

[[QUA:

The

]]

[[ADV:

In case of OVCP Certificate the

]]

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

>

<SIG:

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

>

<SEA:

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

>

<SIG:

In case of an Organizational Certificate the field shall be filled out.

[[QUA:

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

]]

[[ADV:

In case of Code Signing Certificate issued to a natural person, the field is mandatory, the name of the natural person should be written here.

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

]]

>

<SEA:

The field shall be filled out.

>

<UNI:

In case of an Organizational Certificate the field shall be filled out.

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

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

>

In case of a provider Certificate issued for a Trust Service Provider, the "O" field is mandatory, and the real name of the organization providing the service shall be 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.

>

<SIG:

In case of an Organizational Certificate the identifier of the Organization indicated in the "O" field may be in this field.

>

<SEA:

The identifier of the Organization indicated in the "O" field may be in this field.

>

<UNI:

In case of an Organizational Certificate the identifier of the Organization indicated in the "O" field may be in this field.

>

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

<TLS:

[[ADV:

In case of DVCP Certificate this field shall not be filled.

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

]]

[[QUA:

Filling out the field is optional.

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

]]

>

<SIG:

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

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

[[QUA:

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

]]

>

<SEA:

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 shall not be filled out.

In case of Organization- and Sponsor validated Email (S/MIME) Certificate it shall be 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 shall contain 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 [32], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [23] specification.

]]

>

<SEA:

[[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 shall contain 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 [32], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [23] 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 shall contain 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 [32], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [23] specification.

]]

>

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

<TLS:

This field shall not be filled out in Certificates.

>

<SIG:

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.

>

<SEA:

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.

>

<SIG:

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

>

<UNI:

In case of personal – not related to any organization – Certificates this field shall not be 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 [34] - 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 [34] - 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 [34] - 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 [34] - of the place of incorporation of the Organization indicated in the "O" field.

  ]]

  >

  <SIG:

  In case of an Organizational Certificate the two-letter country code - according to ISO 3166-1 [34] - 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 [34] - of the country which issued the document used for the identification of the Subject.

  >

  <SEA:

  The two-letter country code - according to ISO 3166-1 [34] - 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 [34] - 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 [34] - of the country which issued the document used for the identification of the Subject.

>

Filling out is required.

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

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

<TLS:

[[QUA:

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

If it is filled all data shall be verified by the Certification Service Provider.

]]

[[ADV:

In case of DVCP Certificate it shall not be filled.

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

If it is filled all data shall be verified by the Certification Service Provider.

]]

>

<SIG:

In case of an Organizational Certificate, the address is according to the organization's place of incorporation. Optional field, if filled, only verified information can be indicated.

Its use is prohibited in case of Certificates not related to an Organization.

>

<SEA:

The address is according to the organization's place of incorporation. Optional field, if filled, only verified information can be indicated.

>

<UNI:

In case of an Organizational Certificate, the address is according to the organization's place of incorporation. Optional field, if filled, only verified information can be indicated.

Its use is prohibited in case of Certificates not related to an Organization.

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

>

- 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 shall not be filled.

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

]]

>

<SIG:

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 shall not be filled.

>

<SEA:

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 locality of the official address of the natural person should be written here. The value of the field can also be presented without an accent.

In case of other Certificate not related to an Organization, it shall not be 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 shall not be 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.

]]

>

<SIG:

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

Optional field.

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

>

<SEA:

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

Optional field.

>

<UNI:

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

Optional field.

In case of a Certificate not related to an Organization, it shall not be 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 shall not be 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.

]]

>

<SIG:

In case of Organizational Certificate, the postal code of the Organization's place of incorporation. If filled, only verified information can be indicated.

Optional field.

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

[[QUA:

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

]]

>

<SEA:

The postal code of the Organization's place of incorporation. If filled, only verified information can be indicated.

Optional field.

[[QUA:

In case of Email (S/MIME) Certificate it shall not be 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.

Optional field.

In case of a Certificate not related to an Organization, it shall not be 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:

Shall not be filled.

>

<SIG:

The natural person Subject's role, title or job.

In special cases the Certification Service Provider may include more "Title" fields in the Certificate.

>

<SEA:

The natural person Subject's role, title or job.

Shall not be filled.

>

<UNI:

The natural person Subject's role, title or job.

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:

  Shall not be filled.

  >

  <not TLS:

  Filling is optional.

  If filled, it shall be 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 Certificate Policies might contain further "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 shall always contains at least one entry.
  Filling is required.
  Each entry shall be *[[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 [45], 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 [45], and thus shall not contain domain name containing underscore ("_") character.

>

<SIG:

- 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 shall verify the names to be indicated on "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 shall verify the names to be indicated on "Subject Alternative Names" extension.

>

<SEA: >

<UNI:

>

<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 definitely shall be filled out.
<UNI:
In case of Email (S/MIME) Certificate it always shall be filled out.
>
[[QUA:
<SIG:
In case of Email (S/MIME) Certificate it always shall be filled out.
>
<SEA:
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.
Further "Subject Alternative Names" extension field usage is permitted.

<UNI:

– In case of national WRPAC Certificate, the "Subject Alternative Names" extension shall always contain 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 [45], and thus shall not contain domain name containing underscore ("_") character.

>
>

<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.

]]
>

3.1.2 Need for Names to be Meaningful

The following rules shall be 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.*

]]
>
<SIG:

- 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. >
<SIG: The Certification Service Provider doesn't issue Certificate with pseudonym.>
<SEA: 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 shall have a unique name in the Certificate Repository of the Certification Service Provider. In order to ensure the uniqueness, the Certification Service Provider shall assign each Subject an identifier (OID) – unique in the Certification Service Provider's register – which – unless prohibited by other requirements – shall be included in the Subject's unique identifier "Subject DN Serial Number" field,

<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 shall ensure 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

When the Certification Service Provider includes trademark in the fields of the end-user Certificate, than it shall make sure of it's legitimate use.

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 shall ensure and make sure that the Applicant actually owns or manages the private key belonging to the public key of the Certificate.

The manner of the requirement fulfilment shall be recorded in the Certification Practice Statement.

<not TLS:

[[QUA:

If the Subject private key is generated and managed by another Trust Service Provider, then the Trust Service Provider is bound to verify that, the referred Trust Service Provider owns the private key, and it is under the sole control of the Subject.

]]

>

3.2.2 Authentication of an Organization Identity <TLS: or a Domain>

<TLS:

3.2.2.1 Authentication of organization identity

>

Prior to the issuance of an Organizational Certificate the Certification Service Provider shall verify the organizational data authenticity to be on the Certificate based on trusted third party or authentic public registers.

The name of the Organization shall be indicated on the Organizational Certificate s according to the specifications in Section 3.1.1.

The Certification Service Provider can issue the Organizational Certificate exclusively with the consent of the Organization. Natural persons acting on behalf of the Organization shall be duly authorized; the individual's identity shall be verified according to the requirements set out in Section 3.2.3.

According to the trademarks indicated in the Certificate see the chapter 3.1.6.

The Certification Practice Statement shall determine the detailed procedural rules.

<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 shall ensure 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 may only issue 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 may only issue Certificates only for those top-level domains which can be found on the actual IANA Root Zone Database.

The Certification Service Provider shall support the usage of the Internationalized Domain Names according to the IDNA2003 [37] requirements.

The Certification Service Provider shall not issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

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 [60].

DNSSEC validation back to the IANA DNSSEC root trust anchor shall 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 shall :

- perform DNSSEC validation using the algorithm defined in RFC 4035 [41] Section 5, and
- support NSEC3 as defined in RFC 5155 [44], and
- support SHA-2 as defined in RFC 4509 [43] and RFC 5702 [46], and
- properly handle the security concerns enumerated in RFC 6840 [49] 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 shall 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.

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 Random Value or Request Token either in a DNS CNAME, TXT or CAA record for either

- an Authorization Domain Name or
- an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the Certification Service Provider shall provide a Random Value unique to the Certificate request and shall not use the Random Value after

- 30 days or
- if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate.

The Certification Service Provider shall implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [60].

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 shall not accept redirects (3xx HTTP status code).
The Random Value included in the Request Token:

- shall be unique to each Certificate Application
- may remain valid for use in a confirming response for no more than 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 shall implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [60].
[[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 [52].

- 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 shall not accept redirects (3xx HTTP status code).

The Random Value included in the Request Token:

- shall be unique to each Certificate Application

- may remain valid for use in a confirming response for no more than 30 days from its creation.

The Certification Service Provider shall implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [60].

[[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 shall implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 of CABF BR [60].

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 shall ensure that, the Applicant is the authorized*

user of the entire domain namespace covered by the wildcard domain name. The Certification Service Provider shall 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.*

]]

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 [53] 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 shall 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 shall :

- perform DNSSEC validation using the algorithm defined in RFC 4035 [41] Section 5, and
- support NSEC3 as defined in RFC 5155 [44], and
- support SHA-2 as defined in RFC 4509 [43] and RFC 5702 [46], and

- properly handle the security concerns enumerated in RFC 6840 [49] Section 4.

The Certification Service Provider shall 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) shall 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:

<SIG:

- 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 shall use the identification methods described in the (1a) paragraph of Article 24. as follows.

