MICROSEC

e-Szignó Certificate Authority

eIDAS conform
Certificate for Website Authentication
Certification Practice Statement

ver. 3.12

Date of effect: 2024-04-03

OID	1.3.6.1.4.1.21528.2.1.1.167
Version	3.12
First version date of effect	2016-07-01
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	2024-04-03
Date of effect	2024-04-03

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

Version	Effect date	Description
2.0	2016-07-01	- New policies according to the RFC 3647 and the eIDAS requirements.
2.1	2016-09-05	- Changes according to the NMHH comments.
2.2	2016-10-30	- Changes according to the auditor comments.
2.3	2017-04-30	- Changes according to the NMHH comments.
2.4	2017-09-30	- Yearly revision.
2.6	2018-03-24	- Global revision. - Changes in the domain validation methods. - Introducing identity validation by state notaries. - Smaller improvements.
2.7	2018-09-15	- Yearly revision.
2.8	2018-12-14	- Changes based on the suggestions of the auditor.
2.9	2019-04-24	- Changes in the domain validation requirements. - Smaller improvements. Changes in the CABF BR.
2.10	2019-06-25	- Smaller improvements.
2.11	2019-09-25	- Yearly revision.
2.12	2019-12-12	- Changes based on the suggestions of the auditor.
2.13	2020-03-05	- Effect. - Identity validation rules. - Certificate modification. - HSM requirements. - Smaller improvements of wording.
2.14	2020-05-26	- Smaller improvements. - Add High Risk Certificate Report to Section 1.5.2. - Restructuring Chapter 2. - Adding more information for revocation in chapter 4.9. - Improve section 9.4.
2.16	2020-08-14	- Smaller improvements. - Remove OCSP Signing EKU from ICA certificates. - Certificate lifetime is 398 days.
2.17	2020-10-28	- Smaller improvements. - New domain validation possibility. - Improvements according to the auditor's and the supervisory body's findings.

Version	Effect date	Description
2.19	2020-12-28	- Smaller improvements. - More detailed rules for the Certificate renewal initiated by the Service Provider.
2.20	2021-03-03	- Smaller improvements. - Introduction of video-based natural person identification in Section 3.2.3. - Upgrading the rules for the generation of service provider's key pairs in the section 6.1.1. - Upgrading the description of the CRL profile in the section 7.2.
2.22	2021-06-30	- Smaller improvements. - Certificate types. - Who can initiate revocation. - Reporting key compromise. - Publication of conformity assessment results.
2.24	2021-11-30	- Smaller improvements. - Trusted Root Certificate Stores information. - subjectAltName, commonName and Organizational Unit fields requirements. - Change in BR 3.2.2.4.18 Validation method. - HSM certification.
2.25	2022-03-31	- Revision. - Specifying term dual control. - Upgrade algorythmic requirements. - Checking Key quality. - Introducing new SN fields. - KASZ based identity validation. - Upgrading email validation. - Upgrade the rules of electronic signature acceptance. - Process of certificate issuance. - Using linters. - QWAC policy change. - Adding test websites. - Depreciating OU field.

Version	Effect date	Description
3.1	2022-08-31	- Global revision. - Change in policy OID generation rules. - Managing revocation reasons. - ETSI TS 119 461 conformity. - Re-use period of validation data.
3.3	2022-11-30	- Global revision. - Contact person. - Customer Portal. - Stop supporting trademarks. - Certificate issuance process. - Certificate revocation process. - Certificate validity time. - Change in policy OID generation rules.
3.7	2023-08-30	- Global revision. - Revocation reasons. - Certificate validity times. - Key Usage. - Identity validation by a third party. - Managing security incidents. - Supported cryptographic algorithms. - New, dedicated TLS hierachy.
3.10	2023-10-30	- Identity validation of natural persons. - CA hierarchies.
3.11	2023-12-19	- Revision.
3.12	2024-04-03	- Removing SerialNumber extension.

Table of Contents

1 Introduction

This document is the *Certification Practice Statement* concerning the issuance of certificate for website authentication service of e-Szignó Certificate Authority operated by Microsec ltd. (hereinafter: Microsec or *Trust Service Provider*).

The *Trust Service Provider* provides its services for its *Client*s with whom it has contractual relationship.

The present *Certification Practice Statement* describes the framework of the provision of the aforementioned services and includes the detailed procedures and miscellaneous operating rules. It makes recommendations for the *Relying Parties* for the verification of the *Certificate*s created by using the services.

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

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

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

1.1 Overview

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

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

Furthermore the aim of this document is to support the users and relying parties of *Certificate*s, *Certificate Revocation List*s and online Certificate Status Responses issued by the *Trust Service Provider* to understand unambigously the ways of their management, the level of security guaranteed by them as well as the relevant technical, commercial and financial guarantees with legal responsibility related to them.

The content and format of the present document complies with the requirements of the IETF RFC 3647 [26] framework. It consists of 9 sections that contain the security requirements, processes defined by the *Trust Service Provider* and the practices to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, section headings where the document does not impose a requirement have the statement "No stipulation".

Considering the end user activity related to the services used, besides the present *Certification Practice Statement* further requirements may be found in the General Terms and Conditions and the service agreement concluded with the provider, the *Certificate Policies* applied by the

Trust Service Provider (see section 1.2.1) and other regulation or document independent from the *Trust Service Provider* as well.

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

1.2 Document Name and Identification

Issuer	e-Szignó Certificate Authority
Document name	eIDAS conform Certificate for Website Authentication Certification Practice Statement
Document version	3.12
Date of effect	2024-04-03

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

1.2.1 Certificate Policies

All *Certificate*s issued by the *Trust Service Provider* refer to that *Certificate Policy* on the basis of which they were issued.

The first seven numbers of the OID identifying the *Certificate Policy*s is 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 Certificate Authority
(1)	documents
(1)	public documents
(x)	unique identifier number of the document

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

OID	DENOMINATION	SHORT NAME
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, KWTSN
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

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

The detailed requirements of the listed *Certificate Policy*(s) can be found in " e-Szignó Certificate Authority – eIDAS conform Non Qualified Certificate for Website Authentication Certificate Policies ver.3.12." [51]

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

In case of *Website Authentication Certificate*s at the name of the *Subject* the domain name or IP address is indicated.

The *Website Authentication Certificate* can not be pseudonymous.

The *Trust Service Provider* conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [42] published at

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

URL.

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

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [LCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [14] standard;
- each *Certificate Policy* complies with the [DVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [14] standard;
- each *Certificate Policy* complies with the [OVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [14] standard, if the organization name is indicated in the *Certificate*;
- each *Certificate Policy* complies with the [IVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [14] standard, if the natural person's is indicated in the *Certificate*;

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 *Certificate*s.

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

1.2.2 Effect

Subject Scope

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

Temporal Scope

The present version of the *Certification Practice Statement* is effective from the 2024-04-03 date of effect, until withdrawal. The effect automatically terminates at the cessation of the services or at the issuance of the newer version of the *Certification Practice Statement*.

Personal Scope

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

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

People with disabilities

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

In order to establish equal opportunities regarding the service, the *Trust Service Provider* applies every possible and reasonable measure to make its services available without obstructions to disabled people as well. It is especially important them to ensure that the disabled clients receive services, which are adapted to their special needs, of the same quality as those for the other clients.

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

Geographical Scope

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

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

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

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

1.2.3 Security Levels

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

The authentication strength of the *Certificate Subject* in descending order:

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

Based on the used container in descending order by security:

- *Certificate*s issued on *Qualified Electronic Signature Creation Device* [***B*];
- *Certificate*s issued on *Cryptographic Hardware Device* [***H*];
- otherwise, for example *Certificate*s issued by software [***S*].

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

- qualified *Certificate*s issued on *Qualified Electronic Signature Creation Device* [M**B*];
- qualified *Certificate*s issued on *Cryptographic Hardware Device* [M**H*];
- qualified otherwise, for example *Certificate*s issued by software [M**S*];
- non-qualified, III. certification class *Certificate*s issued by e-Szignó Certificate Authority [H**S*];

- non-qualified, II. certification class *Certificate*s issued by e-Szignó Certificate Authority [K**S*];
- non-qualified *Certificate*s issued by other CA than e-Szignó Certificate Authority

During the communication with the *Client*s the *Trust Service Provider* supports the use of electronic channels and enables the use of electronic signature during the administration in most cases possible.

It is a general rule, that during the administration related to the *Certificate*s, 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 *Trust 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 *Certificate*s in case of new qualified *Certificate Application* or the modification of an existing one as a result of the same procedural identification rules it accepts the identification required for qualified *Certificate*).

1.3 PKI Participants

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

- the Microsec e-Szignó Certificate Authority,
- the *Client*s of Microsec e-Szignó Certificate Authority (*Subscriber*s and *Subject*s),
- *Relying Parties*,
- other participants.

1.3.1 Certification Authorities

Data of the *Trust Service Provider*

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

Customer Service Office

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

Introduction of the *Trust Service Provider*

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

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [4] (hereinafter: Eat.):

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

On the 1st of July, 2016. the whole system of services related to electronic signatures changed uniformly on a European basis with eIDAS and its complement Act CCXXII of 2015. [8] coming into force.

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

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

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

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

- qualified certificates for website authentication.

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

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

Quality and Information Security

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, Microsec has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

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

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

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

Based on the results of the risk assessment the *Trust Service Provider*

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

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

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

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

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

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

Business Providing Certification Services

Operating as an independent business unit within the organization of Microsec, e-Szignó Certificate Authority is responsible for creation and management of *Certificate*s, publication of *Certificate* repository and *Certificate* revocation status information, management and delivery of *Electronic Signature Creation Device*s and provision of the online certificate status service.

Tasks related to the management of policies and practices is also provided by this unit. The e-Szignó Certificate Authority has its own *Registration Authority*.

Services

The *Trust Service Provider* provides the following trust services defined by the eIDAS Regulation [1] to the *Subscriber* within the framework of the present *Certification Practice Statement*:

- Issuance of Certificates for Website Authentication

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

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

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

- *Applicant* may apply for a *Certificate* from the *Trust Service Provider*, the *Certificate* issuance is performed according to a *Certificate Policy* or policies;
- the *Applicant* may request the revocation of its *Certificate*;

The *Subscriber* may also request the revocation of the belonging *Subject*'s *Certificate*. These actions may also be requested by the *Organizational Administrator* authorized by the *Subscriber* and registered by the *Trust Service Provider*.

The *Trust Service Provider* makes the *Certificate Revocation List*s publicly available, containing the revocation status of the issued *Certificate*s. The *Trust Service Provider* also makes the *Certificate* public, based on the *Applicant*'s consent. The revoked or expired *Certificate* is invalid.

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

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

Certificate Types

The *Certificate Policies* supported by the present *Certification Practice Statement* are presented in section 1.2.1. The ID of the applied *Certificate Policy* is always indicated in the "Certificate Policies" field of the *Certificate*.

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

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

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

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

Test Certificates

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

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

The issuance of the test certificates is done under the "Microsec e-Szigno Test Root CA 2008" root exclusively created and operating for this task.

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

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

Certification Units

In the following those *Certification Unit*s will be described, that appear in the system of the e-Szignó Certificate Authority and stay under the effect of this *Certification Practice Statement*. Further information can be found in the certificate hierarchy of the *Trust Service Provider* at the following address:

`https://e-szigno.hu/en/pki-services/ca-certificates.html`

Latest, ECC based hierarchy dedicated to TLS

ECC-based dedicated hierarchy in line with Google's new requirements exclusively for issuing *Website Authentication Certificate*.

Each *Certification Unit* in this hierarchy uses at least 256 bit ECC keys.

- "e-Szigno TLS Root CA 2023" – Root certification unit,

  issues subordinate *Certificate*s for the *Certification Unit*s.

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

- "e-Szigno DV TLS CA 2023"

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

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

- "e-Szigno OV TLS CA 2023"

  This *Certification Unit* issues only OV (Organization Validated) and IV (Individual Validated) *Website Authentication Certificate*s in the "e-Szigno TLS Root CA 2023" hierarchy.

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

- OCSP responders

  Every *Certification Unit* certifies dedicated OCSP responder unit, which gives OCSP responses regarding the revocation status of the *Certificate*s issued by the given *Certification Unit*. The OCSP responder unit's name contains the "OCSP Responder" text besides the given *Certification Unit*'s name.

  The "OCSPSigning" extended key usage is present in the OCSP responder *Certificate*s.

In this hierarchy, all the issued end-user *Certificate*s use at least 2048-bit RSA keys or at least 256-bit ECC keys.

Multipurpose, ECC based hierarchy

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

  that issues ECC based *Certificate*s for the *Certification Unit*s of the *Trust Service Provider*.

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

- "e-Szigno Online SSL CA 2017"

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

- "e-Szigno Class3 SSL CA 2017"

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

- "e-Szigno Class2 SSL CA 2017"

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

- OCSP responders;

  every *Certification Unit* certifies dedicated OCSP responder unit, which gives responses regarding the revocation status of the Certificates issued by the given certification unit. The OCSP responder unit's name contains the "OCSP Responder"text besides the given certification unit name. The "OCSPSigning" extended key usage is present in the OCSP responder *Certificate*s.

The aforementioned units have 256-bit ECC based Certificates.

In this hierarchy, all the issued end-user *Certificate*s use at least 2048-bit RSA keys or at least 256-bit ECC keys.

Active, SHA-256 based RSA hierarchy

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

  Issues SHA-256 based *Certificate*s for the *Certification Unit*s of the *Trust Service Provider*.

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

- "Online e-Szigno SSL CA 2016"

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

- "e-Szigno SSL CA 2014"

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

- "Class2 e-Szigno SSL CA 2016"

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

- "e-Szigno DV TLS CA 2023"

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

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

- "e-Szigno OV TLS CA 2023"

  This *Certification Unit* issues only OV (Organization Validated) and IV (Individual Validated) *Website Authentication Certificate*s in the "e-Szigno TLS Root CA 2023" hierarchy.

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

- OCSP responders;

  every *Certification Unit* certifies dedicated OCSP responder unit, which gives responses regarding the revocation status of the Certificates issued by the given certification unit. The OCSP responder unit's name contains the "OCSP Responder" text besides the given certification unit name. The "OCSPSigning" extended key usage is present in the OCSP responder *Certificate*s.

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

In this hierarchy, all provider certificates use RSA keys with a key length of 2048 or 3072 bits. In this hierarchy all the issued end-user *Certificate*s use at least 2048-bit RSA keys or at least 256-bit ECC keys.

Publication of the *Root Certificate*s

The *Trust Service Provider* published the hash of the "Microsec e-Szigno Root CA 2009" *Root Certificate* in the June 17 2010 issue of Expressz (a Hungarian daily newspaper).

All the *Root Certificate*s are available through the webpage of the e-Szignó Certificate Authority.

- The "Microsec e-Szigno Root CA 2009" *Root Certificate* SHA-1 fingerprint [1] :
  `89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e`,

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

The same root also had an even earlier *Root Certificate* that has been never published in the printed media, but

the SHA-256 fingerprint of the same *Root Certificate*:
`3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8 e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78`

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

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

The following trusted certificate stores contain and distribute the "Microsec e-Szigno Root CA 2009" *Root Certificate*:

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

The inclusion of the "e-Szigno Root CA 2017" *Root Certificate* into the trusted certificate stores is in process.
The following trusted certificate stores contain and distribute the "e-Szigno Root CA 2017" *Root Certificate*:

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

has been published in early versions of the Microsec e-Szignó Signature Creation and Verification Program. The SHA-1 fingerprint of this first *Root Certificate* is:
`59 32 E2 00 30 0B AE 8D D7 9D 28 E5 AE 9D B0 05 50 3E 3B 8F`,
and the SHA-256 fingerprint is:
`72 F9 AF 21 58 18 1B AF 16 D6 0C 9B 4E 6F 4B D7 CA 8D 23 41 AD 48 AF DB 67 CB 4C 83 32 D5 46 F6`.
Signatures and *Certificate*s which were verified with the usage of the former *Root Certificate* can also be considered valid.