]]

The Certification Service Provider shall verify the identity of the natural person applying one of the following methods:

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
   - during the personal identification the identity of the natural person shall be verified 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 [7]
     - 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) [12] 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" [67], 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

   <SIG:

   - 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 shall be validated by the Registration Authority by using an authentic public register. In case of any other natural persons the Certification Service Provider doesn't have to 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 shall verify, whether any alteration or counterfeiting happened to the presented identity cards.

<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, 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 identification data shall be checked by the Registration Authority with the help of a trusted third party or an authentic public register.*

>

<TLS:

- *The Registration Authority shall verify the authenticity of the presented cards. The Certification Service Provider shall verify that the Certificate Application was really sent by the identified Subject or Applicant through a trustable communication channel.*

>

]]

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].**

   ]]

   <SIG:

   - 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" [69] 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" [69] 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 [17], 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 can provide opportunity for new Certificate issuance based on the reconciled data of the Subject or Applicant in the case of a Certificate Application during the validity period of the service agreement. The authenticity of the Certificate Application, the accuracy of the data to be in the Certificate and the identity of the person making the application shall also be checked. The verification process shall be precisely determined in the Certification Practice Statement.

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.

The method of the verification shall be precisely defined in the Certification Practice Statement.

An Organizational Administrator can be appointed by a person eligible for representing the Organization. The designation of an Organizational Administrator is not compulsory for every Organization, if not designated, then the person eligible to represent the Organization performs the task aforementioned.

3.2.6 Criteria for Interoperation

The Certification Service Provider might collaborate with other Certification Service Providers during the provision of services, those who expressed the consent to be bound by the compliance with the requirements of this Certificate Policies.

The Certification Service Provider has to make sure, that the other Certification Service Provider it collaborates with is authorized – on the basis of law or official records – to the provision of services publicly.

The collaborating Certification Service Providers shall define the method of the collaboration in the Certification Practice Statements.

As a result of the collaboration, the Clients rights shall not be diminished in any way and the quality of service shall not decrease.

The Certification Service Provider shall disclose its entire cross-certified Certificates it sought or accepted.

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 may accept 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 shall take 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 may re-use the results and evidences collected during the original validation process.

3.3.2 Identification and Authentication for invalid Certificate

The Certification Service Provider can accept re-key requests only during the service provision time.

The identification of the Subject or Applicant shall take 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 shall take 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 shall not 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 shall take 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 shall not be renewed.

3.6 Identification and Authentication for <not TLS: Suspension and> Revocation Request

The Certification Service Provider shall receive and process 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 shall ensure that the besides the rapid processing of the <not TLS: suspension and> revocation requests, the requests only get accepted from authorized parties.

The authenticity of the submitted requests and the eligibility of the submitter shall be verified.

The identification and authentication aspects of such requests shall be recorded in the Certification Practice Statement.

<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 shall verify a telephone number, fax number, email address, or postal delivery address as a "Verified Method of Communication" with the Applicant.

<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 an authorized Contract Signer. The EV Certificate Request shall be signed by the Certificate Requester submitting the document. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver shall independently approve the EV Certificate Request. In all cases, applicable signatures shall be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Subscriber to the terms of each respective document.

]]

>

4 Certificate Life-Cycle Operational Requirements

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 shall not 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 may prepare the Subscriber's service agreement based on the information given in the Registration Application.

The Certification Service Provider shall inform 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 shall also be given to the Subject or Applicant.

The documents containing this information shall be stated in a comprehensible manner, in electronically downloadable format as well as upon request made available in printed form.

The Certificate Application 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)

>

<SIG:

- data to be indicated in the Certificate (for example name, title, name of Organization, name of organizational unit, city, country, email address)

>

<SEA:

- 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 >

  <SEA: person entitled to represent the Subject >

  <SIG: 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)

- the contact of the

  <TLS: Applicant >

  <SEA: person entitled to represent the Subject >

  <SIG: 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)

>

- the Subscriber's data (billing information)

In conjunction with the Certificate Application the Certification Service Provider shall 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 >

  <SEA: person entitled to represent the Subject >

  <SIG: 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

>

<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

<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

> >

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. > <SIG: **[[QUA: for themselves.]]** *[[ADV: for themselves or for other employees of the organization represented.]]* > <SEA: 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 >

<SIG: The Subject – in case of an Organization the Organization representative –>

<SEA: 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 >

<SIG: The Subscriber and the Subject – in case of an Organization the Organization representative –>

<SEA: 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 shall ascertain the identity of the person submitting the Certificate Application (see section 3.2.3).

<TLS:

The Certification Service Provider shall verify 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 Organization shall be identified too, and it shall be ensured, that the person appeared is entitled to represent the Organization 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.

The Certification Service Provider shall register 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 shall register 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 shall register 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 aforementioned records shall be kept 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.

<not SEA:

If the identity of the Subject or Applicant or the Subject's association to the Represented Organization can not be verified without a doubt, or any of the indicated data on the Certificate Application form is incorrect, then the Certificate Application procedure is aborted. Then the Client has the opportunity to correct incomplete or erroneous data, and hand over the missing documents.

>

<SEA:

If the identity of the person entitled to represent the Subject or the identity of the Organization can not be verified without a doubt, or any of the indicated data on the Certificate Application form is incorrect, then the Certificate Application procedure is aborted. Then the Client has the opportunity to correct incomplete or erroneous data, and hand over the missing documents.

>

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Certification Service Provider shall identify the Subject or Applicant according to Section 3.2.

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 shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.

[[QUA:

In case of EVCP Certificate:

The Certification Service Provider shall verify 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 shall 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 shall ensure 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 shall verify the authenticity of all the information provided in the Certificate Application to be indicated in the Certificate before issuing the Certificate.

After processing the Certificate Application, the Certification Service Provider accepts or rejects the Certificate Application.

<TLS:

Managing High-Risk Certificates

The Certification Service Provider shall develop processes that identify high-risk web server Certificate Applications, which shall be monitored more closely. The process of identifying suspicious applications and tighter monitoring process shall be documented in the Certification Practice Statement.

>

<not TLS:

4.2.2.1 CAA records

As part of the issuance process, the Certification Service Provider shall retrieve and process CAA records in accordance with IETF RFC 9495 [54] for each Email Address in the Email (S/MIME) Certificate to be issued.

4.2.2.2 Multi-perspective issuance corroboration

When issuing Email (S/MIME) Certificates, the Certification Service Provider shall implement Multi-perspective issuance corroboration according to CABF TLS Baseline Requirements [60] 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 shall define in the Certification Practice Statement the time limit within which it undertakes the evaluation of the Certificate Application.

4.3 Certificate Issuance

The Certification Service Provider shall only issue the Certificate after the acceptance of the Certificate Application.

<not TLS:

The issued Certificate shall only contain the data of the Subject that was indicated on the Certificate Application and that was verified by the Certification Service Provider during the evaluation process.

>

4.3.1 CA Actions During Certificate Issuance

The Certificate issuance shall be performed in an adequately secure manner.

[[QUA:

<TLS:

The Certification Service Provider shall ensure that the recording of the data included in the Certificate and the verification of the authenticity of the data cannot be performed by the same person.

>

<**not TLS:**

The Certification Service Provider shall act carefully when recording and verifying the authenticity of the data included in the Certificate.

>

]]

[[ADV:

The Certification Service Provider shall act carefully when recording and verifying the authenticity of the data included in the Certificate.

]]

4.3.2 Notification of the Subscriber about the Issuance of the Certificate

The Certification Service Provider shall inform the Subject or Applicant and the Subscriber about the issuance of the Certificate and shall enable 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 > <SIG: Subject > <SEA: 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 before 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

The Certification Service Provider shall disclose the issued Certificate after handing over the Certificate.

The condition for disclosure is the consent of the affected Subject.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

<not SEA:

<TLS: In case of an Organizational Certificate,> <SIG: 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 shall be notified on the Certificate issuance.

>

<SEA:

The person entitled to represent the Subject shall be notified 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.

>

<SIG:

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.

>

<SEA:

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 , 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,> <SIG: accepting the electronic signature or seal verified,> <SEA: 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, and to meet the requirements described in the Certification Practice Statement, 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

>
<SIG:

- Certificates for electronic signatures and the corresponding public keys shall only be used for electronic signature validation

>
<SEA:

- 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 Relying Party shall consider any restrictions indicated in the Certificate or in the regulations referenced in the Certificate

The Certification Service Provider shall make 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.

[[ADV:

The Certification Service Provider can limit the types of Certificates involved in the Certificate renewal in its Certification Practice Statement.

]]

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.

During the *Certificate renewal*, the Subject or Applicant shall be 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 shall also be provided to the Subscriber.

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 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 shall verify 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 shall inform the Subject or Applicant and the Subscriber about the Certificate issuance.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

The Certification Service Provider may transfer, make available for download the renewed Certificate without personal encounter.

4.6.6 Publication of the Renewed Certificate by the CA

The Certification Service Provider shall disclose the renewed Certificate the same method 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 shall be notified on the Certificate issuance.

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 shall be 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 shall also be given to the Subscriber.

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 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 shall verify 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 shall inform the Subject or Applicant and the Subscriber about the Certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The Certification Service Provider shall hand over the Certificate issued for the new public key after the identification of the Subject or Applicant.

4.7.6 Publication of the Re-Keyed Certificate

The Certification Service Provider shall disclose the re-keyed Certificate 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 shall be notified on the Certificate issuance.

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.

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 shall only accept a Certificate modification application within the effect of the service agreement.

During the Certificate modification, the Subject or Applicant shall be 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 shall also be given to the Subscriber.

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.

The Certification Service Provider shall initiate the Certificate modification if it becomes aware of that the Subject's data indicated in the Certificate is changed.

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 shall verify 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 shall proceed the same as the initial verification performed before a new Certificate issuance.

4.8.4 Notification of the Client about the New Certificate Issuance

The Certification Service Provider shall inform the Subject or Applicant and the Subscriber about the Certificate issuance.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The Certification Service Provider may hand over the modified Certificate without a personal meeting, it may make it downloadable.

4.8.6 Publication of the Modified Certificate by the CA

The Certification Service Provider shall disclose the modified Certificate 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 shall be notified on the Certificate issuance.

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.

>

4.9.1 Circumstances for Revocation

Reasons for Revoking a Subscriber Certificate

Certification Authority shall revoke the end-user Certificate within 24 hours and use the corresponding CRLreason if one or more of the following occurs:

- 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 should revoke the end-user Certificate within 24 hours and shall revoke 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 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)

- 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))

The Certification Practice Statement may include additional conditions on which Certification Authority revokes the Certificate.

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 Certification Practice Statement may include other conditions in which case the Certification Authority revokes the Certificate.

The Certification Practice Statement may include other conditions in which case the Certification Authority revokes the Certificate.

4.9.2 Who Can Request Revocation

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:
<SEA:

- **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 shall be able to 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 shall provide 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 on a publicly available way.

4.9.3 Procedure for Revocation Request

The Certification Service Provider shall provide the following possibilities for the submission of the revocation request:

<TLS:

- **Via the Website of the Certification Service Provider 24 Hours a Day**

  The IT system of the Certification Service Provider shall process the applications submitted via its website immediately, the site shall inform the application submitter about the results of the evaluation.

>

- **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**

  on paper signed manually at the customer service of the Certification Service Provider during office hours in person or sent by post. 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))

The Certification Service Provider shall verify the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

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 shall notify the Subject and the Subscriber about the revocation.

High-Priority Certificate Problem Report

The Certification Service Provider shall maintain a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report. If necessary, the National Media and Infocommunications Authority shall be informed about the reported problem, and/or the Certificate(s) concerned shall be revoked.

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 shall process the revocation requests within 24 hours following the arrival of the request.

<TLS:

The Certification Service Provider shall begin investigation of the Website Authentication Certificate related reported problems and shall make decision about further steps within 24 hours.

The Certification Service Provider shall provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

The Certification Service Provider shall revoke the Website Authentication Certificates within 24 hours after the conditions defined in section 4.9.1 are met.

The Certification Service Provider shall revoke 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 shall issue a new Certificate Revocation List for its end user Certificates at least once a day. The validity of these Certificate Revocation Lists shall be maximum 26 hours.

The Certification Service Provider shall continue 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 shall issue a new Certificate Revocation List at least once in 12 months, and in case of a revocation within 24 hours for its Timestamping Unit Certificates used

for Codesigning. The validity of these Certificate Revocation Lists shall be to a maximum of 12 months.

>

Intermediate certification units

The Certification Service Provider shall issue a new Certificate Revocation List at least once a year and in case of a revocation within 24 hours for its intermediate certification units. The validity of these Certificate Revocation Lists shall be to a maximum of 12 months.

4.9.8 Maximum Latency for CRLs

At most 5 minutes shall elapse between the generation and disclosure of the Certificate Revocation List (CRL).

4.9.9 Online Revocation/Status Checking Availability

The Certification Service Provider shall provide online Certificate revocation status (OCSP) service, if there is no CRL based service available.

4.9.10 Online Revocation Checking Requirements

The online Certificate status service shall comply with the requirements of Section 4.10.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements for Key Compromise

The Certification Authority shall specify in the Certification Practice Statement the requirements that must be met by key compromise reports submitted in connection with the Certificates issued by the Certification Authority.

In case of compromise of the private key of one of its certification units the Certification Service Provider shall make every reasonable effort to notify the Relying Parties about the event. The Certification Service Provider shall disclose the status change of its provider Certificates.

In case of the compromise of a private key corresponding to an end user Certificate issued by the Certification Service Provider, the Certification Service Provider shall be able to revoke the end user Certificate in question. The revocation reason information (reasonCode) shall be set to the value "keyCompromise (1)".

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 shall provide a possibility for a temporary cessation of the Certificate's validity to reduce the risk in cases it can be assumed that one of the reasons establishing the revocation of the Certificate persists.
[[QUA:
<SIG: The Email (S/MIME) Certificates shall not be suspended.>
<SEA: The Email (S/MIME) Certificates shall not be suspended.>
]]
<UNI:
The Code Signing Certificates and Email (S/MIME) Certificates shall not be suspended.
>
>

4.9.14 Who Can Request Suspension

<TLS: Not applicable. >
<not TLS:
The same requirements apply to the Certificate suspension as to the certificate revocation – see Section 4.9.2.
>

4.9.15 Procedure for Suspension Request

<TLS: Not applicable. >
<not TLS:
The Certification Service Provider shall enable the initiation of the suspension in each day of the year around the clock.
The Certification Service Provider shall enable the submission of the suspension requests the same way as the submission of the revocation requests according to the requirements of the Section 4.9.3, except that in this case the the suspension password is used for the validation of the suspension request.
In case of the acceptance of the suspension request, the status change shall be recorded in the Certificate status records of the Certification Service Provider without delay.
The requirements of Sections 4.9.3 and 4.9.5 regarding Certificate revocation apply to the evaluation of the suspension requests received through other communication channels.
>

4.9.16 Limits on Suspension Period

<TLS: Not applicable. >
<not TLS:

The Certification Service Provider may limit the duration of the suspended state; this shall be clearly stated in the Certification Practice Statement. After the time period has elapsed, the Certification Service Provider is entitled to the revocation of the suspended certificate without any extra notification.

>

4.10 Certificate Status Services

The Certification Service Provider shall provide the following possibilities for the Certificate revocation status query:

- OCSP – online Certificate revocation status query service
- CRL – Certificate Revocation Lists.

The revoked <not TLS: and suspended> Certificates shall be listed in the Certificate Revocation Lists.

<not TLS:

The suspended Certificates shall be taken out of the Certificate Revocation List in case of a reinstatement (withdraw of the suspension).

>

The revocation <not TLS: and suspension> information shall not be removed from the Certificate Revocation List until after the expiry date of the revoked <not TLS: or suspended> Certificate.

<not UNI:

The revoked Certificates shall not be deleted from the Certificate Revocation List even after their expiry.

>

In case of <TLS: revocation> <not TLS: suspension, reinstatement and revocation> the new status of the Certificate shall appear immediately in the revocation records of Certification Service Provider after the successful completion of the process.

From that moment, the OCSP responses provided by the Certification Service Provider shall contain the new revocation status of the certificate.

In case of the usage of the Certificate Revocation List, the status change shall be disclosed in the next Certificate Revocation List.

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

No stipulation.

4.10.2 Service Availability

The Certification Service Provider shall ensure 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% annually, and the length of downtime shall not exceed 3 hours.

The Certification Service Provider shall ensure that the availability of the revocation status information and the revocation management service is at least 99.9% annually, and the length of downtimes shall not exceed 3 hours on any occasion.

The response time of the revocation status service in case of normal operation shall be less than 10 seconds.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The Certification Service Provider shall revoke 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 shall not provide key escrow service for a private key belonging to a Website Authentication Certificate.

>

<SIG:

The Certification Service Provider shall not provide key escrow service for a private key belonging to a signatory Certificate.

>

<SEA:

The Certification Service Provider shall not provide key escrow service for a private key belonging to a seal Certificate.

>

<UNI:

The Certification Service Provider may provide key escrow service only for the private key belonging to the encryption Certificates.

>

4.12.1 Key Escrow and Recovery Policy and Practices

<TLS: The private key belonging to the Website Authentication Certificate shall not be escrowed.>

<SIG: The private key belonging to the signing Certificate shall not be escrowed. >

<SEA: The private key belonging to the seal Certificate shall not be escrowed.>
<UNI: No stipulation. >

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.
>
<SIG:
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.
>
<SEA:
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:
No stipulation.
>

5 Facility, Management, and Operational Controls

The Certification Service Provider shall apply 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 shall keep a record of the system units and resources related to the service provision and conduct a risk assessment on these. It shall use protective measures proportional to the risks related to the individual elements.

The Certification Service Provider shall monitor the capacity demands, and shall ensure that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The Certification Service Provider shall take care that physical access to critical services is controlled and shall keep 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 shall be implemented at secure locations.

The provided protection shall be proportional to the identified threats of the risk analysis that the Certification Service Provider performed.

5.1.1 Site Location and Construction

The IT system of the Certification Service Provider shall be 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 – shall be 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 that take part in service provision, and for the preservation of the confidential data stored by the provider.