The inclusion of the "e-Szigno TLS Root CA 2023" *Root Certificate* into the trusted certificate stores is in process.

The

`https://e-szigno.hu/en/pki-services/browser-compatibility.html`

webpage contains more information on other browsers and certificate stores that contain the root certificates of the *Trust Service Provider* by default.

The other *Certificate*s of the *Trust Service Provider* can be verified based on the self certified *Root Certificate*s, so these *Certificate*s are only published by the *Trust Service Provider* on its webpage. If – law or in the framework of a contract or agreement between *Trust Service Provider*s – other *Trust Service Provider* issues certificates for the *Certification Unit*s of the *Trust Service Provider*, the *Trust Service Provider* shall publish the *Certificate*s on its webpage. The *Trust Service Provider* undertakes that in case of *Certificate*s issued for the *Trust Service Provider* in this manner, it complies with the cross certifying *Trust Service Provider*'s *Certificate Policy* and considers the included information binding.

Before the expiration date of the provider *Certificate*s, the *Trust Service Provider* generates new provider keys and starts new *Certification Unit*s, and takes all the necessary steps, so that the change of the provider *Certificate*s does not endanger the continuity of the services.

Chained Certification Service

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

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

- The *Trust Service Provider* and the cross-certified CA conclude a contract, the contract contains the exact conditions of the cross-certification. The cross-certified CA contracts the belonging *Client*s by itself, within this contract, the cross-certified CA is appointed as the certification authority.
- The *Trust Service Provider* takes full responsibility for the activities of the chained Certification Authority.
- The cross-certified certification authority can only issue *Certificate*s for a well defined scope of users.
- The cross-certified certification authority shall publish its *Certificate Policy*, and it shall operate according to it.
- The *Trust Service Provider* is entitled to verify the operation of the cross-certified provider.
- The *Trust Service Provider* revokes the *Certificate* issued during the cross certification if the cross-certified certification authority does not comply with its own *Certificate Policy*, or if the cross-certified certification authority indicates that its cross certified provider key is compromised.

- If the *Trust Service Provider* issues provider *Certificate* for another Certification Authority, it announces the fact to the National Media and Infocommunications Authority. If the cross-certified CA issues *Certificate*s that can be used natively and publicly, the cross-certified CA is bound to announce the cross-certification to the National Media and Infocommunications Authority, and ask for registration (except it is already registered at the National Media and Infocommunications Authority). These rules apply to other services related to electronic signatures as subordinate services (e.g. time stamp).

1.3.2 Registration Authorities

The *Trust Service Provider* implements registration and other tasks related to the issuing of *Certificate*s, as well as further certificate management tasks centrally, within the framework of a customer service operating within its own organization.
Tasks of the office:

- registration of the *Subject* indicated on end user *Certificate*s,
- administration and registration activity related to the issuing of *Certificate*s
- maintaining contact with *Client*s (reception of questions, announcements, requests and complaints, and the initiation of their processing),
- performance of certificate actions (revocation, certificate renewal, certificate modification and re-key).

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

- in the customer service office of the *Trust Service Provider*;
- the associate of the *Registration Authority* may visit *Client*s and perform mobile registration activities on the site according to the internal statements of the *Trust Service Provider*.

1.3.3 Subscribers

The *Client*s of the services provided by the *Trust Service Provider*:

- *Subscriber*
  - signs the service agreement with the *Trust Service Provider*,
  - accepts the General Terms and Conditions,
  - defines the scope of the *Applicant*s,
  - consent to the inclusion of organizational data in the *Certificate*,
  - may appoint *Organizational Administrator*s,
  - responsible for the payment of the fees arising from the usage of the service.
- *Applicant*
  - acts during the application for the given *Website Authentication Certificate*

1.3.4 Relying Parties

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

The *Trust Service Provider* maintains its contacts with the *Relying Party*s mainly through its website.

1.3.5 Other Participants

The independent auditor who makes the conformity assessment audit.

The supervisory authority.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The private keys belonging to the end-user *Certificate*s issued by the *Trust Service Provider* based on the present *Certification Practice Statement* can be only used for website or - if the *Website Authentication Certificate* makes it possible - client authentication.

1.4.2 Prohibited Certificate Uses

*Certificate*s issued in accordance with the present *Certificate Policies*, and the private keys belonging to them 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).

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

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

1.5.2 Contact Person

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

Contact person	e-Szignó Certificate 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

High-Priority Certificate Problem Report

The *Trust Service Provider* maintains a continuous 24x7 ability to respond internally to a High Piority Certificate Problem Report. The person reponsible for the processing of the received reports:

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

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

HighPriorityCertificateProblemReport@e-szigno.hu

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

https://e-szigno.hu/en/report-certification-security-events.html

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

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

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

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

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

The *Certification Practice Statement*s 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 *Trust Service Provider*s applying these policies.

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

http://webpub-ext.nmhh.hu/esign2016/

1.5.4 Practice Statement Approval Procedures

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

1.6 Definitions and Acronyms

1.6.1 Definitions

II. certification class	A group of non-qualified *Certificate Policies*, that make possible the *Certificate* issuance based on the *Applicant*'s remote registration.
III. certification class	A group of non-qualified *Certificate Policies*, that bound the *Certificate* issuance to the *Applicant*'s personal registration.
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	In case of a *Website Authentication Certificate* the *Subject* is the webserver, which is identified by a domain name or IP address.
Subject Unique Identifier	The globally unique identifier of the *Subject*, given by the *Trust Service Provider*. The identifier is in the "Subject DN / SerialNumber" field of the *Certificate*, according to the requirements of section 3.1.1.
Trust Service Supervisory Body	"The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [8] 91.§ 1. paragraph)*

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; " *(eIDAS [1] 3. article 16. point)*
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." *(Act CCXXII. of 2015. [8] 1. § 8. point)*
Trust Service Provider	"A natural or a legal person who provides one or more *Trust Service*s either as a qualified or as a non-qualified *Trust Service Provider*." *(eIDAS [1] 3. article 19. point)*
Certificate Transparency (CT) Log provider	CT Log provider defined by Certificate Transparency [35], which stores the issued *Certificate*s and the corresponding *PreCertificate*s.
Electronic Document	"Means any content stored in electronic form, in particular text or sound, visual or audiovisual recording" (eIDAS [1] 3. article 35. point)
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." (eIDAS [1] 3. article 33. point)
Subscriber	A person or organization signing the service agreement with the *Trust Service Provider* in order to use some of its services.
Precertificate	Digitally signed data structure (PreCert) defined by Certificate Transparency [35], which contains *Subject* data to be presented in the *Certificate* to be issued.

Relying Party	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.
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.
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 *Certificate*s, keeps a record, receives the *Certificate* related data changes, and publishes the regulations belonging to the *Certificate* and the information on the current state (especially on possible revocation) of the *Certificate*.
Certification Unit	A unit of the *Trust Service Provider*'s system that signs the *Certificate*s. 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 Unit*s.
Certificate Policy	"A *Trust Service Policy* which concerns the *Certificate* issued within the framework of the *Trust Service*." (Act CCXXII. of 2015. [8] 1. § 24. point)
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.
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 *Certificate*s issued to the given *Organization*.
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.
Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to the key-pair owner that the *Applicant* shall keep strictly secret. In case of webserver authentication the webserver shall use its private key during its authentication procedure. During the issuance of *Certificate*s, the *Certification Authority* uses the private keys of the *Certification Unit* for placing an electronic signature or seal on the *Certificate* to protect it.
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. In case of webserver authentication, the public key of the webserver is needed for the verification of its identity. The authenticity of the *Certificate*s 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.
Registration Claim	The data and statement given beforehand for the preparation of the *Certificate Application* and the service agreement to the *Trust Service Provider* by the *Client* in which the Client authorizes the *Trust 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 *Trust Service Provider*, when the continuation of the normal operation of the *Trust Service Provider* is not possible either temporarily or permanently.
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.
Server Authentication Certificate	*Certificate* which is used to authenticate a server or one of its services. The CN field of these *Certificate*s always contains a FQDN or an IP address. These type of *Certificate*'s are issued for example for the CISCO VPN server, domain controller, SCEP server, VPN server.
Organization	Legal person.
Organizational Certificate	A *Certificate*, which contains the name of an *Organization*. In this case the name of the *Organization* is indicated in the "O" field of the *Certificate*.

Organizational Administrator	The natural person who is acting in the name of the *Subscriber*, and is eligible to issue the *Certificate Application*, to grant the issuance of the *Certificate*, to act during the application, replacement and revocation of the *Certificate*s issued to the *Subscriber*.
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 Service*s." (Act CCXXII. of 2015. [8] 1. § point 41.)
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." (Act CCXXII. of 2015. [8] 1. § point 42.)
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.* (Act CCXXII. of 2015. [8] 1. § point 44.)
Certificate Application	The data and statements given by the *Applicant* to the *Trust 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 *Certificate*s. A Certification Authority has a Certificate Repository in which the issued *Certificate*s are disclosed, but the system containing *Certificate*s available to the application on the computer of the *Relying Party* is also called Certificate Repository.
Client	The collective term for the *Subscriber* and every related *Applicant* denomination.
Customer Portal	It is a web-based service created and continuously improved by e-Szignó Certificate Authority, in which customers 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 *Certificate*s 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*.
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." (eIDAS [1] article 3. point 38.) The webserver domain name 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.

1.6.2 Acronyms

CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator

DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
eIDAS	electronic Identification, Authentication and Signature
FQDN	Fully Qualified Domain Name
IDN	Internationalized Domain Name
IVC	Individual Validation Certificate
IVCP	Individual Validation Certificate Policy
LDAP	Lightweight Directory Access Protocol
NMHH	National Media and Infocommunications Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
TSP	Trust Service Provider

2 Publication and Repository Responsibilities

2.1 Repositories

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

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

The draft version of the new documents to be introduced are disclosed on the website before coming into force.

The documents in force are available on the site in addition to all previous versions of all documents.

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

After concluding the contract, the *Trust Service Provider* makes the General Terms and Conditions, the *Disclosure Statement*, the *Certificate Policy* and the *Certification Practice*

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

The *Trust Service Provider* notifies its *Client*s about the change of the General Terms and Conditions.

2.2 Publication of Certification Information

The *Trust Service Provider* publishes on its webpage (`https://www.e-szigno.hu`) and through LDAP protocol (`ldap://ldap.e-szigno.hu`)

- its provider *Certificate*s;
- the end user *Certificate*s in case of the *Applicant*'s prior consent.

Service Provider Certificates

With the following methods the *Certification Authority* discloses the *Certificate*s of the certification units and the online certificate status service units it operates:

- The denomination of the root certification units, and the hash of its root certificates in the *Certification Practice Statement*. (see section: 1.3.1.) The information related to their change of status are available at the website of the *Certification Authority*.
- The status change of *Certificate*s of intermediate (non-root) certification units is disclosed on the *Certificate Revocation List*s, its website and within the confines of the online certificate status response services.
- For the signers of the online certificate status responses the *Trust Service Provider* – compliant with the best international practice – issues a *Certificate* with extremely short period of validity (for 24 hours) thereby eliminating the need for *Certificate* revocation status verification.

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

End-User Certificates

With the following methods the *Trust Service Provider* discloses status information related to the end-user *Certificate*s which it had issued:

- on *Certificate Revocation List*s,
- within the confines of the online certification status response service.

The end-user *Certificate* revocation status information

is disclosed by the *Trust Service Provider*, and the *Applicant*'s consent is not required for it. For status information disclosing methods, see Section 4.10.

The *Trust Service Provider* guarantees, that the availability of its system publishing its service *Certificate*s, the *Certificate Repository* and the revocation status information on an annual basis will be at least at least 99% per year, while service downtimes may not exceed at most 24 hours in each case.

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

The *Trust Service Provider* doesn't store the issued *PreCertificate*s in its own *Certificate Repository* and doesn't publish them through its own services.

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the service are contained in the service contract to be signed by the *Client* during the conclusion of the contract, or in the General Terms and Conditions [52] document referenced therein.

The *Trust 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 on the webpage of the *Trust 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 *Trust 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 *Trust Service Provider* will close and publish the version of the General Terms and Conditions as amended with remarks on the 7th day prior to its becoming effective.

2.3.2 Frequency of the Certificates Disclosure

The *Trust Service Provider*, regarding the disclosure of *Certificate*s, follows the practices below:

- the *Certificate*s of the root certification units operated by it are disclosed before commencing the service;
- the *Certificate*s of the intermediate certification units operated by it are disclosed within 5 workdays after issuance;

- the *Trust Service Provider* publishes the *PreCertificate* corresponding to the enduser *Certificate* before the issuance of the *Certificate* through CT Log providers;

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

2.3.3 The Changed Revocation Status Publication Frequency

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

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

2.4 Access Controls on Repositories

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

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

2.5 Websites for testing

The *Trust Service Provider* operates special test websites to test and demonstrate the operation and usability of the valid, expired and revoked *Website Authentication Certificate*s. The websites are available on the following links:

RSA based Certificates

Valid Certificate

`https://sslca2014-valid.e-szigno.hu`

Expired Certificate

`https://sslca2014-expired.e-szigno.hu`

Revoked Certificate

`https://sslca2014-revoked.e-szigno.hu`

ECC based Certificates

Valid Certificate

`https://ec3sslca2017-valid.e-szigno.hu`

Expired Certificate

`https://ec3sslca2017-expired.e-szigno.hu`

Revoked Certificate

`https://ec3sslca2017-revoked.e-szigno.hu`

3 Identification and Authentication

3.1 Naming

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

The indicated Issuer ID and the Subject ID amongst the basic fields of the Certificate comply with the ITU X.520 standard [40], the RCF 5280 [30] and IETF RFC 6818 [33] recommendations name-specific format requirements, in addition the *Trust Service Provider* supports the "Subject Alternative Names" and "Issuer Alternative Names" fields located amongst the extensions.

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

3.1.1 Types of Names

Denomination of the *Subject*

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

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

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

  The value of the field shall be encoded as follows:

  Fully-Qualified Domain Name or Wildcard Domain Name :
  If the value is a Fully-Qualified Domain Name 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 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.

IPv4 address :
If the value is an IPv4 address, then the value shall be encoded as an "IPv4Address" as specified in RFC 3986 [28], 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 [31], Section 4. pg. 81

Always filled out.

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

The *Website Authentication Certificate* shall not be pseudonymous.

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

  In case of IVCP *Certificate* the surname of the natural person indicated in the *Certificate* is in this field.

  In case of DVCP and OVCP *Certificate* it is not filled.

  The name of a person may be indicated in a *Website Authentication Certificate* only if the person is the legal user, owner of the domainor IP address, or has the authorisation of them, and if the *Applicant* requests it. The value of this field shall be generated from the full name of the natural person, which is in the same form as verified by the *Trust Service Provider* according to the section 3.2.3.

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

  In case of IVCP *Website Authentication Certificate* the given name of the natural person indicated in the *Certificate* is in this field.

  In case of DVCP and OVCP *Certificate* it is not filled.