5.1.2 Physical Access

The Certification Service Provider shall protect 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 shall ensure 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 should be physically out of reach
- the logged-in terminals shall not be left without supervision
- no work process should be 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 should be appointed responsible people to carry out regular physical security assessments. The results of the examinations shall be recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The Certification Service Provider shall apply 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 shall be 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 should provide the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity should be reduced to the level required by the IT systems.

Cooling systems with proper performance should be used 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 shall be adequately protected from water intrusion and flooding.

5.1.5 Fire Prevention and Protection

[[QUA:

Smoke and fire detectors shall be installed in the Data Centre of the Certification Service Provider that automatically alert the fire brigade.

]]

[[ADV:

Smoke and fire detectors shall be installed in the Data Centre of the Certification Service Provider.
]]
Manual fire extinguishers of the appropriate type and amount compliant with the relevant regulations should be placed in a visible place in each room.

[[QUA:
Automatic fire extinguishers shall be applied in the Data Centre.
]]

5.1.6 Media Storage

The Certification Service Provider shall protect its media storages from unauthorized access and accidental damage. All audit and archive data shall be created in duplicate. The two copies should be stored separately from each other physically, at locations in a safe distance from each other. The stored media storages shall be 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 shall take care of the destruction of its devices, media storages becoming superfluous in compliance with environmental regulations.

Such devices and media storages shall be permanently deleted or made unusable in accordance with the widely accepted methods under the personal supervision of employees of the Certification Service Provider.

5.1.8 Off-Site Backup

The Certification Service Provider shall create 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 – shall be 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 shall be resolved.

Based on the randomly selected backup data a restoration test shall be made at least yearly. The main circumstances and results of the restoration test shall be recorded in an audit report.

5.2 Procedural Controls

The Certification Service Provider shall take 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 shall be 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 shall create trusted roles <not UNI: (in the wording of the regulation, scope of activities) > <not UNI: according to the requirements of decree 24/2016. [13] > for the performance of its tasks. The rights and functions shall 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.

Trusted roles to be implemented:

- manager with overall responsibility for the provider's IT system
- security officer: individual with overall responsibility for the security of the service
- system administrator: individual performing the IT system installation, configuration and maintenance
- 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 provider, responsible for verifying the enforcement of control measures the provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures
- registration officer: responsible for the approval of <TLS: production, issuance and revocation> <not TLS: production, issuance, revocation and suspension> of end-user certificates

For the provision of trusted roles, the manager responsible for the security of the Certification Service Provider shall formally appoint 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 shall be kept of the trusted roles.

>

<not UNI:

Up to date records shall be kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority shall be notified without delay.

>

5.2.2 Number of Persons Required per Task

It shall be defined in the Certification Service Provider's security and operational regulations 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 shall 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 shall be revoked without delay in case of the cessation of user rights.

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 is bound to ensure 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.

5.3 Personnel Controls

The Certification Service Provider shall take 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 shall address 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 shall 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 shall ensure 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

Each employee of the Certification Service Provider shall have the necessary education, practice and professional experience for the provision of his scope of activities. Even during recruitment, particular emphasis shall be given to the personality traits when selecting potential employees and only reliable persons can be hired for trusted roles.

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 shall only hire 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 shall verify 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 shall train 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 shall train 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 shall take and pass an exam on the knowledge of the related requirements and procedures for data verification before their appointment, and this fact shall be documented.

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 shall ensure that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training shall be held.

Further training shall be held if there's a change within the processes or the IT system of the Certification Service Provider.

The training material shall be updated at least in every 12 months and shall contain the new threats and actual security practices.

The training shall be 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

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The Certification Service Provider shall regulate 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.

5.3.7 Independent Contractor Requirements

The same rules shall be applied to workers employed with a contractual relationship as to employees.

The trusted role holder person shall be in an employment relationship with the Certification Service Provider.

5.3.8 Documentation Supplied to Personnel

The Certification Service Provider shall continuously provide for the employees the availability of the current documentation and regulations necessary to perform their roles.

5.4 Audit Logging Procedures

In order to maintain a secure IT environment, the Certification Service Provider shall implement and operate an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

The Certification Service Provider shall log 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, the following data shall be stored:

- 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.

The audit records shall not be modified or deleted.

All of the essential event logs shall be available to the independent system auditors, who examine the compliance of the Certification Service Provider's operation.

The following events shall be logged 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.)

<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.

>

<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 Certification Service Provider shall ensure the regular evaluation of the created logs.

The created daily log files shall be evaluated in the next working day if possible, but not later than 1 week.

The evaluation of the log files shall be performed by an independent system auditor with the right expertise, system privileges and appointment.

The Certification Service Provider can use automatized tools to assist the evaluation of the electronic logs.

The notifications received from the automatized monitoring tools shall be processed and evaluated within 24 hours.

During the evaluation, the authenticity and integrity of the examined logs shall be ensured. During the evaluation, the system generated error messages shall be analysed.

The significant changes in the traffic should be analysed with statistical methods.

The fact of the audit, the audit results and the measures taken in order to remove any deficiencies found shall be properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the online system, the logs shall be archived and their secure preservation shall be ensured for the amount of time defined in Section 5.5.2.

5.4.4 Protection of Audit Log

The Certification Service Provider shall protect the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data shall be ensured:

- protection against unauthorized disclosure: only authorized persons – primarily the independent system auditors – shall access the logs
- availability: authorized persons shall be granted access to the logs
- integrity: any data alteration, deletion in the log files and change in the order of the entries, etc. shall be prevented.

5.4.5 Audit Log Backup Procedures

Daily log files shall be created from the continuously generated log entries during the operation in each system.

The daily log files shall be 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 Certification Practice Statement.

5.4.6 Audit Collection System (Internal vs External)

The Certification Service Provider specifies the operation of its logging processes in its Certification Practice Statement.

The Certification Service Provider can use automatic audit and logging systems if it can ensure that they are active at the time of the system launch and they operate continuously until the system's shutdown.

If there's any anomaly in the automatic audit and logging systems, the operation of the Certification Service Provider shall be suspended until the incident is resolved.

5.4.7 Notification to Event-causing Subject

In case of the detected errors, the Certification Service Provider at its discretion can decide whether it notifies the person, role, device or application of the error that caused it.

5.4.8 Vulnerability Assessments

Vulnerability assessment shall be carried out each year by the Certification Service Provider to help discover potential internal and external threats, which may lead to unauthorized access, may affect the Certificate issuing process, or allow modification of the data stored in the Certificate.

The occurrence probability of the event and the expected damage shall be mapped too.

It shall regularly assess the implemented processes, security measures, information systems, so that they are able to correctly withstand the threats detected.

After evaluation of the detected errors, if necessary the defence systems shall be amended to prevent similar mistakes in the future.

5.5 Records Archival

5.5.1 Types of Records Archived

The Certification Service Provider shall be prepared to the proper secure long-term archiving of electronic and paper documents.

The Certification Service Provider shall archive 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

<SIG:

- information related to the impersonation of the Electronic Signature or Seal Creation Device

>
<SEA:

- 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 is bound to preserve 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

  <SIG:
  - until the completion of the dispute concerning the electronic signature generated with the certificate

  >
  <SEA:
  - 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 is bound to store every archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy can be made in accordance with the applicable law from the only authentic paper based copy of the document available.

Each of the two locations shall fulfil the requirements for archiving security and other requirements.

During the preservation of the archived data, it shall be ensured that:

- their integrity is preserved
- they are protected against unauthorized access
- they are available
- they preserve authenticity.

The archived electronic data shall be provided with at least an advanced electronic signature or seal and a qualified Time Stamp.

5.5.4 Archive Backup Procedures

The duplicate of the archived data shall be stored at a physically separate location from the Certification Service Provider's site according to the requirements of Section 5.1.8.

5.5.5 Requirements for Time Stamping of Records

Every electronic log entry shall be provided with a time sign, on which the system provided time is indicated at least to one second precision.

The Certification Service Provider shall ensure that in its service provider systems, the system clock is at maximum different from the reference time with 1 second. The system time used for generating the time signal shall be synchronized to the UTC time at least once a day.

The daily log files shall be provided with a 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 shall be ensured.

5.5.6 Archive Collection System (Internal or External)

The log entries shall be 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.

5.5.7 Procedures to Obtain and Verify Archive Information

The Certification Service Provider can create the log files manually or automatically. In case of automatic logging system, the certified log files shall be generated daily.

The archived files shall be protected from unauthorized access.

Controlled access to the archived data shall be 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 shall ensure that the used Certification Units are continuously having the 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 shall generate a new key pair for the Certification Units, and inform its Clients in time. The new provider key shall be generated and managed according to this regulation.

If the Certification Service Provider changes any of its end-user Certificates issuer provider Certificate keys, it shall comply with the following requirements:

- it shall disclose 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 can only be signed with the new provider keys
- it shall preserve its old Certificates and public keys.

5.7 Compromise and Disaster Recovery

In case of a disaster, the Certification Service Provider is obliged to take 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 shall take the necessary amendments, corrective measures to prevent future occurrence of the incident.

<not UNI:

Once the problem resolved, the event shall be reported to the National Media and Infocommunications Authority, as the supervisory authority.

>

<UNI:

Once the problem resolved, the event shall be 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 shall have a business continuity plan.

The Certification Service Provider shall establish and maintain 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 shall continually test the operation of the backup system and shall review its business continuity plans annually.