  The name of a person can be indicated in a *Website Authentication Certificate* only if the person is the legal user, owner of the domain or IP address , or has the authorisation of them, and if the *Applicant* requests it. The value of this field must be generated from the full name of the natural person, which is in the same form as verified by the *Trust Service Provider* according to the section 3.2.3.

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

  It is not filled.

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

  It is not filled.

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

  The *Trust Service Provider* doesn't fill this field.

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

  The *Certificate* never contains the "Serial Number" field.

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

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

  In case of DVCP and IVCP *Certificate* it is not filled.

  In case of OVCP *Certificate* the field may be used only if the *Applicant* requests it (in this case we call the *Certificate* as *Organizational Certificate*). The name of an *Organization* can be indicated in a *Website Authentication Certificate* only if the *Organization* is the legal user, owner of the domain or IP address, or has the authorisation of them.

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

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

  In case of an OVCP *Certificate* the identifier of the *Organization* indicated in the "O" field can be in this field according to Section 5.1.4 of ETSI EN 319 412-1 [15].

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

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

  In case of DVCP and IVCP *Certificate* this field is not filled.

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

  This field will not be filled out in *Certificate*s.

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

  In case of DVCP *Certificate* the two-letter country code - according to ISO 3166-1 [22] - of the country belonging to the 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 [22] - of the place of incorporation of the *Organization* indicated in the "O" field.

  In case of IVCP *Certificate* the two-letter country code - according to ISO 3166-1 [22] - of the address of the natural person named in the "SN" and "GN" fields.

  Always filled out.

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

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

  Not filled.

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

  In case of DVCP *Certificate* it is not filled.

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

  In case of IVCP *Certificate* the city name of the address of the natural person named in the "SN" and "GN" fields.

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

  In case of DVCP *Certificate* it is not filled.

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

  In case of IVCP *Certificate* the member state or province name, or the full name of the country – given in the "C" field – of the address of the natural person named in the "SN" and "GN" fields.

  Optional field.

- Postal Code – OID: 2.5.4.17 – Zip code

  In case of DVCP *Certificate* it is not filled.

  In case of OVCP *Certificate* zip or postal information of the place of incorporation of the *Organization* indicated in the "O" field.

  In case of IVCP *Certificate* zip or postal information of the address of the natural person named in the "SN" and "GN" fields.

  Optional field.

- Title (T) – OID: 2.5.4.12 – Title of the subject

  Not filled.

- Email Address (EMAIL) – OID: 1.2.840.113549.1.9.1 – The email address of the *Subject*

  Not filled.

The *Certificate*s issued in accordance with the present *Certification Practice Statement* might contain further – in accordance with the referenced *Certificate Policies* – "Subject DN" fields.

Only verified text values may be indicated on these fields (they shall not contain values indicating lack of data for example: ".", "-" or " ").

Extensions

- Subject Alternative Names - "Subject Alternative Names"

  The "Subject Alternative Names" extension is not listed as a critical extension in the *Certificate*. The content will be filled as follows.

  The "Subject Alternative Names" extension always contain at least one entry.

  Each entry is one of the following types:

  dNSName :

  The entry shall contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the *Trust 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 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 or the FQDN portion of the Wildcard Domain Name shall consist solely of Domain Labels that are P-Labels or Non-Reserved LDH-Labels.

iPAddress :
The entry shall contain an IPv4 or IPv6 address that the *Trust Service Provider* has validated in accordance with Section 3.2.2.3.
The entry shall not contain a Reserved IP Address.

Wildcard FQDNs are permitted.

The "Subject Alternative Names" extension shall not contain a Reserved IP Address or an Internal Name.

The "dNSName" field shall be in the "preferred name syntax", as specified in RFC 5280 [30], and thus shall not contain domain name containing underscore ("_") character.

The Denomination of the Certificate Issuer Certification Unit

The identifier of the *Certificate* issuer (Issuer field) is made up as follows:

- commonName (CN) – OID: 2.5.4.3
  The name of the *Certificate* issuer certification unit in English (see section: 1.3.1.).
- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  The name of the *Trust Service Provider* in English without accents.
- Organization Identifier (OrgId) – OID: 2.5.4.97
  Filling out is optional.
- Organizational Unit (OU) – OID: 2.5.4.11
  It is not filled.
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  City of the seat of the *Trust Service Provider* without accents.
- CountryName (C) – OID: 2.5.4.6
  "HU"
  Two letter code of the country of the seat of the *Trust Service Provider* according to ISO 3166-1 [22].
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  "`info@e-szigno.hu` "
  Filling out is optional.

The same data is indicated in the provider *Certificate* of the *Certificate* issuer, in the subject identifier field.

The Alternate Names of the Certificate Issuer Certification Unit

The Issuer Alternative Names field is not filled in the end user *Certificate*s.
Denominations indicated in the end user *Certificate* issuer's provider *Certificate*:

- In case of provider *Certificate*s based on SHA-256 only the email address is indicated in the alternate names field (rfc822Name).

3.1.2 Need for Names to be Meaningful

The following rules are applied to the "SubjectDN" field:

- the identifier shall be meaningful;
- the personal name in the *Certificate* shall be indicated the same way as verified by the *Trust 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 *Trust Service Provider* according to the section 3.2.2.

3.1.3 Anonymity or Pseudonymity of Subscribers

Website Authentication Certificate shall not be pseudonymous.

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 *Trust Service Provider*. In such case, the *Trust Service Provider* shall not give any further information on the *Client* than indicated in the *Certificate*, – provided that the law does not require it – only provides the information to help interpret the indicated data.

3.1.5 Uniqueness of Names

The *Subject* has a unique name in the *Certificate Repository* of the *Trust Service Provider*. In order to ensure the uniqueness, the *Trust Service Provider* gives each *Subject* an identifier (OID), – unique in the *Trust Service Provider*'s register – , which is indicated on the *Subject*'s unique identifier "Subject DN Serial Number" field.
The *Subject*s' unique identifiers (OID) are distributed in accordance with the order of processing the received *Certificate Application*s, ensuring the uniqueness of the "Subject" field in the *Certificate*.

Procedures to Resolve Disputes Relating the Names

The *Trust Service Provider* ensures that the *Client* is entitled to use the indicated names.
The *Trust Service Provider* revokes the *Certificate* in case of illegal use of the name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

The *Trust Service Provider* never includes trademark in the issued *Certificate*.

The *Trust Service Provider* uses the e-Szignó trademark during its service provision. The owner has given his consent to use the trademark.

3.2 Initial Identity Validation

The *Trust 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.

The *Trust 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 *Trust Service Provider* ensures and makes sure that the *Applicant* actually owns or manages the private key belonging to the public key of the *Certificate* .

If the *Applicant* requests the *Certificate* issuance for a key provided by it – typically in case of software certificates –, then the *Trust Service Provider* accepts the *Certificate Application* in PKCS#10 format, which at the same time verifies, that the holder of the private key did indeed request the *Certificate*.

3.2.2 Authentication of an Organization Identity or a Domain

3.2.2.1 Authentication of organization identity

The identity of the *Organization* is verified in the following cases:

- if the *Subject* of the *Certificate* to be issued is the *Organization*;
- if the *Subject* of the *Certificate* to be issued is the device or system operated by the *Organization* (including the *Website Authentication Certificate*s requested by the *Organization* ;

Prior to the issuance of an *Organizational Certificate* the *Trust Service Provider* verifies the organizational data authenticity to be included on the *Certificate* based on authentic public registers .

Furthermore it is verified in these cases, that:

- whether the natural person acting on behalf of the *Organization* is entitled to act on behalf of the *Organization*;
- whether the *Organization* consented to the issuance of the *Certificate*.

For performing the verification, the *Client* shall give the following data:

- the official denomination, registered office and legal status of the *Organization*,
- official registration number of the *Organization* (e.g. company registration number, tax identification number), if applicable;
- the name of the organization unit within the *Organization*, if its indication in the *Certificate* is requested,

The following certificates and evidences have to be attached to the *Certificate Application*:

- the submitter's statement, justifying that the data given for the *Organization* identification is correct and comply with reality;
- a certificate regarding that on behalf of the organization the *Certificate Application* submitter natural person is entitled to submit the application [2];
- In case of paper based documents the specimen signature of the person entitled to represent the *Organization* or other, official document equal to the specimen signature, which contains the name and signature of the persons entitled to represent the *Organization* [3];
- the *Organization* existence, name and the legal status verification document [4].

The *Trust Service Provider* is bound to verify the validity and authenticity of the presented documents.

Identity validation of foreign Organizations

The *Trust Service Provider* does not exclude the verification of *Organization*s registered abroad, as far as the data verification with adequate records of the country or obtaining a certificate issued by a trusted third party is feasible.
In respect of data verification, the *Trust Service Provider* accepts:

- information obtained directly from the government register of the foreign country by the *Trust Service Provider* or queried by a third party but authenticated by the primary data provider;
- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information is correct;
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the given information is correct.

[2] Section 3.2.5. contains the details regarding the verification of the authorizations and privileges.
[3] In case of Court of Registration registered firms the above documents can be acquired by the *Trust Service Provider*.
[4] In case of Court of Registration registered firms the above documents can be acquired by the *Trust Service Provider*.

The *Trust Service Provider* may accept other documents and evidences too, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the *Trust Service Provider* is the *Client*ś responsibility.

The *Trust Service Provider* only accepts valid documents, and evidences not older than 3 months.

The *Trust Service Provider* does not issue the *Certificate* if it considers that based on its internal rules it can not verify with corresponding confidence a certificate issued abroad, a document or the data of the foreign organization.

3.2.2.2 Validation of Domain Authorization or Control

At least one domain name or IP address shall be in the *Website Authentication Certificate*s.

Before the issuance of *Website Authentication Certificate*s the *Trust Service Provider* ensures about the genuineness of the domain name 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 or IP address.

If more than one domain name or IP address is indicated in the *Certificate*, the aforementioned verification shall be carried out in each case.

If a domain name containing a wildcard "*" character is indicated in the *Certificate* (wildcard certificate), the *Trust Service Provider* ensures that, the *Applicant* is the authorized user of the entire domain namespace covered by the wildcard domain name. The *Trust Service Provider* does not issue a *Certificate*, in which the domain name space to be covered by the wildcard domain name is a registered gTLD or ccTLD (for example: "*.com", "*.co.uk"), or a subdomain under these TLDs under which public domain name registration is directly possible. The *Trust Service Provider* checks the public domain names open for direct registration in the "ICANN DOMAINS" section of "Public Suffix List" (`https://publicsuffix.org/list/public_suffix_list.dat`).

The *Trust Service Provider* issues *Certificate*s for public domain names and IP addresses used on the Internet, not for domain names and IP addresses reserved for internal use.

The *Trust Service Provider* issues *Certificate*s only for those top level domains which can be found on the actual IANA Root Zone Database.

The *Trust Service Provider* supports the usage of the Internationalized Domain Names according to the IDNA2003 [25] requirements.

The *Trust Service Provider* doesn't issue *Certificate* for the ".onion" 'special use' top level domain.

The *Trust 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 [42].

The *Trust Service Provider* maintains a record of which of the following domain validation methods was used, including the relevant CA/BF BR version number.

3.2.2.2.1 Validating the Applicant as a Domain Contact (BR 3.2.2.4.1)

This validation method is not used.

3.2.2.2.2 Email to Domain Contact (BR 3.2.2.4.2)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The *Trust Service Provider* sends the Random Value to an email address identified as a Domain Contact.

Each email may be used for identification of multiple Domain Names.

The *Trust Service Provider* may send the email identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email.

The Random Value is unique in each email.

The *Trust Service Provider* may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for 30 days from its creation.

3.2.2.2.3 Phone Contact with Domain Contact (BR 3.2.2.4.3)

This validation method is not used.

3.2.2.2.4 Constructed Email to Domain Contact (BR 3.2.2.4.4)

Confirming the *Applicant*'s control over the FQDN by

- sending an email to one or more addresses created by using
  - "admin",
  - "administrator",
  - "webmaster",
  - "hostmaster" or
  - "postmaster"

  as the local part, followed by the atsign ("@"), followed by an Authorization Domain Name,
- including a Random Value in the email, and
- receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value is unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged.

The Random Value remains valid for use in a confirming response for 30 days from its creation.

3.2.2.2.5 Domain Authorization Document (BR 3.2.2.4.5)

This validation method is not used.

3.2.2.2.6 Agreed-Upon Change to Website (BR 3.2.2.4.6)

This validation method is not used.

3.2.2.2.7 DNS Change (BR 3.2.2.4.7)

Confirming the *Applicant*'s control over the FQDN by confirming the presence of a Request Token containing a Random Value in a DNS TXT record for an Authorization Domain Name.

The *Trust Service Provider* provides unique Request Token for each *Certificate Application* which is valid only for 30 days.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.8 IP Address (BR 3.2.2.4.8)

This validation method is not used.

3.2.2.2.9 Test Certificate (BR 3.2.2.4.9)

This validation method is not used.

3.2.2.2.10 TLS Using a Random Number (BR 3.2.2.4.10)

This validation method is not used.

3.2.2.2.11 Any Other Method (BR 3.2.2.4.11)

This validation method is not used.

3.2.2.2.12 Validating Applicant as a Domain Contact (BR 3.2.2.4.12)

This validation method is not used.

3.2.2.2.13 Email to DNS CAA Contact (BR 3.2.2.4.13)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The Random Value is sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in IETF RFC 8659 [36] Section 3.

The CAA Email Contact value shall be given in the CAA contactemail property which has the email address as its parameter. The email address shall be given in the format defined by the rfc 6532 [32] section 3.2 with no additional padding or structure.

Example:

$ORIGIN example.com

CAA 0 contactemail "domainowner@example.com"

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated. The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) shall remain unchanged.

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.14 Email to DNS TXT Contact (BR 3.2.2.4.14)

Confirming the *Applicant*'s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The Random Value is sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

The DNS TXT record shall be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record shall be a valid email address as defined in RFC 6532 [32] section 3.2, with no additional padding or structure, or it cannot be used.

Each email may confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email may be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated. The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) shall remain unchanged.

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.15 Phone Contact with Domain Contact (BR 3.2.2.4.15)

Confirming the *Applicant*'s control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN.

Each phone call may confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. In the event that someone other than a Domain Contact is reached, the *Trust Service Provider* may request to be transferred to the Domain Contact.

In the event of reaching voicemail, the *Trust Service Provider* may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the *Trust Service Provider* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.16 Phone Contact with DNS TXT Record Phone Contact (BR 3.2.2.4.16)

Confirming the *Applicant*'s control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN.

The DNS TXT record shall be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record shall be a valid Global Number as defined in RFC 3966 [27] section 5.1.4, or it cannot be used.

Each phone call may confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The *Trust Service Provider* may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the *Trust Service Provider* may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the *Trust Service Provider* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.17 Phone Contact with DNS CAA Phone Contact (BR 3.2.2.4.17)

Confirming the *Applicant*'s control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN.

Each phone call may confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The relevant CAA Resource Record Set shall be found using the search algorithm defined in IETF RFC 8659 [36] Section 3.

The phone number shall be in the CAA contactphone property as its parameter. The entire parameter value shall be a valid Global Number as defined in RFC 3966 [27] section 5.1.4, or it cannot be used. Global Numbers shall have a preceding + and a country code and may contain visual separators.

Example:

$ORIGIN example.com.

CAA 0 contactphone "+36 (1) 123-4567"

The *Trust Service Provider* may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.

In the event of reaching voicemail, the *Trust Service Provider* may leave the Random Value and the ADN(s) being validated. The Random Value shall be returned to the *Trust Service Provider* to approve the request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Once the FQDN has been validated using this method, the *Trust Service Provider* may also issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.2.18 Agreed-Upon Change to Website v2 (BR 3.2.2.4.18)

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 *Trust 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 *Trust Service Provider* doesn't accept redirects (3xx HTTP status code).

The Random Value included in the Request Token:

- is unique to each *Certificate Application*;
- will remain valid for use in a confirming response for 30 days from its creation.

The *Trust Service Provider* shall not issue *Certificate*s for other FQDNs that end with all the labels of the validated FQDN unless the *Trust Service Provider* performs a separate validation for that FQDN using an authorized method.

This method is not suitable for validating Wildcard Domain Names.

3.2.2.2.19 Agreed-Upon Change to Website - ACME (BR 3.2.2.4.19)

This validation method is not used.

3.2.2.2.20 TLS Using ALPN (BR 3.2.2.4.20)

This validation method is not used.

3.2.2.3 Authentication for an IP Address

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 *Trust Service Provider* confirms that prior to issuance, the *Trust 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 *Certificate*s 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 *Trust Service Provider* maintains a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address.

3.2.2.3.1 Agreed-Upon Change to Website (BR 3.2.2.5.1)

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 *Trust Service Provider* via HTTP/HTTPS over an Authorized Port.

The Random Value shall not appear in the request.

The *Trust Service Provider* shall provide a Random Value unique to the *Certificate Application* and shall not use the Random Value longer than 30 days.

3.2.2.3.2 Email, Fax, SMS, or Postal Mail to IP Address Contact (BR 3.2.2.5.2)

Confirming the *Applicant*'s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value shall be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

The *Trust Service Provider* may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value shall be unique in each email, fax, SMS, or postal mail.

The *Trust Service Provider* may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.3.3 Reverse Address Lookup (BR 3.2.2.5.3)

Confirming the *Applicant*'s control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under section 3.2.2.2. of this document.

3.2.2.3.4 Any Other Method (BR 3.2.2.5.4)

This validation method is not used.

3.2.2.3.5 Phone Contact with IP Address Contact (BR 3.2.2.5.5)

Confirming the *Applicant*'s control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the *Applicant*'s request for validation of the IP Address. The *Trust Service Provider* shall place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call shall be made to a single number.

In the event that someone other than an IP Address Contact is reached, the *Trust Service Provider* may request to be transferred to the IP Address Contact.

In the event of reaching voicemail, the *Trust Service Provider* may leave the Random Value and the IP Address(es) being validated. The Random Value shall be returned to the *Trust Service Provider* to approve the request.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.2.3.6 ACME "http-01" method for IP Addresses (BR 3.2.2.5.6)

This validation method is not used.

3.2.2.3.7 ACME "tls-alpn-01" method for IP Addresses (BR 3.2.2.5.7)

This validation method is not used.

3.2.3 Authentication of an Individual Identity

The identity of the *Website Authentication Certificate* requester natural person shall be verified.

The *Trust Service Provider* verifies the identity of the natural person applying one of the following methods, subject to the availability of technical and other conditions.

1. **During face to face identity validation**

   In case of *Certificate*s 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:

  - officier 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 *Trust Service Provider*

- the identity of the natural person is verified during personal identification based on a suitable official proof of identity card;

  The identification can be based on the following official documents:

  - in case of natural persons within the scope of Act LXVI. of 1992. (henceforth: Nytv. [3]) official cards appropriate for verifying identity defined in Nytv. in accordance with Eüt. 82.§ (3) [8];
  - in case of natural persons outside the scope of Nytv. [3] 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 [5] in accordance with Eüt. 82.§ (4) [8];
  - in case of identification of natural persons who have none of the documents mentioned above the *Trust Service Provider* applies personal identity validation in accordance with Eüt. 82.§ (5) [8] 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" [50], 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;

- the natural person's address shall be checked against a residence card suitable for identification;

- The person performing the identity validation verifies, whether any alteration or counterfeiting happened to the presented identity cards.

During the initial identity validation the *Trust 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*.

In case of *Certificate*s belonging to the II. certification class:

- there's no need for personal meeting for the identification of the person, in such cases the *Trust Service Provider* can identify the *Applicant* remotely;

  During remote identification, the *Trust 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 *Trust Service Provider*.

- the *Applicant* sends a copy of one of its official identity cards suitable for identity validation to the *Trust Service Provider*.

- the *Applicant* sends the copy of its official identity cards suitable for the validation of its address to the *Trust 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;
- The *Trust Service Provider* performs data reconciliation with authentic public registers in case of certificates belonging to the II. certification class.
- the natural person's address shall be checked against a residence card suitable for identification;
- The *Registration Authority* verifies the authenticity of the presented cards in this case too. Furthermore the *Trust Service Provider* verifies that the *Certificate Application* was really sent by the identified *Applicant* through a trustable communication channel. Then the *Trust Service Provider* asks for confirmation from the *Applicant* through such a contact that was not given during the application procedure, but it originates from other sources. There is no need for confirmation through more reliable communication channel, in case of identification performed by an appropriate electronic identification device or by a *Certificate Application* submitted with an appropriate electronic signature.
- The *Applicant* can prove its identity at its own discretion according to the III. certification class.

Further rules for the identity validation of foreign citizens

The *Trust Service Provider* may accept the identification carried out by a public notary as equivalent to the identity validation made by its own *Registration Authority*, if the public notary registered in such foreign country,

- which concluded an international bilateral treaty with Hungary on the mutual recognition of public deeds or
- which country ratified the "Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents" of 5th October 1961. (Apostille)

The document issued by the public notary shall follow the requirements specified in the given agreement.

The *Trust Service Provider* may accept the *Certificate Application* signed before the notary public if the notarial certification clause shows that

- the notary public has verified the identity of the *Applicant* based on a suitable official document for identity validation (ID card, passport etc.);
- the *Applicant* has signed the *Certificate Application* in the presence of the notary public.

The *Trust Service Provider* always accepts the original documents when issued in Hungarian or English language. In case of documents issued on any other language the *Trust Service Provider* may request the official Hungarian translation of the documents translated by the OFFI (Hungarian Office for Translation and Attestation).

The *Trust Service Provider* may also accept other documents and evidences, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the *Trust Service Provider* is the *Client*'s responsibility.

The *Trust Service Provider* only accepts valid documents and evidences not older than 3 months.

The *Trust Service Provider* does not issue the *Certificate* if it considers that based on its internal rules, that it can not verify with corresponding confidence the certificate, document or the data of the foreign organization.

2. **By identification traced back to a certificate of an electronic signature**

In this case:

- The *Applicant* submits the *Certificate Application* in electronic form with 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 *Trust Service Provider* verifies the authenticity and confidentiality of the *Certificate Application* on the entire certification chain.

3. **Using other nationally recognized methods of identification offering security equivalent to personal presence**

The *Trust Service Provider* may also verify the identity of the natural person in accordance with 541/2020. (XII. 2.) Hungarian Government Decree [12], using the following methods which are recognized as equivalent to the face to face validation at national level.

(a) identification by means of an electronic communication device providing video technology (hereinafter: video technology identification)

(b) identification using the identification service provided by the Hungarian Government pursuant to Section 4 (1) of the Decree (hereinafter: KASZ identification)

In this case, the *Trust 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.

Video technology identification

During the video technology identification, the *Trust Service Provider*:

(a) In the case of video technology identification, the *Trust 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 *Trust Service Provider* that the person in the ID document is the same as the *Client* in the video.

(b) The *Trust Service Provider* sets out in detail in the "Information on online video identification terms" [53] 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 on the *Trust 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" [53] document and during the video recording, the *Trust 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 *Trust Service Provider* records and keeps for at least 10 years from the date of recording the entire communication established between the *Trust 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 *Trust Service Provider*, and the *Client* can be identified with the image shown on the ID document based on his / her image.

(f) The *Trust 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 *Trust 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 *Trust Service Provider*.

(h) A live telecommunications connection is also eligible if the *Trust 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 *Trust Service Provider* shall issue the *Certificate* only if the video technology identification fully complies with the above requirements.

KASZ identification

(a) In the case of KASZ identification, the IT system provided by the *Trust 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 *Trust 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 *Trust Service Provider* uses the central and regulated electronic administration services required for identification as a market participant in accordance with the E-Administration Act [8] and its implementing regulation.

(c) The *Trust Service Provider* may use the authentication service through the central authentication agent service or independently.

The *Trust Service Provider* uses the data reconciled during a previous natural person identification procedure, if the *Applicant* requests new *Certificate* instead of an expired or a revoked one, or if he requests a new *Certificate* besides the existing one during the validity period of the service agreement. The authenticity of the *Certificate Application*, the validity of the data to be icluded in the *Certificate* and the identity of the *Applicant* is validated by the *Trust Service Provider*.

3.2.4 Non-Verified Subscriber Information

Only that data can be in the *Certificate* issued by the *Trust Service Provider* which has been verified by the *Trust Service Provider*.

3.2.5 Validation of Authority

The identity of the natural person representing the legal person shall be verified according to the requirements of Section 3.2.3. before issuing an *Organizational Certificate*.

The right of representation of the natural person shall be verified.

Persons entitled to act on behalf of an *Organization*:

- a person authorized to represent the given *Organization*,
- a person who is mandated for that purpose by an authorized person to represent the *Organization*,
- an *Organizational Administrator* appointed by an authorized person to represent the *Organization*.

The *Organizational Administrator* can be appointed during *Certificate Application*, or anytime later with the help of the corresponding form. The identifier information of the designated person(s) shall be given on the form, by which he/she can be identified in later litigation. The form shall be signed (manually or by creating a qualified electronic signature based on a non pseudonymous *Certificate*) by the representative of the *Organization*, which is verified by the registration associate of the *Trust Service Provider* when received.

Appointing an *Organizational Administrator* is not mandatory, and multiple *Organizational Administrator*s can be appointed too. If there is no appointed *Organizational Administrator*, then the person entitled to represent the *Organization* can perform this task.

3.2.6 Criteria for Interoperation

The *Trust Service Provider* does not work together with other Certification Authorities during the provision of the service.

3.2.7 Email address validation

This section defines the used processes and procedures for confirming the *Applicant*'s control of Mailbox Addresses to be included in issued *Certificate*s.

The *Trust Service Provider* verifies that *Applicant* controls the email accounts associated with all Mailbox Fields referenced in the *Certificate* or has been authorized by the email account holder to act on the account holder's behalf.

The *Trust Service Provider* never delegates the verification of mailbox authorization or control.

The *Trust Service Provider* maintains a record of which validation method was used to validate every domain or email address in issued *Certificate*s, including the relevant version number from the S/MIME Baseline Requirements [43] or TLS Baseline Requirements [42].

Completed validations of *Applicant*'s authority may be valid for the issuance of multiple *Certificate*s over time. In all cases, the validation shall have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to *Certificate* issuance.

Validating control over mailbox via domain

The *Trust Service Provider* may confirm that the *Applicant* has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the *Certificate*.

The *Trust Service Provider* uses only the following approved methods in Section 3.2.2.4 of the TLS Baseline Requirements [42] to perform this verification:

- Email to Domain Contact (BR 3.2.2.4.2)
- Constructed Email to Domain Contact (BR 3.2.2.4.4)
- DNS Change (BR 3.2.2.4.7)
- Email to DNS CAA Contact (BR 3.2.2.4.13)
- Email to DNS TXT Contact (BR 3.2.2.4.14)
- Phone Contact with Domain Contact (BR 3.2.2.4.15)
- Phone Contact with DNS TXT Record Phone Contact (BR 3.2.2.4.16)
- Phone Contact with DNS CAA Phone Contact (BR 3.2.2.4.17)
- Agreed-Upon Change to Website v2 (BR 3.2.2.4.18)

Validating control over mailbox via email

For applications submitted on the *Trust Service Provider*'s web site, the *Trust Service Provider* validates the *Applicant*'s email address by verifying the email address before completing the *Certificate Application* form. The web page asks for the *Applicant*'s email address before filling in the form and does not allow other details to be filled in. The *Trust Service Provider* will send a four-digit random number which is unique in each sent email, and a unique URL with a limited validity period, including a unique random number, to the email address provided.

The information required for validation will only be sent to the email address to be validated, it will not be shared in any other way.

The *Applicant* can only complete the form by entering the received four-digit number on the form, or by clicking on the unique link provided. Each incoming *Certificate Application* therefore has an email address that is verified during operation.

In the case of a *Certificate Application* submitted otherwise, the *Trust Service Provider* sends an email with a unique random number, or with a unique URL with a limited validity period, including a unique random number, to the email address to be verified.

The information required for validation will only be sent to the email address to be validated, it will not be shared in any other way.

Applicant shall respond and confirm the request by entering the random number or by clicking on the unique link provided.

The random number is valid for no more than 30 days.

3.3 Identification and Authentication for Re-key Requests

Re-key is the process when the *Trust 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 *Trust Service Provider* verifies the existence and checks the validity of the affected *Certificate*.

The *Trust Service Provider* accepts re-key requests in case of valid and not valid (revoked or expired) *Certificate*s 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 *Applicant* takes place as described in section 3.2.3.

When the expiry date of the new *Certificate* is not later than the *Certificate* to be re-keyed, the *Trust Service Provider* re-uses the results and evidences collected during the original validation process.

3.3.2 Identification and Authentication for invalid Certificate

The *Trust Service Provider* accepts re-key requests – only during the validity period of the service agreement– in case of *Certificate*s revoked or expired.

The identification of the *Applicant* takes place as described in section 3.2.3.

3.4 Identification and Authentication in Case of Certificate Renewal Requests

Certificate renewal is the process when the *Trust 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 *Certificate*s.

3.4.1 Identification and Authentication in Case of a Valid Certificate

The identification of the *Applicant* takes place as described in section 3.2.3.

In case of *Certificate* renewal initiated by the *Trust Service Provider*, the *Trust 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 renewed.

3.4.2 Identification and Authentication in Case of an Invalid Certificate

Invalid *Certificate* can't be renewed.

3.5 Identification and Authentication for Certificate Modification requests

Certificate modification is the process, when the *Trust 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 *Applicant* takes place as described in section 3.2.3.

If the modified *Certificate* expires on the same time as the original *Certificate*, during the procedure, the *Trust Service Provider* may use the results of inspections performed prior to the issuance of the original *Certificate*.

3.5.2 Identification and Authentication in Case of an Invalid Certificate

Invalid *Certificate* can't be renewed.

3.6 Identification and Authentication for Revocation Request

The *Trust Service Provider* receives and processes the requests related to the revocation of the *Certificate*s, and the announcements (for example related to the private key compromise or to the improper use of the *Certificate*) concerning the revocation of the *Certificate*s.

The *Trust Service Provider* ensures that the requests only get accepted from authorized parties besides the rapid processing of the suspension and revocation requests.

In each case, the *Trust Service Provider* verifies the authenticity of the submitted request and the eligibility of the person submitting the request.

The identification and authentication aspects of such requests are described in section 4.9. .

In case of *Website Authentication Certificate*s, suspension is not possible.

3.7 Verified Method of Communication

To assist in securely communicating with the *Applicant* and confirming that the *Applicant* is aware of and approves issuance, the *Trust Service Provider* verifies an email address, telephone number, fax number or postal delivery address as a "Verified Method of Communication" with the *Applicant*.