In case of a disaster, the availability of the services shall be restored as quickly as possible.

The Certification Service Provider shall manage and classify the incidents according to Commission Implementing Regulation 2024/2690 [5].

The Certification Service Provider shall review the security incidents of the past period at least once a year and shall examine whether the measures taken are adequate to prevent the recurrence of the error.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The IT systems of the Certification Service Provider shall be built from reliable hardware and software components. The critical functions shall be implemented using redundant system elements so that in the event of an item failure they shall be able to operate further.

The Certification Service Provider shall make a full daily backup of its databases and the generated log events.

The Certification Service Provider shall make full 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 shall include 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 shall restart its services as soon as possible.

During the restoration of services, the certificate status information service systems shall have top priority.

5.7.3 Entity Private Key Compromise Procedures

In case of the Certification Service Provider's private key compromise or suspected compromise the following steps should be taken without delay:

- all of the affected Certificates of the Certification Service Provider shall be revoked
- new provider private key shall be generated for the restoration of the services
- the revoked provider Certificate's data shall be disclosed according to the regulated method in Section 2.2

<TLS:

- every Website Authentication Certificate shall be revoked that were signed by the affected private keys
- new Website Authentication Certificates shall be issued instead of the revoked Certificates by using the new provider keys

>

- the information related to the compromise shall be disclosed for every Subscriber and Relying Party

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 shall be defined in the Certification Service Provider's business continuity plan.

In the event of disaster, the regulations shall come into force, the damage control and the restoration of the services shall begin.

The secondary services site shall be 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 shall restore 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

The Certification Service Provider shall comply with the requirements laid down in in the legislation in case of service termination.

During the termination the priority tasks are:

- <not UNI: the National Media and Infocommunications Authority, > the Relying parties and the Subscribers shall be notified about the planned termination in time
- the Certification Service Provider shall make every effort to ensure that at the latest by the service termination another provider takes over the records and service obligations
- new Certificate issuance shall be terminated
- provider Certificates shall be revoked, and provider private keys shall be destroyed
- after the termination of the service, a full system backup and archiving shall be carried out

<not UNI:

- the archived data shall be handed over to the provider that takes over the services, or to the National Media and Infocommunications Authority.

>

6 Technical Security Controls

The Certification Service Provider shall use reliable systems and equipment protected against modification for the management of the cryptographic keys and activation data for the whole life-cycle.
The capacity demands shall be continuously monitored and the future capacity demands shall be estimated, so that the necessary availability of processing and storage needs are ensured.

6.1 Key Pair Generation and Installation

The Certification Service Provider shall ensure the secure production and management of its generated private keys corresponding to the industry standards and regulatory requirements in force corresponding production and management.

6.1.1 Key Pair Generation

The Certification Service Provider may only use key generation algorithms for the key pair generation, which comply with the requirements set out in the following normative:

- ETSI TS 119 312 [28]

<TLS:

- CABF Baseline Requirements recommendation [60]

>

- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2023. Act CIII [12] 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 shall 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 [36], or
  - meets the requirements of FIPS 140-2 [63] level 3 or higher, or
  - meets the requirements of FIPS 140-3 [64] level 3 or higher, or
  - meets the requirements of CEN 419 221-5 [33], or
  - is a reliable system that is evaluated in accordance with ISO/IEC 15408 [35] 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 shall ensure 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

In case of generating the key pair for the Subjects, the Certification Service Provider shall ensure that:

- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.

<not TLS:

- In case of Certificate Policies requiring the use of a **[[QUA: 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 **[[QUA: Qualified Electronic Signature or Seal Creation Device or on its]]** Cryptographic Hardware Device which makes the disclosure of the private key impossible.

>

- <SIG:

  [[QUA: If the private key is handed over to the Subject, the private keys generated outside a Qualified Electronic Signature or Seal Creation Device or a Cryptographic Hardware Device are stored in an adequately secure environment by the Certification Service Provider to prevent the disclosure.]]

  [[ADV: The generated private keys are stored by the Certification Service Provider until the key handover in an adequately secure environment to prevent disclosure.]]

  >

  <SEA:

  [[QUA: If the private key is handed over to the Subject, the private keys generated outside a Qualified Electronic Signature or Seal Creation Device or a Cryptographic Hardware Device are stored in an adequately secure environment by the Certification Service Provider to prevent the disclosure.]]

  [[ADV: The generated private keys are stored by the Certification Service Provider until the key handover in an adequately secure environment to prevent disclosure.]]

  >

After the documented handover of private key to the Subject or Applicant the Certification Service Provider destroys every copy of the handed over private key stored by it, in such a way that its restoration and usage becomes 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.

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 shall not generate key-pairs for the end-user Certificates.

>

<not TLS:

If the Certification Service Provider generated the Subject's private key, then the following requirements shall be met:

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.

>

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.

6.1.4 CA Public Key Delivery to Relying Parties

The Certification Service Provider shall make available its top-level provider Certificate public keys to the Relying Parties in such a way, that makes attacks targeting key modification impossible. Particularly, the Certification Service Provider at least shall disclose its provider Certificates via its website.

The Certification Service Provider shall disclose 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 name of the root certification units and the hash of its root certificates figure in the Certification Practice Statement. Their status change information shall be available via the website of the Certification Service Provider.
- The status change information of the intermediate (not root) certification units' certificates shall be 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 only discloses that Certificate's revocation status in a way that in case of key compromise or other problem new Certificate won't be issued for the old

private key signing the OCSP responses. The Certification Service Provider shall issue 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 shall only use cryptographic algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [28]

<TLS:

- CABF Baseline Requirements recommendation [60]

>

- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2023. Act CIII [12] 96. § (1) b)

6.1.6 Public Key Parameters Generation and Quality Checking

The requirements for the key parameter generation are in Section 6.1.1.

Devices with appropriate device certificates used in the creation of keys shall be operated with strict compliance with the requirements set out in the certification to ensure the quality of the generated key parameters.

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 shall include the "Key Usage" extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [57] 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.

>

<SIG:

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.

>

<SEA:

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 shall ensure the secure management of the private keys held by it and shall prevent 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.

During the management of the Hardware Security Modules the signing private keys stored on the decommissioned Hardware Security Modules shall be deleted so that it is practically impossible to restore the keys.

6.2.1 Cryptographic Module Standards and Controls

The systems of the Certification Service Provider issuing Certificate, signing OCSP responses and CRL lists shall store the private keys in such secure hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [36], or
- the requirements of FIPS 140-2 [63] level 3 or higher, or
- the requirements of FIPS 140-3 [64] level 3 or higher, or
- the requirements of CEN 419 221-5 [33], or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to ISO/IEC 15408 [35] 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 provider keys may only be stored in encrypted forms outside of the Hardware Security Module. For coding only those algorithms and key parameters shall be used by the current order of the National Media and Infocommunications Authority that was issued according to the year 2023. Act CIII [12] 96. § (1) b)

that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The provider private keys shall be stored in a physically secure site even in an encrypted form, where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the coded keys shall be destroyed or they shall be recoded using algorithm and key parameters that ensure greater protection.

6.2.2 Private Key (N out of M) Multi-Person Control

The Certification Service Provider shall to ensure 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 may escrow its own provider private keys only in encrypted form.

6.2.4 Private Key Backup

The Certification Service Provider shall make security copies of its provider private keys, and at least one copy of those shall be stored at a different place from the service provider location.

Making backups may only be done in protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people.

At least the same strict security standards shall be applied to the management and preservation of backups as for the operation of the production system.

The Certification Service Provider shall not make any copy of the end-user private keys.

6.2.5 Private Key Archival

The Certification Service Provider shall 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 shall be created in a cryptographic module that meets the requirements.

The private keys shall not exist in an open form outside of the Hardware Security Module.

The Certification Service Provider may only export the private key from the Hardware Security Module for the purpose of making a secure copy.

The private key transport between the Hardware Security Modules is only permitted in the form of a secure copy.

6.2.7 Private Key Storage on Cryptographic Module

The Certification Service Provider shall store the private keys used for the provision of the service according to the present Certificate Policies in a Hardware Security Module.

There is no restrictive term applied for the storage form in the Hardware Security Module.

6.2.8 Method of Activating Private Key

The Certification Service Provider's private keys shall be activated in accordance with the procedures and requirements defined in the used cryptographic module user guide and the certification documents.

The Certification Service Provider shall ensure 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 shall ensure 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 shall be configured and handled over to the Subject or Applicant so that:

- **it can be clearly established that the device has not been used <SIG: 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): shall be configured and handled over 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 Certification Service Provider's private keys shall be deactivated in accordance with the procedures, requirements defined in the used Hardware Security Module's user guide and the certification documents.

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 shall ensure 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 <SIG: for electronic signature creation > <SEA: 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 software 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 shall ensure 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 shall be destroyed in a way that makes further use of the private keys impossible.

The provider private keys shall be destroyed 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.

Each backup copy of the private key shall be destroyed 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 is bound to destroy 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.

]]

>

<SIG:

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.

>

<SEA:

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 shall be stored in a cryptographic module that

- has a certificate according to ISO/IEC 19790 [36], or
- has a certificate according to FIPS 140-2 Level 3 [63], or
- has a certificate according to FIPS 140-3 Level 3 [64], or
- has an at least EAL-4 level Common Criteria [65] based certificate attesting compliance with the requirements of the CEN 419 221-5 [33], 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 shall archive every issued Certificate.

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 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.

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.

During the Certificate renewal and Certificate modification the Certification Service Provider may issue the new Certificate for the same end-user private key.

<SEA:

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.

Life-Cycle of the Time Stamping Keys

The following requirements shall be met for the private keys used for Time Stamp certification:

- The Time Stamping Service Provider shall specify the end of the validity period of the signing keys used in the Time Stamping Units
- the end of the key validity period shall not be a later time than the end of the Certificate validity period
- the end of the validity period shall not be a later date than the end of the implemented cryptographic algorithms and key parameters' validity period

>

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.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Certification Service Provider's private keys shall be 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 need to be 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 shall provide for:

- **the activation data to be 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 shall provide for:

- the activation data to be 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.

>

In case of private keys created for and handed over to the Subject or Applicant via software by the Certification Service Provider the Certification Service Provider shall create the activation data and shall assign them to the private key in a physically secure environment, with an adequate quality random number generator.

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 devices, activation data necessary for the private key activation shall be stored securely by the employees of the Certification Service Provider, the passwords may only be stored encoded.

<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 may only record the activation data for the purpose of delivering them to the Subject or Applicant**
- **the Certification Service Provider shall distribute the activation data to the Subject 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 may only record the activation data for the purpose of delivering them to the Subject or Applicant
- the Certification Service Provider shall distribute the activation data to the Subject 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 the IT system of the Certification Service Provider the compliance with the following requirements shall be ensured:

- the user identity is verified before granting access to the system or the application
- roles are assigned to users and it shall be ensured that all users only have permissions appropriate for its roles
- a log entry is created for every transaction, and the log entries shall be 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

In order to provide IT security and service quality the Certification Service Provider shall implement a control system by internationally accepted methodologies, and the adequacy of those shall be certified by a certificate issued by an independent certification body.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Certification Service Provider shall only use applications and devices in its production IT system that:

- 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.

The procurement shall be conducted in a way that excludes the modification of the hardware and software components.

The hardware and software components applied for the provision of services may not be used for other purposes.

The Certification Service Provider with proper protection measures shall prevent malicious software to enter the devices used in the certification service.

Prior to the first use and later on the hardware and software components shall be regularly checked searching for malicious codes.

The Certification Service Provider shall act with the same carefulness in case of program update purchases as at the acquisition of the first version.

Reliable, adequately trained staff shall be employed over the course of installing software and hardware.

The Certification Service Provider may only install software to its service provider IT equipment necessary for the purpose of service provision.

The Certification Service Provider shall have a version control system where every change shall be documented.

The Certification Service Provider shall implement procedures for unauthorized change detection.

6.6.2 Security Management Controls

The Certification Service Provider shall implement processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system shall detect 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 shall ensure that the program to be installed is the proper version and that it is free from any unauthorized modification. The Certification Service Provider shall regularly check the integrity of the software in its system used in the service.

6.6.3 Life Cycle Security Controls

The Certification Service Provider shall ensure the protection of the used Hardware Security Modules during their whole life cycle.

- the Hardware Security Modules used shall have the right certification
- upon receipt of the Hardware Security Modules, it shall be verified that the protection of the Hardware Security Modules against tampering was ensured during transportation
- the protection of the Hardware Security Modules against tampering shall be ensured during storage
- during operation, the requirements of the Hardware Security Modules security target, user guide and the certification report shall be observed at all times
- private keys stored on decommissioned Hardware Security Modules shall be deleted in such a way that it is impossible to recover the keys
- decommissioned Hardware Security Modules shall be handled and disposed of in accordance with the requirements of their security target, instructions for use and certification report.

6.7 Network Security Controls

The Certification Service Provider shall keep its IT system configuration under strict control, and it shall document every change including the smallest modification, development, software update too.

The Certification Service Provider shall implement proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system.

The Certification Service Provider shall check the authenticity and integrity of every software component at their first loading.

The Certification Service Provider shall apply proper network security measures for example:

- shall divide its IT system into well separated security zones
- shall separate dedicated network for administration of IT systems and the live operational network
- shall separate the production systems for the TSP services from systems used in development and testing
- shall establish 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
- shall operate the IT systems used for the live operational network in secure network zones
- shall restrict access and communications between zones to those necessary for the operation of the service
- shall disable the not used protocols and accounts
- shall disable unused network ports and services
- shall only run network applications unconditionally necessary for the proper operation of the IT system
- shall review the established rule set on a regular basis.

The Certification Service Provider shall undergo or perform 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.

6.8 Time stamping

The Certification Service Provider shall use Time Stamps provided by a qualified time stamp provider listed on the trusted list of one of the European Union member states for the protection of the integrity of the log files and other electronic files to be archived.

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 shall comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [57]

[[QUA:

- **IETF RFC 3739 [39]**

]]

- IETF RFC 5280 [45]
- IETF RFC 6818 [48]

<TLS:

- IETF RFC 6962 [51]

>

- ETSI EN 319 412-1 [23]

<SIG:

- ETSI EN 319 412-2 [24]

>
<UNI:

- ETSI EN 319 412-2 [24] in case of Certificates issued to natural persons

>
<SEA:

- ETSI EN 319 412-3 [25]

>
<UNI:

- ETSI EN 319 412-3 [25] in case of Certificates issued to legal persons

>
<TLS:

- ETSI EN 319 412-4 [26]

>
[[QUA:

- **ETSI EN 319 412-5 [27]**

]]
<TLS:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [60]

[[QUA:

- **Guidelines for the Issuance and Management of Extended Validation Certificates [62]**

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

- **CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [59] in case of Email (S/MIME) Certificate**

>>
]]
<UNI:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates [61] in case of Code Signing Certificate
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [59] 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 shall be "v3" Certificates according to the X.509 specification [57].

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. [45]
- Serial Number
  The unique identifier generated by the Certificate issuer certification unit.

  In case of the end-user Certificates the "Serial Number" field shall contain a random number with at least 8 bytes (64 bits) entropy.
- Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for digitally signing the Certificate.
- Signature
  Electronic signature or 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 [56] 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 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 [56] name format (see in section 3.1).

  Always filled out.

- Subject Public Key Algorithm Identifier

  The Identifier of the Subject Public Key Algorithm.

- 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 may only use certificate extensions according to the X.509 specification [57] , the usage of self-defined critical extensions is not allowed.

Specific requirements concerning certificates extension:

Certificate of the Root Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field shall not be 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 signature or seal certifying the Certificate.

  Filling in is mandatory.

  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.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  Filling in is optional.

- 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 can be present in the Certificate.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The field is mandatory and the values shall be:

  - "keyCertSign",
  - "cRLSign".

- Extended Key Usage – not critical
  OID: 2.5.29.37
  The further scope definition of the approved key usage.

  Shall not be present.

There shall not be any 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.

  Filling in is mandatory for this field, and it shall not be critical.

  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 signature or seal certifying the Certificate.

  Filling in is mandatory.

  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.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  Filling in is optional.

- 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 may be present in the Certificate.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The field is mandatory and the value shall be:

  – "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

  – shall contain 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)

  >

  <SIG:

  [[QUA:

  The Intermediate Certification Unit Certificates issued after 2019-01-01 shall contain 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 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)

]]

>

<SEA:

[[QUA:

The Intermediate Certification Unit Certificates issued after 2019-01-01 shall contain 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 shall contain 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 shall contain 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 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 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 shall provide online certificate status service. The availability of this service shall be indicated here.
  – To the facilitation of the certificate chain building the Certification Service Provider shall give the access path through http protocol of the Certificate of the Certificate issuer certification unit.

There may not be any 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 shall fill 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 [22]

  <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.

>

<SIG:

* **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.

>

<SEA:

* **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 [21] 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 [21] 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)*

]]

>

In all cases of end-user certificates at least one Certificate Policy shall be indicated according to what the Certification Service Provider issued the Certificate and according to what it later acts on. At least one such Certificate Policy identifier (OID) and the related Certification Practice Statement availability (URL) shall be indicated on the Certificates issued by the Certification Service Provider.

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 signature or seal certifying the Certificate.

  Filling in is mandatory.

  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.

Filling in is mandatory.

- 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 shall not be present in the end-user Certificates.

  The "pathLenConstraint" field shall not be 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 field is mandatory and the value shall be exclusively set to:

  [[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 shall be set (other value shall not be 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 mandatory value is:

  - "serverAuth (1.3.6.1.5.5.7.3.1)"

In the Website Authentication Certificates, in case of the request of the Clientand in case of Website Authentication Certificate issued under a multipurpose Root Certificate, the following further value may be set:

- "clientAuth (1.3.6.1.5.5.7.3.2)"

>

<not TLS: <not UNI:

[[QUA:

<SIG: 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)**

>

<SEA: 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:

Mandatory to set, and the values in the non-qualified signing and seal end user Certificates 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 shall be set (other value is not allowed).

>

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL availability relevant to the Certificate through http protocol.