To verify a "Verified Method of Communication" with the *Applicant*, the *Trust Service Provider*

- verifies that the "Verified Method of Communication" belongs to the *Applicant* based on
  - records provided by the applicable Telecommunication Service Provider in case of telephone number or fax number;
  - a Qualified Government Information Source;
  - a Verified Professional Letter issued by a public notary;
  - based on the identity validation of the *Applicant*.
- confirms the "Verified Method of Communication". The registration officier of the *Trust Service Provider* contacts the *Applicant* by using the "Verified Method of Communication". The reliability of the "Verified Method of Communication" is proved by physical presence of the *Applicant* or by using a "Communication Channel Verification Password".

4 Certificate Life-Cycle Operational Requirements

The issuance of a new *Certificate* for a new *Subject* shall precede the transmission of the *Registration Application* required to the *Trust Service Provider* and signing of the service agreement on the *Subscriber*'s part as well as signing of the *Certificate Application* of the *Applicant*'s part.

Certificate replacement is the process, when previously registered (and during that, identified) *Subject* requests a new *Certificate* instead of the existing one (issued pursuant to a valid service agreement).

Certificate replacement can take place for the below reasons:

- *Certificate renewal* means requesting a *Certificate* with the same data indicated in it as in the previous one by the *Subject* and both *Certificate*s are issued for the same public key. The details of *Certificate renewal* are discussed in section 4.6.
- *Certificate modification* means requesting the modification of the *Subject*'s *Certificate* considering the change of the *Subject*'s data included in the *Certificate*. The *Trust Service Provider* receives *Certificate modification* requests during the validity period of the *Certificate*. Over the course of Certificate modification, the new *Certificate* is issued to the same public key. The details of *Certificate modification* are described in section 4.8.
- *Re-key* means a new *Certificate* issuance by the *Trust Service Provider* for a new public key at the request of the *Subject* during the *Certificate*'s validity period or after expiration. The details of *Certificate renewal* are discussed in section 4.7.

When *Client*s – with a valid service agreement– request a new *Certificate*, then the modification of the service agreement is necessary.

The status of a *Certificate* can be valid, revoked or expired. Regulations related to the status changes are discussed in section 4.9., and the *Certificate* status service is discussed in section 4.10.

The *Trust Service Provider* provides Certificate maintenance only under the force of the related service agreement. The requirements related to the termination of service agreement are discussed in section 4.11.

4.1 Application for a Certificate

For each new *Certificate* issuance, *Certificate Application* submission is required. Prior to submitting the first *Certificate Application*, the *Applicant* shall submit a *Registration Application* to the *Trust Service Provider*, this can be done through the website of the *Trust Service Provider*, for instance. The *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 *Trust Service Provider* for the management of their personal data in the Registration request.

The *Trust Service Provider* doesn't consider the data indicated in the *Registration Application* authentic until the *Applicant* confirms them in a *Certificate Application*.

In case the conclusion of a new service agreement is necessary, the *Trust Service Provider* prepares the *Subscriber*'s service agreement based on the information given in the *Registration Application*.

The service agreement shall contain the types of *Certificate* available for specific *Subject*s in the frame of the services within the confines of the Agreement.

A new *Certificate* can be requested within the confines of a previously concluded service agreement. If the *Certificate* (*Certificate* replacement) is issued as a replacement of a *Certificate* indicated in the service agreement, it is not necessary to modify the service agreement. If the *Client* requests a new *Certificate* in addition to the extant ones, the service agreement shall be modified.

The *Trust Service Provider* informs the *Subscriber* about the *Certificate* usage terms and conditions prior to the conclusion of the contract.

If the *Applicant* is not the same as the *Subscriber*, then the aforementioned information is also given to the *Applicant*.

The *Trust Service Provider* publishes the documents containing the information in an intelligible form, in an electronically downloadable form on its website, and upon request makes it available at the customer service office for on-site reading. At the Customer Service Office, the *Client* has the opportunity to read the documents and consult.

In the *Certificate Application* the *Subject* shall at least include the data below:

- data to be indicated in the *Certificate* (for example domain name, IP address, name of *Organization*, city, country);
- the personal identification information of the

  Applicant

  (full name, number of the identity document, mother's name, date and time of birth);
- the contact of the

  Applicant

  (telephone number, email address);
- in case of *Organizational Certificate* application, the data of the *Organization* (official name, domicile, optionally: identification data, denomination ot the organization department);
- the *Subscriber*'s data (billing information);

In conjunction with the *Certificate Application* the *Trust Service Provider* ask for and check at least the following documents, certifications, procurations and declarations (in case of remote identification the copies of these):

- documents necessary to identify the

  Applicant

  according to Section 3.2.3;
- in case of *Organizational Certificate* application, the documents for the identification of the *Organization* according to Section 3.2.2;
- in case of *Organizational Certificate* application, the evidence issued by the *Organization* that the *Applicant* is entitled for representing the *Organization* according to section 3.2.5.;

4.1.1 Who May Submit a Certificate Application

Certificate Application may only be submitted by natural persons, to request a *Certificate* for themselves 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 *Trust Service Provider*) concerning *Certificate* issuance and maintenance.

The

Applicant

may submit the *Certificate Application* in the following ways:

- on paper signed manually at the customer service of the *Trust Service Provider* or at the mobile registration associate of the *Trust Service Provider*, on a date previously agreed (then, in case of *Certificate*s 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 *Trust Service Provider* (then, in case of *Certificate*s belonging to the III. certification class the personal identification will take place another time)
- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate* (see section 1.2.3.); and
  - sent to the *Trust Service Provider*'s `info@e-szigno.hu` email address.

The *Subscriber* and the

Applicant

shall provide their contact information during the *Registration Application*.

4.1.2 Enrolment Process and Responsibilities

During the process of the application the *Trust Service Provider* ascertains the identity of the person submitting the *Certificate Application* (see section 3.2.3).

The *Trust Service Provider* verifies that the *Certificate Application* was really sent by that person whose data (personal ID documents) is in the *Certificate Application* through a different – reliable – communication channel.

In case of *Organizational Certificate* application the *Trust Service Provider* identifies the *Organization* (see section: 3.2.2.) and it ensures, that the *Applicant* is entitled to represent the *Organization* (see section: 3.2.5.) and to request a *Certificate* related to the *Organization* (see section: 3.2.2.).

The *Applicant* shall provide all the necessary information for the conduct of the identification processes.

If it is necessary the *Trust Service Provider* performs data reconciliation with authentic government registers such as the personal data and address register or the company register). In case of a database if it can be arranged, the *Trust Service Provider* performs the data reconciliation electronically.

During the process the *Trust Service Provider* specifies the unique name of the *Subject* and assigns a globally unique ID (OID) to the *Subject*. This happens as defined in section 3.1.

The *Trust Service Provider* registers all the necessary information on the identity of the *Applicant* and the *Organization* for the provision of service and for keeping contact.

The *Trust Service Provider* registers the service agreement signed beforehand by the *Subscriber* that shall contain the *Subscriber*'s statement that the *Subscriber* is aware of its obligations and undertakes the compliance.

The *Trust Service Provider* registers the *Certificate Application* signed by the *Applicant* which shall contain the following:

- a confirmation, that the data provided in the *Certificate Application* are accurate;
- a consent, that the *Trust Service Provider* records and processes the data provided in the application;
- the consent about the disclosure of the *PreCertificate*;
- the declaration whether it consents to the disclosure of the *Certificate*;

The *Trust Service Provider* keeps the aforementioned records for the time period required by law.

The *Trust Service Provider* archives the contracts, the *Certificate Application* form and every attestation that the *Represented Organization*, the *Applicant* or the *Subscriber* handed in.

If the identity of the *Applicant* or in case of an *Organizational Certificate* the identity of the *Organization*

can not be verified without a doubt or any of the indicated data in the *Certificate Application* is incorrect, then the *Trust Service Provider* gives the *Client* the opportunity to correct the missing or incorrect data, and to provide the missing attestations within 3 months from the submission of the *Certificate Application* according to its inner regulations.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The *Trust Service Provider* identifies the *Applicant* according to Section 3.2 ., and it verifies the authenticity of the request.

In case of requesting an *Organizational Certificate*, the *Organization* is going to be identified too, and the verification of the privileges takes place according to section 3.2. The *Trust Service Provider* registers all the information used by the *Subject* or in case of an *Organizational Certificate* the *Organization* to certify its identity, including the registration number of the documentation used for the certification and the incidental limitations related to its validity.

The *Trust Service Provider* may use the original authentic documents in its possession or the authentic electronic copies made of them during the validation until the validity period indicated on the document or until the given document is invalidated in some other way.

The *Trust 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 398 days.

The *Trust Service Provider* maintains a list of the High Risk Certificate Requests which contains the rejected *Certificate Application*s and all the *Certificate*s revoked due to any security issue.

Prior to the *Certificate*'s approval the *Trust Service Provider* checks this list. If any of the requested domain, the *Subscriber* or the *Applicant* is included in the list, the *Trust Service Provider* handles the request with high priority to ensure that such requests are properly verified.

4.2.2 Approval or Rejection of Certificate Applications

To avoid any conflicts of interests, the *Trust Service Provider* ensures its personal and operational independence contrary to the *Subscriber*s. It does not constitute a breach of conflicts of interests, if the *Trust Service Provider* issues *Certificate*s for its associates.

The *Trust Service Provider* verifies the authenticity of all the information given in the *Certificate Application* to be indicated on the *Certificate* before issuing the *Certificate*.

As part of the issuance process, the *Trust Service Provider* checks for a CAA record for each dNSName in the subjectAltName extension of the *Certificate* to be issued, according to the procedure in IETF RFC 8659 [36], following the processing instructions set down in IETF RFC 8659 for any records found.

The *Trust Service Provider* will only issue the requested *Certificate* if the following conditions are independently met for each dNSNames in the subjectAltName extension of the *Certificate* to be issued:

- in case of Wildcard FQDN, the 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"'
- in case of non-Wildcard FQDN, the CAA record
  - does not contain an entry 'issue', or
  - contains the entry 'issue "e-szigno.hu"'

Right before the issuance of the *Certificate* the *Trust Service Provider* checks again the CAA records automatically.

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

If the identity of the natural person or the organization which is to be identified, or in case of a personal *Certificate*, or any of the indicated data on the *Certificate Application* form is incorrect, and is not corrected by the *Client* upon request of the *Trust Service Provider*, then the *Trust Service Provider* rejects the application.

In case of rejection of the *Certificate Application*, the *Trust Service Provider* informs the *Applicant* and the *Subscriber* about the fact of the rejection, but the *Trust Service Provider* is not obliged to justify its decision.

4.2.3 Time to Process Certificate Applications

The *Trust Service Provider* undertakes the processing of the *Certificate Application* within 5 workdays if all the necessary data and document is available.

4.3 Certificate Issuance

In case of certificates belonging to the III. certification class, the *Trust Service Provider* only issues the *Certificate* to the *Subject* in case of the acceptance of the *Certificate Application*.

The issued *Certificate* only contains the data that was indicated in the *Certificate Application* and that was verified by the *Trust Service Provider* during the evaluation process.

In case of *Certificate*s belonging to the II. certification class, the *Trust Service Provider* only issues the *Certificate* to the *Subject* after verifying the data given in the *Registration Application* and receiving the signed *Certificate Application* and service agreement. The issued *Certificate* only contains that *Subject* data , that was given in the *Registration Application*, and that the *Trust Service Provider* verified during the evaluation.

4.3.1 CA Actions During Certificate Issuance

The *Certificate* issuance happens according to strictly regulated and controlled processes, the details are stated by the *Trust Service Provider*'s inner regulations and requirements.

The *Trust Service Provider* has developed its internal administrative processes by analyzing the risks, and applies the principle of "dual control" when recording the data included in the *Certificate* and verifying the authenticity of the data.

The *Trust Service Provider* publishes the *PreCertificate* corresponding to the *Certificate* through the CT Log providers listed on the web page of the *Trust Service Provider*, and puts the digitally signed SCT(s) sent by the CT Log provider(s) into the *Certificate* to be issued.

The issued *PreCertificate* and *Certificate* is added immediately to the internal *Certificate Repository* of the *Trust Service Provider*. From this time it can be suspended and revoked, the revocation status information will be available through the OCSP and CRL services of the *Trust Service Provider*.

The *Trust Service Provider* verifies the issued *Certificate* by using automated tools (certlint, zlint).

- In case of any "ERROR" message the *Trust Service Provider* suspends the publication of the *Certificate* and starts an investigation to analyze the problem
  - the *Trust Service Provider* immediately revokes the really faulty *Certificate* and continues the investigation to find the source of the problem
  - in case of false error message the *Trust Service Provider* continues the publication of the *Certificate* according to the normal process, and upgrades the configuration of the automated tools or informs the developer of the tool about the potential problem
- the *Certificate* which successfully passed the automated test will be published according to the process described in section 4.3.2.

The beginning of the validity period of the *Certificate* shall not be earlier than the real issuance time of the *Certificate*.

The *Trust Service Provider* never backdates *Certificate*s.

4.3.2 Notification of the Subscriber about the Issuance of the Certificate

The Certification Authority informs the *Applicant* and the *Subscriber* on the issuance of the *Certificate* and enables the *Applicant* to receive the *Certificate*.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

In case of *Certificate*s belonging to the III. certification class *Applicant* shall verify the accuracy of the data indicated in the *Certificate* during the takeover of the *Certificate*.

In case of Certificates belonging to the II. certification class, the *Applicant* (or its representative) do not have to separately state the takeover of the issued *Certificate*. By signing the service agreement the *Subscriber* verifies in addition the acceptance of the *Certificate Policy* the *Certification Practice Statement* and other documents containing contractual conditions.

The *Applicant* accepts the *Certificate* by using the *Certificate*, no separate declaration is required.

4.4.2 Publication of the Certificate by the CA

After the issuance of the *Certificate*, in case of the *Applicant*'s prior consent, the *Trust Service Provider* discloses the *Certificate* in its public *Certificate Repository*.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

In case of an Organizational *Certificate* the contact of the *Represented Organization* is notified by the *Trust Service Provider* on the *Certificate* issuance without delay.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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.

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 *Trust Service Provider*, in the course of performing the webserver authentication, the *Relying Party* is recommended to proceed prudentially particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- the public keys belonging to the *Website Authentication Certificate*s shall only be used for website or - if the *Website Authentication Certificate* makes it possible - client authentication;

- the verifications related to the *Certificate* should be carried out for the entire certificate chain up to a trusted root or intermediate provider certificate;
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

The *Trust Service Provider* makes available a service for its *Client*s and *Relying Parties* that they can use to verify the issued *Certificate*s.

4.6 Certificate Renewal

The process when the *Trust Service Provider* issues a new *Certificate* for a new validity period for the same public key with unchanged *Subject* identity information is called *Certificate* renewal.

If the *Subject* would like to use the *Certificate* after the expiration, then it shall initiate the *Certificate* renewal. The *Certificate* renewal technically means the issuance of a new *Certificate*, with the same *Subject* identification data, but new validity period. Other data can change in the *Certificate*, like the CRL, OCSP references or the provider key used for signing the *Certificate*.

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is only permitted when all of the following conditions are met:

- the *Certificate* renewal request was submitted within the validity period of the *Certificate*;
- the *Certificate* to be renewed is not revoked;
- the private key corresponding to the *Certificate* is not compromised;
- the *Subject* identity information indicated in the *Certificate* is still valid.

The *Trust Service Provider* shall only accept a *Certificate* renewal application within the effect of the service agreement.

If a previous *Certificate* of the *Subject* is revoked, then new *Certificate* can only be requested in the frame of *Re-key* (see section: 4.7.) or new *Certificate Application* (see section: 4.1.).

If any of the *Subject* data indicated in the *Certificate* changed, then new *Certificate* shall be requested within the framework of *Certificate* modification (see section 4.8.).