  <TLS: Optional to fill. >

  <not TLS: Mandatory in case of end-user Certificates.>

- 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 in case of end-user certificates and the field shall contain the following data:

  – For the purpose of the fast and reliable verification of the current Certificate revocation status, the Certification Service Provider shall provide online certificate status service. The availability of this service shall be indicated here.
  – To faciliate the certificate chain building the Certification Service Provider shall give 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 shall be 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)**

>

<SIG:

– **that indication that the Certificate was issued for signing purposes – 'id-etsi-qct-esign' (0.4.0.1862.1.6.1)**

>

<SEA:

– **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. >

<SEA:

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:

Only the use of the QCType field is allowed.

]]

>

<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 shall not be 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.

  It shall not be included in a live Website Authentication Certificate.

- 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.

>

Other Certificate extension shall not be used.

<SEA:

[[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 signature or seal certifying the Certificate.

  Filling in is mandatory.

  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.

  Filling in is mandatory.

- **Subject Alternative Names – not critical**
  OID: 2.5.29.17

  Filling in is optional.

- **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 shall not be present in the Certificate issued for the Time Stamping Unit.

  The "pathLenConstraint" field shall not be 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 this field shall be mandatory and exclusively set to:

  - **nonRepudiation**
  - **digitalSignature**

- **Private Key Usage Period – not critical**
  OID: 2.5.29.16
  Determination of the permitted private key usage period.

  Usage is optional. If it is implemented, than both "notBefore" and "notAfter" values shall be set.

- **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 this field shall be mandatory and exclusively set to:

  - **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 shall provide online certificate status service. The availability of this service shall be indicated here.**
  - **To the facilitation of the certificate chain building the Certification Authority shall give 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 shall be 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))**

]]
There shall not be any more Certificate extension.
]]
[[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 signature or seal certifying the Certificate.

  Filling in is mandatory.

  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.

  Filling in is mandatory.

- *Subject Alternative Names – not critical*
  OID: 2.5.29.17

  Filling in is optional.

- *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 shall not be present in the Certificate issued for the Time Stamping Unit.

  The "pathLenConstraint" field shall not be 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 this field shall be mandatory and exclusively set to:

  - *nonRepudiation*
  - *digitalSignature*

- *Private Key Usage Period – not critical*
  OID: 2.5.29.16
  Determination of the permitted private key usage period.

Usage is optional. If it is implemented, than both "notBefore" and "notAfter" values shall be set.

- *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 this field shall be mandatory and exclusively set to:

  - *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 shall provide online certificate status service. The availability of this service shall be indicated here.*
  - *To the facilitation of the certificate chain building the Certification Authority shall give 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 shall be 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))***

]]

There shall not be any more Certificate extension.

]]

>

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 signature or seal certifying the Certificate.
  The field value: the SHA-1 hash of the provider public key.

  Filling in is mandatory.

- 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.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  Filling in is optional.

- 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 shall not be present in the Certificate issued for the OCSP Responder.

The "pathLenConstraint" field shall not be 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 this field shall be mandatory and exclusively set to:

  – digitalSignature

- Private Key Usage Period – not critical
  OID: 2.5.29.16
  Determination of the permitted private key usage period.
  Usage is optional. If it is implemented, than both "notBefore" and "notAfter" values shall be set.

- 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 this field shall be mandatory and exclusively set to:

  – 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. Shall always be filled.

- 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.

There shall not be any more Certificate extension.

7.1.3 Algorithm Object Identifiers

The denomination of the cryptographic algorithm that has been used to certify the Certificate. Only such signer algorithm shall be used, which is compliant with the requirements defined in section 6.1.5.

The cryptographic algorithms that can be used by the Certification Authority shall be listed in the Certification Practice Statement.

7.1.4 Name Forms

The Certification Service Provider shall use a distinguished name – composed of attributes defined in the standards IETF RFC 5280 [45], ETSI EN 319 412-2 [24], ETSI EN 319 412-3 [25] and ETSI EN 319 412-4 [26] – for the Subject identification in the Certificates issued based on this Certificate Policy.

The Certificate shall contain 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 shall be identical to the value in the "Subject DN" field of the issuer Certificate.

7.1.5 Name Constraints

The Certification Service Provider can use name constraints if needed with the use of the "name-Constraints" field. In this case this field shall be marked as critical.

7.1.6 Certificate Policy Object Identifier

The Certification Service Provider shall include the not critical (Certificate Policy) extension in the Certificates issued based on these Certificate Policies 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 shall contain 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 shall issue version "v2" Certificate Revocation Lists according to the IETF RFC 5280 [45] 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 [45] 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 [45].

   (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 [45].

   (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 [45].

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 can be 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.
- Guide to Suspended Certificates (holdInstruction) – not critical
  OID: 2.5.29.23
  This field may contain the guide for managing the suspended Certificate.

(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 shall contain the monotonically increasing serial numbers of the Certificate Revocation Lists.

Certificate Revocation List Extension can be used by the Certification Authority:

- Expired Certificates on the CRL (expiredCertsOnCRL) – not critical
  OID: 2.5.29.60
  The Certification Authority may indicate 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.

   Name and OID of the cryptographic algorithm sets to be supported:

   - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
   - "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
   - "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
   - "ecdsaWithSHA256" (1.2.840.10045.4.3.2)
   - "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
   - "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

3. Signature (signatureValue)
   The electronic signature or electronic seal of the Certification Authority certifying the Certificate Revocation List.

   The Certificate Revocation List shall be authenticated by the Certification Authority using the same key as used to sign or seal the issued Certificate.

The Certification Authority is not obliged to fill out the extensions.

7.3 OCSP Profile

The Certification Service Provider shall operate an online certificate status service according to the IETF RFC 6960 [50] and IETF RFC 9654 [55] 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 Service Provider shall support at least the following cryptographic algorithms:

  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
  - "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
  - "ecdsaWithSHA256" (1.2.840.10045.4.3.2)
  - "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
  - "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

- (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 [45].

- 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 [45].

- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response.
  Value according to UTC with encoding according to IETF RFC 5280 [45].

  <TLS: Mandatory. >

  <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 shall support the "v1" version according to the standard IETF RFC 6960 [50] of the online certificate status requests and responses.

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 [50] 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 may be 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 shall have a screening of its operations by an external auditor and shall send 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 shall comply 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 [20]**
- **ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [19]**
- **ETSI EN 301 549 Harmonised European Standard; Accessibility requirements for ICT products and services [18]**
- **ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [21]**
- **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 [22]**

<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 [29]**

>

<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 [30]**

>>

- **ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [31]**

]]

[[ADV:

The Certification Service Provider shall have its operation periodically examined by independent external auditor. During the audit it shall be 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 [19]*
- *ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [21]*

<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; [30]*

>

- *ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [31]*

]]

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 shall be published via the website of the Certification Service Provider.

The Certification Service Provider reserves the right to inspect at any time involving an independent expert the operation of the providers who operate according to the present Certificate Policy(s) in order to verify compliance with the requirements.

8.1 Frequency or Circumstances of Assessment

The Certification Service Provider shall have the conformance assessment carried out annually.

<TLS:

An audit period shall not exceed one year in duration. The successive period-of-time audits shall cover the entire lifetime of each trusted Certification Unit, continuously (without gaps) from cradle to grave. >

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 can be performed only 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

8.4 Topics Covered by Assessment

The review shall cover at least 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

If the Certification Service Provider cooperates with an external Registration Authority, or it issued a subordinate Certificate for the certification unit of another organization then the listed areas shall be examined at these external organizations as well.

8.5 Actions Taken as a Result of Deficiency

The independent auditor shall summarize 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 shall be 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 shall publish the summary report on the assessment. It is not needed to disclose the discrepancies revealed during the independent system assessment, they can be treated as confidential information.

8.7 Self-Audits

The Certification Service Provider shall ensure regular monitoring of its internal processes, the details of which shall be specified in the Certification Practice Statement and in its inner regulations. It shall check the adequacy of the operation during a comprehensive internal audit at least once per every year.

<TLS:

A random check shall be performed quarterly on at least 3% **[[QUA: – in case when issued by external Registration Authority at least 6% –]]** of the Website Authentication Certificate issued since the previous inspection, whether they comply with the related Certificate Policies and Certification Practice Statement. >

<UNI:

A random check shall be performed 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 shall be performed 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 should be validated by using automated test tools (linters). >

If the Certification Service Provider cooperates with an external Registration Authority, then its processes shall be audited annually.

In case of a provider Certificate issued to a certification unit operated by another organization, the operation of the external certification unit shall be audited annually.

The Certification Service Provider may perform 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 fees applied by the Certification Service Provider shall be publicly disclosed in accordance with the applicable regulations.

9.1.1 Certificate Issuance or Renewal Fees

The Certification Service Provider may determine fees for its services related to issuance, renewal, modification or re-keying of the Certificates.

9.1.2 Certificate Access Fees

The Certification Service Provider shall grant 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 shall provide free of charge online CRL and OCSP service on the status of the issued Certificates for the Relying Parties.

9.1.4 Fees for Other Services

The Certification Service Provider may determine a service fee for other services provided to the Subscribers .

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

<TLS:

In order to facilitate trust the Certification Service Provider shall take financial responsibility to fulfil all its obligations defined in the present Certificate Policy, the related Certification Practice Statement and the service agreement concluded with the Client.

>

<not TLS: <not UNI:

In order to facilitate trust the Certification Service Provider shall comply with the financial and liability requirements below.

>>
<UNI: No stipulation.>

9.2.1 Insurance Coverage

[[QUA:
In order to cover the costs associated with the termination of the service activity and to sustain reliability the Certification Service Provider shall meet at least one of the following requirements:

- **The Certification Service Provider has at least an amount of 25 million HUF as an unconditional and irrevocable bank warranty.**
- **The Certification Service Provider provides deposit for the National Media and Infocommunications Authority as beneficiary at a financial institution to guarantee the payment of costs. The sum of the deposit shall be at least 25 million HUF.**
- **An EU company with at least 100 million HUF registered capital provides financial guarantee to the Certification Service Provider covering the costs. The amount of this financial guarantee shall be at least 25 million HUF.**

]]
[[ADV:
No stipulation.
]]

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

<not UNI:

- The Certification Service Provider shall have liability insurance to ensure reliability.
- The liability insurance policy shall cover 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 shall provide 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.

>
<UNI:
The Certification Service Provider need 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 shall manage the data of the Clients in accordance with the respective regulations.

9.3.1 Scope of Confidential Information

The Certification Service Provider shall specify the scope of data that are considered confidential information in its Certification Practice Statement.

9.3.2 Information Not Within the Scope of Confidential Information

The Certification Service Provider may consider all data public that are not specified as confidential in the Certification Practice Statement. Public data is for example:

- all data indicated in the Certificate
- data related to the status of the Certificate.

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 shall oblige its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

Circumstances when the Certification Service Provider may disclose the confidential data shall be determined case-by-case in the Certification Practice Statement.

<not UNI:
Such circumstances are, for example:

- mandatory provision of information to the supervisory authority ,
- providing information in civil litigation,
- provision of information upon request of the affected person.

>

9.4 Privacy of Personal Information

The Certification Service Provider shall take care of the protection of the personal data it manages. The operation and regulations of the Certification Service Provider shall comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [8] and the 2016/679 EU General Data Protection Regulation [3].

The Certification Service Provider shall:

- preserve
- upon expiry of the obligation to retain – unless the Client otherwise indicates – delete from the client database

the registered personal data and information on the Client in accordance with the legal requirements.

9.4.1 Privacy Plan

The Certification Service Provider shall have a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing shall be published via the website of the Certification Service Provider.

9.4.2 Information Treated as Private

The Certification Service Provider shall protect 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 shall store securely and protect the personal data related to the Certificate issuance and not indicated in the Certificate. The data shall be 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 shall only disclose 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 <SIG: 94. § of the Digital Citizenship Act [12] > <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 may be 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

may be disclosed as a part of the Certificate by the Certification Service Provider.

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 Certificate Policy 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 Certificate Policy and any other use for commercial or other purposes is strictly prohibited.

The present Certificate Policy 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 shall be determined in the Certification Practice Statement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The Certification Service Provider is responsible for the obligations set by the terms of this Certificate Policy, in the related Certification Practice Statement and in the service agreement concluded with the Client:

<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 [9] 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 [9] 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).

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 Certification Service Provider requires from the collaborating Registration Authorities to fully comply with the provisions of this Certificate Policy and the respective Certification Practice Statement.
The responsibilities of the Registration Authority are:

- to determine the identity of the <SEA: person authorized to represent the> Subject or Applicants

<not SEA:

- to determine the organizational identity of the Represented Organization, the identity and the eligibility of representation of the person acting on behalf of the Represented Organization

>

- to warrant the authentication of the recorded registration data
- prior to concluding service agreement to inform the user of the services on the availability and content of the Certificate Policy and the Certification Practice Statement and the terms and conditions of the service
- 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 Certificate Policy, the service agreement and its attachments – in particular the general terms and conditions -– and the Certification Practice Statement.

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

<SIG:

- 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 Certificate Policy and 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 <SIG: any of the electronic signatues or> <SEA: 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

<SIG:

- 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 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.

The Certification Practice Statement may include further obligations for the Subject or Applicant.

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

<SEA: No stipulation.>

<not SEA:

The Represented Organization is responsible for the certifications it issues, in particular the certifications, which proves that the Subject or Applicant is entitled to the usage of the Certificate containing the name of the Organization.

>

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 <SIG: 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

<not SIG: <not SEA:
The Certification Service Provider may limit its liability for loss.
>>
<not TLS: <not UNI:
The Certification Service Provider may limit its liability for loss.

- by Certificate,
- by the highest one-time amount of the obligations (transaction limit) that may be undertaken with the certificate,
- overall in relation to all certificates and damage events.

>>

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 the Certification Practice Statement, the service agreement, or the contracts concluded with the Clients.

9.9.2 Indemnification by Subscribers

The Certification Service Provider sets the term of claim for damages from Subscribers in the Certification Practice Statement and the service agreement.

9.9.3 Indemnification by Relying Parties

The Certification Service Provider sets the term of its claim for damages from Relying parties in the Certification Practice Statement.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific Certificate Policy is specified on the cover of the document.

9.10.2 Termination

The Certificate Policy is valid without a time limit until withdrawal or the issuance of the newer version of the Certificate Policy .

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the Certificate Policy the Certification Service Provider publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal via its website.

9.11 Individual Notices and Communications with Participants

The Certification Service Provider shall operate a customer service in order to maintain contact with its Clients.

9.12 Amendments

The Certification Service Provider reserves the right to change the Certificate Policy 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 reviews the Certificate Policy 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 Certificate Policy , 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 Certificate Policy appeared in the 2 tags at the end of the OID of the document identifier, so two Certificate Policy with different contents - brought into force - could not have the same OID identifier.

Starting with Certificate Policy version 3.1, the version number does not appear at the end of the OID, so the Certificate Policy OID identifier has the same value in all released versions. Individual Certificate Policy can be identified by using the document OID and version number together.

9.13 Dispute Resolution Provisions

The Certification Service Provider shall aim for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement shall follow the principle of gradual approach.

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 present Certificate Policy is compliant with the following 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 [8]
- (Hungarian) Act V of 2013. on the Civil Code [9]
- (Hungarian) Act CIII of 2023 on the digital state and certain rules for the provision of digital services [12]

<not UNI:

- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [13]

- (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 [14]
- (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 [16]

> <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 [15]

>>

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

The providers operating according to this Certificate Policy may only assign their rights and obligations to a third party with the prior written consent of the Certification Service Provider.

9.16.3 Severability

Should some of the provisions of the present Certificate Policy 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 [62] or the]]** CABF BR [60], 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 [59], 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 [59], 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 Certificate Policy , 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 II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[8] (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 CCXXII of 2015 on the general rules of electronic administration and trust services .

[11] (Hungarian) Act CXXX of 2016 on Civil Procedure .

[12] (Hungarian) Act CXIII of 2023 on the digital state and certain rules for the provision of digital services .

[13] (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 137/2016. (VI. 13.) on the requirements for the use of electronic signatures and stamps related to the provision of electronic administration services .

[16] (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] (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.

[18] ETSI EN 301 549 V3.2.1 (2021-03); Harmonised European Standard; Accessibility requirements for ICT products and services.

[19] ETSI EN 319 401 V3.2.1 (2026-01); Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] ETSI EN 319 412-5 V2.5.1 (2025-06); Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[28] ETSI TS 119 312 V1.5.1 (2024-12); Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[34] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

[35] ISO/IEC 15408 (parts 1 to 3) Information technology - Security techniques - Evaluation criteria for IT security.

[36] ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.

[37] IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.

[38] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

[39] IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.

[40] IETF RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, January 2005.

[41] IETF RFC 4035: Protocol Modifications for the DNS Security Extensions, March 2005.

[42] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.

[43] IETF RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs), May 2006.

[44] IETF RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, March 2008.

[45] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[46] IETF RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC, October 2009.

[47] IETF RFC 5952: A Recommendation for IPv6 Address Text Representation, August 2010.

[48] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

[49] IETF RFC 6840: Clarifications and Implementation Notes for DNS Security (DNSSEC), February 2013.

[50] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.

[51] IETF RFC 6962: Certificate Transparency, June 2013.

[52] IETF RFC 8555: Automatic Certificate Management Environment (ACME), March 2019.

[53] IETF RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019.

[54] IETF RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses, October 2023.

[55] IETF RFC 9654: Online Certificate Status Protocol (OCSP) Nonce Extension, August 2024.

[56] ITU X.501 Information technology - Open Systems Interconnection - The Directory: Models.

[57] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[58] ITU X.520 Information technology - Open Systems Interconnection - The Directory: Selected attribute types.

[59] 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.

[60] 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.

[61] 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.

[62] Guidelines for the Issuance and Management of Extended Validation Certificates, v.2.0.1. CA/Browser Forum, `https://cabforum.org/extended-validation/`, 2024.

[63] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[64] FIPS PUB 140-3 (2019 March 22): Security Requirements for Cryptographic Modules.

[65] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.

[66] CEN CWA 14169: Secure signature-creation devices “EAL 4+”, March 2004.

[67] PRADO - Public Register of Authentic identity and travel Documents Online, https://www.consilium.europa.eu/prado/en/prado-start-page.html .

[68] e-Szignó Certification Authority - General Terms and Conditions. .

[69] Microsec ltd. - Information on online video identification terms .