During the *Certificate renewal*, the *Applicant* is informed if the terms and conditions have changed since the previous *Certificate* issuance.

If the *Applicant* is not the same as the *Subscriber*, then the information aforementioned is also provided to the *Subscriber*.

The *Certificate* renewal is performed within the framework of a valid service agreement, there is no need for its modification.

4.6.2 Who May Request Renewal

The *Certificate* renewal shall be initiated by a person behalf of the *Client*, who is entitled to submit an application for a new *Certificate* of the same type at the time of the submission of renewal application.

The applicant shall state in the *Certificate* renewal application, that the *Subject* identification data indicated in the *Certificate* are still valid.

The *Trust Service Provider* provides the following possibilities for the *Client*s to submit *Certificate* renewal application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *Certificate* of the *Applicant*, with a security classification not lower than the requested *Certificate* (see section 1.2.3.) sent to the *Trust Service Provider*'s `info@e-szigno.hu` email address.
- on paper signed manually at the customer service of the *Trust Service Provider* or at the mobile registration associate of the *Trust Service Provider*, on a date previously agreed (then, in case of *Certificate*s belonging to the III. certification class the personal identification will take place that time)
- on paper signed manually and sent to the customer service of the *Trust Service Provider* (then, in case of *Certificate*s belonging to the III. certification class the personal identification will take place another time)

The *Trust 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 *Trust Service Provider* becomes aware that the *Certificate* does not comply with the referred to *Certificate Policy* or *Certification Practice Statement*;
- if the service provider signing key used to issue the *Certificate* shall be replaced out of turn.

4.6.3 Processing Certificate Renewal Requests

During the evaluation of the *Certificate* renewal application, the *Trust Service Provider* verifies that:

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the submitter of the *Certificate* renewal application stated that the data of the *Subject* to be indicated in the *Certificate* are unchanged and accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;

- the *Certificate* to be renewed is not 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 *Trust Service Provider* informs the *Applicant* and the *Subscriber* about the *Certificate* issuance.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

The renewed *Certificate* can be received (downloaded) without personal encounter.

The *Applicant* accepts the *Certificate* by using the *Certificate*, no separate declaration is required.

4.6.6 Publication of the Renewed Certificate by the CA

The *Trust Service Provider* discloses the renewed *Certificate* and the corresponding *PreCertificate* the same way as the original *Certificate*.

4.6.7 Notification of Other Entities about the Certificate Issuance

In case of an *Organizational Certificate* the contact of the *Represented Organization* is notified by the *Trust Service Provider* on the *Certificate* issuance without delay.

4.7 Certificate Re-Key

Re-key means the process when the *Trust Service Provider* issues a new *Certificate* for the *Subject* in a way 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 *Trust Service Provider* shall only accept *Re-key* applications within the scope of the service agreement.

During the *Certificate Re-key*, the *Applicant* is informed by the *Trust Service Provider* if the terms and conditions have changed since the previous *Certificate* issuance. If the *Applicant* is not the same as the *Subscriber*, then the information aforementioned is also given to the *Subscriber*.

Certificate Re-key is performed within the framework of a valid service agreement, there is no need for its modification.

4.7.2 Who May Request Certification of a New Public Key

The *Certificate Re-key* shall be initiated by a person who would be entitled to submit a new *Certificate Application* at the time of the submission of the *Re-key* application.

The applicant shall state in the *Certificate Re-key* application, that the *Subject* identification data indicated in the *Certificate* are still valid, or they shall give the new data and make a statement of its validity.

The *Trust Service Provider* ensures the following possibilities for the *Client*s to submit *Certificate* re-key application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *Certificate* of the *Applicant*, with a security classification not lower than the requested *Certificate* (see section 1.2.3.) sent to the *Trust Service Provider*'s `info@e-szigno.hu` email address.
- on paper signed manually at the customer service of the *Trust Service Provider* or at the mobile registration associate of the *Trust Service Provider*, on a date previously agreed (then, in case of *Certificate*s 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 *Trust Service Provider* (then, in case of *Certificate*s belonging to the III. certification class the personal identification will take place another time).

4.7.3 Processing Certificate Re-Key Requests

During the evaluation of the *Certificate Re-key* application the *Trust Service Provider* verifies that:

- the submitted application is authentic;
- the submitter of the application has the appropriate entitlement and authorization;
- the data indicated in the application are accurate;
- based on the currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity of the *Certificate* to be issued.

Before processing the *Re-key* request the identity of the person submitting the Certificate *Re-key* application shall be verified according to section 3.3.

4.7.4 Notification of the Client about the New Certificate Issuance

The *Trust Service Provider* informs the *Applicant* and the *Subscriber* about the *Certificate* issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The *Trust Service Provider* hands over the *Certificate* issued for the new public key after the identification of the *Applicant*.

4.7.6 Publication of the Re-Keyed Certificate

The *Trust Service Provider* discloses the renewed *Certificate* and the corresponding *PreCertificate* the same way as the original *Certificate*.

4.7.7 Notification of Other Entities about the Certificate Issuance

In case of an *Organizational Certificate* the contact of the *Represented Organization* is notified by the *Trust Service Provider* on the *Certificate* issuance without delay.

4.8 Certificate Modification

Certificate modification means the process when the *Trust Service Provider* issues a new *Certificate* for the *Subject* with changed *Subject* identity information but with unchanged public key.

The *Certificate* modification technically means new *Certificate* issuance. The *Trust Service Provider* is bound to revoke the previous *Certificate*, that contains invalid data (see section: 4.9.).

Previous data can change in the new *Certificate* issued during the *Certificate* modification, such as the validity period, the CRL and OCSP references or the *Trust Service Provider* key used for *Certificate* signing.

4.8.1 Circumstances for Certificate Modification

Certificate modification becomes necessary in the following cases:

- change of data indicated in the *Subject*'s *Certificate*;
- in the *Certificate* issuing system of the *Trust 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 *Trust 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 revoked;
- the private key corresponding to the *Certificate* is not compromised.

The *Trust Service Provider* only accepts *Certificate* modification application in the scope of the Service Agreement.

If the previous *Certificate* of the *Subject* is revoked or expired, then the new *Certificate* can be requested within the framework of *Re-key* (see section: 4.7.) or new *Certificate Application* (see section: 4.1.).

During the *Certificate* modification, the *Applicant* is informed if the terms and conditions have changed since the previous *Certificate* issuance.

If the *Applicant* is not the same as the *Subscriber*, then the information aforementioned is also given to the *Subscriber*. The *Certificate* modification is performed within the framework of a valid service agreement, there is no need for its modification.

4.8.2 Who May Request Certificate Modification

The *Certificate* modification shall be initiated by a person who is entitled to submit a new *Certificate Application* at the time of the submission of the modification application.

In the *Certificate* modification request, the applicant shall give the new data and shall make a statement of their accuracy.

The *Trust Service Provider* initiates the *Certificate* modification if it becomes aware of that the *Subject*'s data indicated in the *Certificate* is changed.

The *Trust Service Provider* ensures the following possibilities for the *Client*s to submit *Certificate* modification application:

- in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *Certificate* of the *Applicant*, with a security classification not lower than the requested *Certificate* (see section 1.2.3.)
  - sent to the *Trust Service Provider*'s `info@e-szigno.hu` email address, or
  - submitted on the *Applicant*'s *Customer Portal*.
- on paper signed manually at the customer service of the *Trust Service Provider* or at the mobile registration associate of the *Trust Service Provider*, on a date previously agreed (then, in case of *Certificate*s 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 *Trust Service Provider* (in this case, in case of *Certificate*s belonging to the III. certification class, the personal identification will take place another time).

4.8.3 Processing Certificate Modification Requests

During the evaluation of the submitted *Certificate* modification application, the *Trust Service Provider* verifies that:

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the data given in the application are accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;
- based on the currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the *Certificate* to be issued.

The *Trust Service Provider* verifying the validity of the *Subject*'s data proceeds the same as the initial verification performed before a new *Certificate* issuance.

Before the execution of the Certificate modification application, the applicant shall be identified according to section 3.5.

4.8.4 Notification of the Client about the New Certificate Issuance

The *Trust Service Provider* informs the *Applicant* and the *Subscriber* about the *Certificate* issuance.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

During *Certificate* modification, there is no new key generation, thus there is no need to handover key to the *Subject*. The modified *Certificate* can be received (downloadable) without personal encounter.

The *Subject* accepts the *Certificate* by its usage, and there is no need for further statement.

4.8.6 Publication of the Modified Certificate by the CA

The *Trust Service Provider* discloses the renewed *Certificate* and the corresponding *PreCertificate* the same way as the original *Certificate*.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

In case of an *Organizational Certificate* the *Organizational Administrator* of the *Represented Organization* is notified by the *Trust Service Provider* on the *Certificate* issuance without delay.

4.9 Certificate Revocation and Suspension

The process when the *Trust 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.

The *Website Authentication Certificate* shall not be suspended.

Revocation Reason

The *Trust Service Provider* may store information on the reason for the revocation in the *Certificate* revocation status register, which it may disclose in the *Certificate* revocation status services.

When the *Client* initiates the revocation, the following revocation reasons may be given:

- key compromise (keyCompromise (1))
- the *Certificate* is no longer needed (cessationOfOperation (5))
- right of use has been terminated (privilegeWithdrawn (9))

The options available in each revocation service are described in the description of the specific service.
When the *Trust Service Provider* initiates the revocation, the following revocation reasons may be given:

- unspecified (unspecified (0), which results in no reasonCode extension being provided)
- key compromise (keyCompromise (1))
- *Certificate* modification (affiliationChanged (3))
- *Certificate* renewal (superseded (4))
- right of use has been terminated (privilegeWithdrawn (9))

Using the Private Key of a Revoked Certificate

The use of the private key belonging to the revoked *Certificate* shall be eliminated immediately.
If possible, the private key belonging to the revoked *Certificate* shall be destroyed immediately after revocation.
Responsibility regulations related to revocation:

- If the *Trust Service Provider* has already published the revoked status of the *Certificate*, the *Trust Service Provider* does not take any responsibility, if the *Relying Party* considers the *Certificate* valid.

4.9.1 Circumstances for Revocation

Reasons for Revoking a Subscriber Certificate

Certification Authority revokes the end-user *Certificate* and uses the corresponding CRLreason in the following cases:

- a fully compliant revocation request is submitted to the *Trust Service Provider* using the web-based revocation service operated by it

  (see in section 4.9.3)

- a fully compliant revocation request is submitted to the *Trust Service Provider* using the SMS-based revocation service operated by it

  (see in section 4.9.3)

- the *Applicant* or the *Subscriber* requests the revocation of the *Certificate* in writing

  (see in section 4.9.3)

- the *Applicant* or the *Subscriber* notifies *Certification Authority* that the *Certificate Application* is not approved and subsequently the approval is not given

  (privilegeWithdrawn (9))

- the *Certification Authority* becomes aware that the private key corresponding to the public key in the *Certificate* has been compromised

  (keyCompromise (1))

- the *Certification Authority* obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the *Certificate* should not be relied upon

  (superseded (4))

- 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 *Trust 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))

- the *Certification Authority* becomes aware that the usage of the Fully Qualified Domain Name or IP address indicated in the *Certificate* is no longer legally permitted (e.g court withdrew the right to use the domain, or the owner does not renew the domain registration)

  (cessationOfOperation (5))

- the *Certification Authority* becomes aware that the wildcard certificate was used for deceptive domain name authentication

  (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 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 *Certificate*s, and maintenance is not provided for the existing CRL and OCSP services

  (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)

- 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))

- the *Certification Authority* is made aware of a demonstrated or proven method that exposes the *Subscriber*'s private key to compromise, or if there is clear evidence that the specific method used to generate the private key was flawed

  (keyCompromise (1))

- the *Certification Authority* issued the *Certificate* based on a document from a third party, and it withdraws that document in writing

  (privilegeWithdrawn (9))

- the format and technical content of the *Certificate* presents an unacceptable risk to the *Relying Parties* (for example, if the used cryptographic algorithm or key size is no longer secure)

  (keyCompromise (1))

- the *Certification Authority* becomes aware that the private key of the *Certificate* issuer certification unit might be compromised

  (unspecified (0), ami eredményeként nem lesz reasonCode a visszavonási állapotban)

- the *Certification Authority* becomes aware that the *Subscriber* failed to fulfil any of its financial obligations according to the service agreement

  (privilegeWithdrawn (9))

- the termination of service agreement

  (privilegeWithdrawn (9))

- the *Certification Authority* has terminated its activities

  (unspecified (0), ami eredményeként nem lesz reasonCode a visszavonási állapotban)

- the supervisory body enacts (smth.) in a legally binding and executable decision

  (unspecified (0), ami eredményeként nem lesz reasonCode a visszavonási állapotban)

- the law makes revocation mandatory

  (unspecified (0), ami eredményeként nem lesz reasonCode a visszavonási állapotban)

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 intermediate certification unit requests the revocation of the *Certificate* in writing
- the Subordinate CA notifies the *Trust 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 *Certificate*s, and maintenance is not provided for the CRL and OCSP services related to the *Certificate*s
- 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

Reasons for Revoking a Subordinate CA Certificate Operated by Another CA

Certification Authority is bound to take action on the revocation of the *Certificate* of the intermediate certification unit operated by other *Certification Authority* in the following cases:

- the CA operating the intermediate certification unit requests the revocation of the *Certificate* in writing
- the Subordinate CA notifies the *Trust Service Provider* that the original *Certificate Application* was not authorized and does not retroactively grant authorization
- the issuer *Certification Authority* becomes aware that the operator of the intermediate certification unit is not in the exclusive possession of the private key
- the issuer *Certification Authority* becomes aware that the public key in the *Certificate* does not anymore 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 issuer *Certification Authority* becomes aware that the *Certificate* is not issued according to the related *Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit operator 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*
- the *Certification Authority* is no longer entitled to issue *Certificate*s, and maintenance of the CRL and OCSP services for the existing *Certificate*s is not provided
- 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 the other *Certification Authority*
- if *Certification Authority* issued the *Certificate* based on a document from a third party, and that third party withdraws the document in writing
- the format and technical content of the *Certificate* presents an unacceptable risk to the Relying parties (for example, if the used cryptographic algorithm and key size is no longer safe)
- the *Certification Authority* operating the certification unit or the issuer *Certification Authority* of its *Certificate* has terminated its activities
- the law makes the revocation mandatory

4.9.2 Who Can Request Revocation

The revocation of the *Certificate* may be requested by anyone using the following services operated by the *Trust Service Provider*, who knows the secret revocation password and the requested identification data.

- web-based revocation service
- SMS-based revocation service

The revocation of the *Certificate* may be requested in writing by the *Client*s, namely:

- the *Subscriber*;
- the *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*;

and

- the *Trust Service Provider*.

Additionally, *Subscriber*s, *Relying Parties*, Application Software Suppliers, and other third parties may submit High Risk Certificate Problem Reports informing the *Trust Service Provider* of reasonable cause to revoke the *Certificate*, like fraud, misuse or key compromise.

The *Trust Service Provider* provides clear instructions on how to report suspected Private Key Compromise, *Certificate* misuse, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to *Certificate*s on the following website:

`https://e-szigno.hu/en/report-certification-security-events.html`

and in section 1.5.2 of the present *Certification Practice Statement*.

4.9.3 Procedure for Revocation Request

The *Trust Service Provider* ensures the following possibilities to submit a revocation request:

- **Through the Website of the *Trust Service Provider* 24 Hours a Day**

  The revocation request can be submitted through the following website of the *Trust Service Provider*:

  `https://e-szigno.hu/revocation`

  When suspending via the website of the *Trust Service Provider* the *Client* needs to provide the following information:

- the suspension password as a data certifying the authenticity of the revocation request,
- the last three parts of the *Subject* OID in the *Certificate* (e.g. 2.2.123), or in case of natural person *Subject* instead of the OID the date of birth of the *Subject*.

Revocation requests submitted via the website of the *Trust Service Provider* are processed without delay by the information system of the *Trust Service Provider* and it immediately notifies the applicant about the result on its website.

In case of a successful revocation, the changed revocation status appears in the internal *Revocation Status Registry* of the *Trust Service Provider* immediately. The inner processes of the *Trust Service Provider* ensure that the processing ends within at most 5 minutes from the provision of data, so the changed revocation state is updated from the receipt of the request within maximum that interval.

When a request submitted via the *Trust Service Provider* website, the revocation reason is always:

- key compromise (keyCompromise (1))

The *Trust Service Provider* logs every suspension request. In case of a successful suspension, the *Trust Service Provider* notifies the *Subject* and the Subscriber about the fact of the suspension by email.

The *Trust Service Provider* guarantees availability of suspension service only for suspension requests received from SMS text. If the webpage of the *Trust Service Provider* is not available, the *Trust Service Provider* recommends the *Client* to request suspension by sending SMS.

- **By Sending a Fixed-format SMS Text Message 24 Hours a Day**

The *Client*s of the *Trust Service Provider* may indicate in an SMS text message sent to the *Trust Service Provider*'s revocation phone number if a private key is possessed by an unauthorized person.

The *Trust Service Provider* immediately begins the processing of the revocation requests arriving in text messages. The *Trust Service Provider*'s system sends an automatically generated reply message to the phone number of the requester about the result of processing and the success of the revocation.

In the request sent in the text message the following data shall be provided separated by a space character:

- date of birth of the *Subject* in the "YYYY-MM-DD" format, or the last three digits of the OID as indicated in the *Certificate*,
- the revocation password of the *Certificate*.

Example of formally correct revocation request:

- "2.1.134 pacsirta"

When a request submitted via SMS text message, the revocation reason is always:

– key compromise (keyCompromise (1))

The *Trust Service Provider* always declines the revocation request arriving in a text message from a hidden phone number regardless of the content of the message.

In order to ensure the availability of the revocation service, the *Trust Service Provider* also maintains telephone numbers operated by two different mobile service providers. If sending an SMS to one phone number fails (no confirmation is received within a few minutes), please try sending the message to the other phone number.

Phone numbers to receive revocation SMS:

"+36 (20) 263-4943"

"+36 (30) 326-2187"

- **By Using *Customer Portal***

  A revocation request can be submitted 24 hours a day using the *Customer Portal* operated by the *Trust Service Provider*.

  Access address of the *Customer Portal*:

  `https://portal.e-szigno.hu/login`

  On the *Customer Portal* interface, the *Client* shall select the *Certificate*s to be revoked and then select the reason for revocation from the list below:

  – key compromise (keyCompromise (1))
  – cessation of operation (cessationOfOperation (5))
  – privilege withdrawn (privilegeWithdrawn (9))

  Following options are available for authentication of the revocation request to be submitted:

  – **Electronic Signature or Electronic Seal**

    By creating an electronic signature or electronic seal based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate* (see section 1.2.3.) of the *Applicant* on the *Customer Portal* interface.
    The submitted revocation requests are processed by the *Trust Service Provider* during working hours as described in chapter 4.9.5.
    Using this method, a large number of *Certificate*s can be revoked in one application.

  – **Entering the Suspension Password**

    the *Client* shall enter the suspension password for the *Certificate* to be revoked on the *Customer Portal* interface.
    Revocation requests submitted this way are processed without delay by the information system of the *Trust Service Provider* and it immediately notifies the applicant about the result on its website.
    By using this method, those *Certificate*s can be revoked in one request that have the same suspension password.

- **Sent by Email, with an Electronic Signature or Electronic Seal**

  in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate* (see section 1.2.3.) sent to the *Trust 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))
  - right of use has been terminated (privilegeWithdrawn (9))

- **On Paper, Signed Manually**

  The paper-based, manually signed application can be submitted in person at the *Trust Service Provider*'s Customer Service during service hours, or sent by post to the *Trust Service Provider*'s Customer Service address as defined in chapter 1.3.1. In the submitted application, the applicant must select the revocation reason from the list below:

  - key compromise (keyCompromise (1))
  - the *Certificate* is no longer needed (cessationOfOperation (5))
  - right of use has been terminated (privilegeWithdrawn (9))

In case of a Revocation request submitted in writing the *Trust Service Provider* verifies the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

In case of Revocation request signed with a valid electronic signature, there is no need for further verification of the identity of the applicant and the authenticity of the request.

In case of submitting revocation request on paper, via mail the *Trust Service Provider* verifies the manual signature on the request.

If the revocation was requested by the *Client*, and it does not state the reason for revocation, then the *Trust Service Provider* considers that the reason for revocation is that the *Subject* does not want to use the *Certificate* anymore (cessationOfOperation (5)).

If the *Client* request the revocation due to key compromise, the *Trust Service Provider* ensures a possibility during the revocation process, to request a new *Certificate* in the framework of *Re-key* to replace the *Certificate* to be revoked. The rules for *Re-key* are in section 4.7.

When the revocation is requested in writing, the *Trust Service Provider* makes possible to ask the revocation in advance for a later date by giving the requested date of the revocation.

The revocation request shall contain the data to identify the *Certificate*.

The requester shall provide particularly the following information:

- the exact denomination of the *Subject*;
- the *Certificate*'s unique identifier;

- the requested date of the revocation, if the revocation shall not happen immediately;
- identification data of the *Client*.

In case of invalid or incomplete revocation request the *Trust Service Provider* rejects the request. The *Trust 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 *Trust Service Provider* makes a decision about the acceptence of the request. Depending on the content of the request the *Trust Service Provider* revokes the *Certificate* immediately or sets up the date of revocation according to the request.

In case of a successful revocation the *Trust Service Provider* notifies the *Subject* and the *Subscriber* about the revocation by email.

Further information about the suspension and revocation can be found on the home page of the *Trust Service Provider* on the following link:

`https://e-szigno.hu/en/certificate-suspension-and-revocation.html`

High-Priority Certificate Problem Report

The *Trust Service Provider* maintains a continuous 24x7 ability to respond internally to a High Priority Certificate Problem Report.

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

The *Trust Service Provider* begins investigating the Certificate Problem Report within 24 hours after receiving and decides whether revocation is appropriate based on the following criteria:

- the nature of the alleged problem,
- the consequences of revocation,
- the number of Certificate Problem Reports received about a particular *Certificate* or *Subscriber*,
- the entity making the complaint, and
- relevant legislation.

The *Trust Service Provider* provides a preliminary report on its findings to both the *Subscriber* and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the *Trust Service Provider* works with the *Subscriber* and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the *Certificate* will be revoked, and if so, a date which the *Trust Service Provider* will revoke the *Certificate*.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frame set forth in Section 4.9.5.

If necessary, the *Trust Service Provider* informs the National Media and Infocommunications Authority about the reported problem.

4.9.4 Revocation Request Grace Period

The *Trust 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 *Trust Service Provider* processes the following revocation requests immediately 24 hours a day:

- revocation requests issued through the website of the *Trust Service Provider*
- revocation requests issued by sending a fixed-format SMS text message

The *Trust Service Provider* processes the revocation requests issued by any other way within 24 hours following the official arrival time of the request.

The *Trust Service Provider* determines the date of receipt of the revocation request in the following way:

- In case of revocation requests sent by electronic mail to the dedicated email address `revocation@e-szigno.hu` during office hours of the Customer Service, the official time of arrival is when the email is received on the server of the *Trust Service Provider*.
- In the case of a request submitted in *Customer Portal* during the opening hours of the Customer Service, the official time of receipt is the actual time of the request submission, recorded by the server.

  Requests submitted outside of Customer Service opening hours are considered received at the beginning of the next Customer Service opening hours.
- In case of applications submitted in person, the time of arrival is when the customer service officier of the *Trust Service Provider* receives the application.
- In case of applications sent by post, the time of arrival is when the mail arrives to the *Trust Service Provider* at office hours.

The *Trust Service Provider* undertakes to meet these requirements only for revocation requests sent to the indicated addresses stated in section 1.3.1. In case of revocation request sent to other addresses – specially directly sent to specific associate of the *Trust Service Provider* – or via other channels, the *Trust Service Provider* does not offer any availability.

The *Trust Service Provider* begins investigation of the *Website Authentication Certificate* related reported problems and makes decision about further steps within 24 hours.

The *Trust Service Provider* provides a preliminary report on its findings to both the *Subscriber* and the entity who filed the Certificate Problem Report.

The *Trust Service Provider* revokes the *Website Authentication Certificate*s within 24 hours after the conditions defined in section 4.9.1 are met.

The *Trust Service Provider* revokes the *Website Authentication Certificate* issuer intermediate certification units' *Certificate*s 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 *Trust 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 *Certificate*s located in the *Certificate* chain according to the relevant technical standards. The verification should cover the verification of the *Certificate*s' 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

The *Trust Service Provider* issues a new *Certificate Revocation List* for its end user *Certificate*s at least once a day. The validity of these *Certificate Revocation List*s is 25 hours.

The *Trust Service Provider* issues a new *Certificate Revocation List* for its intermediate certification units every day at the same time. The validity of the *Certificate Revocation List*s is 25 hours.

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation/Status Checking Availability

The *Trust Service Provider* provides online *Certificate* status (OCSP) service.

4.9.10 Online Revocation Checking Requirements

The online *Certificate* status service complies with the requirements of Section 4.10 .

Certification Authority provides OCSP service through GET method.

4.9.11 Other Forms of Revocation Advertisements Available

The *Trust Service Provider* makes available in its public *Certificate* Repository – with their status – the revoked *Certificate*s. Thus by searching in the *Certificate* Repository the *Client*s and the *Relying Parties* can personally (without the help of an application) verify the revocation status of a *Certificate*.

4.9.12 Special Requirements for Key Compromise

Any interested party may submit a key compromise report to the *Certification Authority* if it becomes aware that the private key of any *Certificate* issued by the *Certification Authority* has been compromised.

The fastest way to report is on the following website:

`https://e-szigno.hu/en/report-certification-security-events.html`

At the time of report, the reporter must prove that the private key has indeed been compromised. The report must specify:

- the compromised private key itself, or
- the PKCS#10 certificate request signed by the compromised private key and containing the following text in the "CN" field: "Proof of Key Compromise".

In case of any certification unit's private key is compromised, the *Trust Service Provider* makes every reasonable effort in order to notify the *Relying Parties* about the incident. It publishes any status change on the provider *Certificate*s on its webpage.

In case of compromised *Certificate*s issued by the *Trust Service Provider*, the *Trust Service Provider* is able to revoke the end-user *Certificate* belonging to the compromised private key. The revocation reason information (reasonCode) in this case is set to keyCompromise (1) value.

4.9.13 Circumstances for Suspension

The validity of the *Website Authentication Certificate*s shall not be suspended.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

The *Trust Service Provider* provides the following possibilities for the *Certificate* revocation status query:

- OCSP – online *Certificate* revocation status query service,
- CRL – *Certificate Revocation List*s.

The *Trust Service Provider* maintains an internal *Revocation Status Registry*, which contains the current revocation status information of all the *Certificate*s issued by the *Trust Service Provider*, including the valid, revoked and suspended statuses.

In case of revocation the new status of the *Certificate* – see section: 4.9. – appeares immediately in the revocation records of *Trust Service Provider* after the successful completion of the process.

The *Revocation Status Registry* contains also the revocation status information of the expired *Certificate*s, which will be available till the expiry date of the issuing CA.

The *Trust Service Provider* generates the *Certificate Revocation List* based on the actual information received from the *Revocation Status Registry*, so any change in the revocation statuses will be published in the first *Certificate Revocation List* issued after the given change.

The OCSP responses issued by the OCSP responders of the *Trust Service Provider* are always based on the revocation status information received from the *Revocation Status Registry* at the time which is indicated in the OCSP response.

OCSP response issued by the *Trust Service Provider* may contain "good" status information only for the *Certificate*s that were issued by the given certification unit and are stored in the *Trust Service Provider*'s *Certificate Repository* (positive OCSP).

4.10.1 Operational Characteristics

Each certification unit of the *Trust Service Provider* issues *Certificate Revocation List* with the frequency below:

- Each root certification unit of the *Trust Service Provider* issues a CRL once in at the most of 24 hours.
- The productive (subordinate) certification units operated within the system of the *Trust Service Provider* issue CRL within 60 minutes after the revocation status change of any *Certificate* issued by the given certification unit, but at least once in every 24 hours.

The validity period of the *Certificate Revocation List* is 25 hours.

The all-time current *Certificate Revocation List*s for the specific *Certificate*s can be reached at the following address:

`https://e-szigno.hu/en/pki-services/ca-certificates.html`

The effective date of the *Certificate Revocation List*s ("thisUpdate") marks also the time when the certification unit assembled and started signing the *Certificate Revocation List*. After that, in case of long *Certificate Revocation List*s the publication of the *Certificate Revocation List* may even take 1 or 2 minutes. The appearance of the next *Certificate Revocation List* ("nextUpdate") marks the latest next time, from what the list is publicly available. Accordingly, the time interval between the date of the *Certificate Revocation List* entering into force, and the date of publication of the next *Certificate Revocation List* can be longer than the time intervals above, but this does not affect the time interval between the appearance of the CRLs is at most 24 hours.

Regarding, that amongst the provided services, the validity of the *Certificate* can be determined the fastest and the easiest with OCSP, the *Certification Authority* recommends the use of OCSP to its *Client*s.

Online Certificate Status Protocol (OCSP)

The *Trust Service Provider* publishes the revocation status of the *Certificate*s with the OCSP service too.

The *Trust Service Provider* provides OCSP service according to the IETF RFC 6960 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the *Certificate*s issued by the certification unit (section 1.3.1.).

The main characteristics of the OCSP service:

- The OCSP service is publicly and freely available, any *Relying Party* can avail itself of it same as the *Certificate Revocation List*s. There is no need for authentication at query.
- The OCSP service can be reached through the URLs indicated on the *Certificate*s on the default HTTP port (port 80).
- The OCSP service fulfils the requirement of the IETF RFC 5019 [29] to support the large scale PKI environments which require a ligthweigth solution to minimize communication bandwidth and clientside processing.
- Based on the IETF RFC 6960 "Response Pre-production" process, the issued OCSP response can be created before the query and does not necessarily contain the nonce element. The *Trust Service Provider* can give the same response for multiple queries. The "thisUpdate" and "producedAt" time values are identical, but these can precede the time of the query.
- The "nextUpdate" indicated in the response is always filled, and contains a time value not later than the responder certification expiration time.
- The "thisUpdate" value indicated in the issued OCSP response is never older than 24 hours, because the *Trust Service Provider* creates a new OCSP response at least in every 24 hours.
- The time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never smaller than 8 hours.
- The time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never greater than 10 days.
- the value in the "nextUpdate" field shall be before or equal to the "notAfter" value of all certificates included within the "BasicOCSPResponse.certs" field or, if the certs field is omitted, before or equal to the "notAfter" value of the CA certificate which issued the certificate that the "BasicOCSPResponse" is for.
- The OCSP responses always contain the current information listed in the revocation registry of the *Trust Service Provider* at the "thisUpdate" time of the OCSP response, but if the "thisUpdate" time of the OCSP response is earlier than the time for which the verification is carried out – which is either earlier or coincides with the time of the query –, then the OCSP response is not clear evidence for a third party regarding the revocation status of the *Certificate*.

4.10.2 Service Availability

The *Trust Service Provider* ensures that the availability of the *Certificate Repository* and the terms and conditions pertaining to the *Certificate*s issued by the *Trust Service Provider* is at least 99% per year, and the length of downtime shall not exceed at most 24 hours.

The *Trust Service Provider* ensures that the availability of the revocation status information and the revocation management service is at least at least 99% per year, and the length of downtimes shall not exceed at most 24 hours on any occasion.

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

4.10.3 Optional Features

The *Trust Service Provider* provides various (CRL and two types of OCSP) services according to the descriptions in this section, in the framework of *Client*s and *Relying Parties* can verify the revocation status of the *Certificate*s issued by the *Trust Service Provider*. Besides these, the *Trust Service Provider* makes available in its public *Certificate Repository* – with their status indicated – the revoked *Certificate*s, so while searching in the *Certificate Repository* the *Client*s and *Relying Parties* can (without the help of an application) verify the revocation status of the *Certificate*.

4.11 End of Subscription

The *Trust Service Provider* revokes the end-user *Certificate*s in case of the termination of the contract concluded with the *Subscriber*.

4.12 Key Escrow and Recovery

The *Trust Service Provider* does not provide key escrow service for a private key belonging to a *Website Authentication Certificate*.

4.12.1 Key Escrow and Recovery Policy and Practices

The private key belonging to the *Website Authentication Certificate* shall not be escrowed.

4.12.2 Symmetric Encryption Key Encapsulation and Recovery Policy and Practices

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.

5 Facility, Management, and Operational Controls

The *Trust Service Provider* applies physical, procedural, and personnel security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.

The *Trust Service Provider* keeps a record of the system units and resources related to the service provision, and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.

The *Trust Service Provider* monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The *Trust Service Provider* takes care that physical access to critical services is controlled, and keeps physical risk of the assets related to critical services at a minimum.

The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the *Trust Service Provider*'s information, and physical zones.

Services that process critical and sensitive information are implemented at secure locations in the system of the *Trust Service Provider*.

The provided protection is proportional to the identified threats of the risk analysis that the *Trust Service Provider* has performed.

In order to provide adequate security:

- The *Trust Service Provider* implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.

- The Customer Service office of the *Trust Service Provider* was designed, to be able to meet the requirements for registration services under realistic costs.

- The *Trust Service Provider* constructed its mobile registration units, so that they comply with the requirements imposed on the registration service.

- The *Trust Service Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

5.1.1 Site Location and Construction

The IT system of the *Trust Service Provider* is located and operated within a properly secured *Data Centre* with physical and logical protection that prevents illegitimate access. Defensive solutions – as for example guarding, security locks, intrusion detection systems, video surveillance system, access control system – are applied over the course of locating and establishing the *Data Centre* that are built on each other and interdependent and together they provide a powerful protection system for the IT systems participating in service provision, and for the preservation of the confidential data stored by the provider.

5.1.2 Physical Access

The *Trust Service Provider* protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.

Trust Service Provider ensures that:

- each entry to the *Data Centre* is registered;

- only authorized staff members with trusted roles with the right permissions can entry to the computer room individually;

- persons without independent authorization can only stay in the *Data Centre* in justified cases, for the time required and accompanied by personnel with appropriate rights;
- the entry logs shall be archived continuously and evaluated weekly.

The activation data (passwords, PIN codes) of the devices shall not be stored openly even in the *Data Centre*.
In the presence of unauthorized persons:

- data media containing sensitive information are physically out of reach;
- the logged-in terminals are not left without supervision;
- no work process is carried out during which confidential information may be revealed.

When leaving the computer room the administrator shall verify that:

- every equipment of the *Data Centre* is in an adequately secure operation state;
- there's no terminal left logged-in;
- physical storage devices are locked properly;
- systems, devices providing physical protection operate properly;
- the alarm system has been activated.

There are appointed responsible people to carry out regular physical security assessments. The results of the examinations are recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The *Trust Service Provider* applies an uninterruptible power supply unit in the *Data Centre* that:

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems;
- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other;
- in case of lasting power outage has its own power generation equipment, which – by allowing refueling – is able to provide the necessary energy for any period of time.

The air of the outer environment shall not get into the *Data Centre* directly. The *Data Centre* air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.
The humidity is reduced to the level required by the IT systems.
The *Trust Service Provider* uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4 Water Exposures

The *Data Centre* of the *Trust Service Provider* is adequately protected from water intrusion and flooding. The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it.

In the protected computer room security is further increased by the use of a raised floor.

5.1.5 Fire Prevention and Protection

In the *Data Centre* of the *Trust Service Provider*, a fire protection system approved by the competent fire headquarters operates.

There is the type and quantity of manual fire extinguishers in accordance with the relevant regulations at clearly visible locations in each room.

5.1.6 Media Storage

The *Trust Service Provider* protects its media storages from unauthorized access and accidental damage. All audit and archive data is created in duplicate. The two copies are stored physically separated from each other in fireproof safes, at locations in a safe distance from each other in the operator room of the data centre used for the trust services.

The stored media storages are protected from damaging environmental influences such as low or high temperatures, dirt, moisture, sunlight, strong magnetic fields, strong radiation.

5.1.7 Waste Disposal

The *Trust Service Provider* ensures the environmental standards compliant disposal of the superfluous assets, and media.

The *Trust Service Provider* does not use the electronic storage media containing information classified as confidential even for storing data classified as not confidential after deleting their content and devices like that shall not be taken outside of the premises of the *Trust Service Provider*. The *Trust Service Provider* physically destroys – according to the rules of disposal – the defective for any other reason unusable, redundant media storages containing confidential classified information:

- chops paper documents up in a shredder machine;
- disassembles the hard drives and smashes the critical components;
- destroys the optical disc with a suitable shredder machine.

5.1.8 Off-Site Backup

The *Trust Service Provider* creates a backup weekly from which the whole service could be restored in case of a fatal error. The backups – at least including the last full backup – are stored at an external location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the backup locations is resolved.

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

5.2 Procedural Controls

The *Trust Service Provider* takes care that its systems are operated securely, according to the rules, and with a minimal risk of defects.

Procedural precautions have the objective of supplementing, and at the same time intensifying the effectiveness of physical safeguards, along with those applicable to personnel, by means of appointing and isolating trusted roles, documenting the responsibilities of various roles, as well as specifying the personnel headcounts and exclusion roles necessary for the various tasks, moreover identification and authentication expected in the various roles.

The *Trust Service Provider*'s internal governance system ensures that its operation complies with legal, as well as its internal regulations. In its system a responsible person shall be clearly assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the *Trust Service Provider*'s system. The auditing activity of the independent system auditor and the *Trust Service Provider*'s internal auditor ensures the system's appropriate operation.

5.2.1 Trusted Roles

The *Trust Service Provider* creates trusted roles (in the wording of the regulation, scope of activities) according to the requirements of decree 24/2016. [9] for the performance of its tasks. The rights and functions are be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

The *Trust Service Provider* defines the following trusted roles, with the following responsibilities:

Manager with overall responsibility for the IT system of the *Trust Service Provider*
: The individual responsible for the IT system.

Security officer
: Senior security associate, the individual with overall responsibility for the security of the service.

System administrator
: Infrastructure administrator. The individual with the task to install, configure and maintain the systems of the *Trust Service Provider*. Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring the development of technology, and for the detection and proposing of development solutions of the vulnerabilities of each system component.

Operator
: System operator, individual performing the IT system's continuous operation, backup and restore.

Independent system auditor
: Individual who audits the logged, as well as archived dataset of the *Trust Service Provider*, responsible for verifying the enforcement of control measures the service provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.

Registration officer

Individual responsible for the approval of production, issuance, revocation of end-user certificates.

For the provision of trusted roles the manager responsible for the security of the *Trust Service Provider* formally appoints the *Trust Service Provider*'s employees.

Only those persons may hold a trusted role who are in employment relationship with the *Trust Service Provider*. Trusted roles shall not be hold in the context of a commission contract.

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

5.2.2 Number of Persons Required per Task

The security and operational regulations of the *Trust Service Provider* define that the following tasks can be only performed in protected environment, with the contemporaneous presence of two employees holding trusted roles:

- the generation of the *Trust 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 *Trust Service Provider* have unique identification data, enabling secure identification and authentication of the users.

The users can only access the IT systems critical from the aspect of the provision of the certification service after identification and authentication.

The identification and authentication data are revoked without delay in case of the cessation of user rights.

Every user of the IT system and every actor in the administrative process is identified individually.

For the verification of the physical access, the *Trust Service Provider* uses an RFID card based access control system, and for the logical access control, it uses VPN Certificates issued on a Secure Signature-Creation Device. Before successful authorization, not even a single security-critical task can be performed. Every employee of the *Trust Service Provider* has exactly as many access rights, as it is absolutely necessary for the assigned role.

5.2.4 Roles Requiring Separation of Duties

Employees of the *Trust Service Provider* can hold multiple trusted roles at the same time, but the *Trust Service Provider* ensures that:

- the security officer and the registration officer shall not hold the independent system auditor role;
- the system administrator shall not hold the security officer and the independent system auditor role;
- the manager with overall responsibility for the IT system shall not hold the security officer and the independent system auditor role.

In addition to the aforementioned, the *Trust Service Provider* seeks the complete separation of trusted roles.

5.3 Personnel Controls

The *Trust Service Provider* takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the *Trust 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 *Trust Service Provider* addresses personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties – who get in contact with the *Trust Service Provider*'s services – shall sign a non-disclosure agreement.

At the same time, the *Trust Service Provider* ensures for its employees obtaining as well as further developing of common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

5.3.1 Qualifications, Experience, and Clearance Requirements

As a hiring requirement, the *Trust Service Provider* requires at least intermediate education degree, but the *Trust Service Provider* continues to takes care that employees receive appropriate training. Immediately after recruitment, the *Trust Service Provider* grants a training for its new employees, under the course of which they acquire the knowledge necessary to carry out the job. Registration officer can only be an employee, who finished a training course during which, he/she acquired the ability to recognize the ID cards acceptable by the *Trust Service Provider* (ID card, passport and driver's license). The *Trust Service Provider* usually supports the professional development of the employees, but it also expects employees to independently develop their skills in their respective fields. Some of the employees of the *Trust Service Provider* have the role to detect and gather the technical and business innovations and to organize, and share this knowledge with their colleagues.

Trusted roles can be held at the *Trust Service Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Trust Service Provider*. All personnel

in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the *Trust 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 *Trust Service Provider* only hires employees for trusted or leading roles, who

- have a clean record and there's no proceeding in progress against them that may affect the impunity.
- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

At the time of the appointment, shall the leading role holder *Trust 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 *Trust Service Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process, like previous employment, professional references, most relevant educational qualifications.

5.3.3 Training Requirements

The *Trust Service Provider* trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge;
- the specifics and the way of handling the *Trust 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 *Trust 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 *Trust Service Provider* trains the employees concerned with registration about the dangers and risks related to the verification of the data to be indicated on the Certificate.

The employees concerned with registration take and pass an exam on the knowledge of the related requirements and procedures for data verification before their appointment, and this fact is documented by the *Trust Service Provider*.

Only employees having passed the training shall gain access to the he production IT system of the *Trust Service Provider*.

5.3.4 Retraining Frequency and Requirements

The *Trust Service Provider* ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.

Further training is held if there's a change within the processes or the IT system of the *Trust Service Provider*.

The training material is updated at least in every 12 months and contains the new threats and actual security practices.

The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

5.3.5 Job Rotation Frequency and Sequence

The *Trust Service Provider* does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The *Trust Service Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *Trust Service Provider*, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability. Upon appointment every trusted role employee as part of the employment documents:

- gets written information about legal liabilities, rights, certification and management standards for the treatment of personal data,
- gets a job description that includes the concerning security tasks,
- signs a confidentiality agreement in which the related consequences non-compliant with security measures, (criminal sanctions) can be found too.

All of these include the labor legislation or criminal consequences, that sanction the different discipline – job obligations – violation or breaking the law.

5.3.7 Independent Contractor Requirements

The *Trust Service Provider* only assigns trusted roles to its employees.

The *Trust Service Provider* chooses persons employed with engagement contract or subcontract to perform the other tasks, chosen if possible, from the list of previously qualified suppliers. The *Trust Service Provider* concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons, and will not be exploited in any other way. The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the *Trust Service Provider* does not hold any trainings for them.

5.3.8 Documentation Supplied to Personnel

The *Trust Service Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents in writing:

- the organizational security regulations of the *Trust Service Provider*,
- the confidentiality agreement to be signed,
- personal job description,
- educational materials on the occasion of the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational security regulations.

5.4 Audit Logging Procedures

In order to maintain a secure IT environment the *Trust Service Provider* implements and operates an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

The *Trust Service Provider* logs every security-related event that can provide information on events, changes happened in the IT system or in its physical environment according to the generally accepted information security practice. In case of every log entry, it stores the following data:

- the time of the event;
- the type of the event;
- the identification of the user or the system who/what triggered the event;
- the success or failure of the audited event.

All new audit record is appended to the audit records. The earlier saved audit records can't be modified or deleted.

All of the essential event logs are available to the independent system auditors, who examine the compliance of the *Trust Service Provider*'s operation.

The *Trust Service Provider* logs The following events at minimum:

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- LOGGING:
  - the shutdown, restart of the logging system or some of its components;
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
  - the modification or deletion of the stored logging data;
  - the activities performed because of the logging system's failure.
- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles;
  - in case of password based authentication:
    - the change of the number of permitted unsuccessful attempts;
    - reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
    - readmission of the user blocked because of the unsuccessful login attempts;
  - changing the authentication technique (for example from password based to PKI based).
- KEY MANAGEMENT:
  - all events for the entire life cycle of service keys (key generation, saving, loading, destruction etc.);
- CERTIFICATE MANAGEMENT:
  - every event related to the issuance and the status change of the provider *Certificate*s.
  - every request including *Certificate* issuance, re-key, key renewal and revocation;
  - events related to the request processing;
  - all control activities undertaken in relation to the issuance of *Certificate*s, including the time of the telephone conversations related to the verification, the telephone number, the name of the called person and the acquired information;
  - approval or rejection of the *Certificate Application*s;

  - *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*.
- CONFIGURATION CHANGE:
  - hardware;
  - software;
  - operating system;
  - patch;
  - installation, update and removal of software on a Certificate System;
- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the system components used for providing the trust service;
  - access to a system component used for providing the trust service;
  - a known or suspected breach of physical security;
  - firewall or router traffic.

- OPERATIONAL ANOMALIES:
  - system crash, hardware failure;
  - software failures;
  - software integrity validation error;
  - incorrect or wrongly addressed messages;
  - network attacks, attack attempts;
  - equipment failure;
  - electric power malfunctions;
  - uninterruptible power supply error;
  - an essential network service access error;
  - violation of the *Certification Practice Statement*;
  - deletion of the operating system clock.
- OTHER EVENTS:
  - appointment of a person to a security role;
  - operating system installation;
  - PKI application installation;
  - initiation of a system;
  - entry attempt to the PKI application;
  - password modification, setting attempt;
  - saving the inner database, and restore from a backup;
  - file operations (for example creating, renaming, moving);
  - database access.

5.4.2 Frequency of Audit Log Processing

The independent system auditors of the *Trust Service Provider* evaluates the generated log files every working day.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the *Trust Service Provider* uses automated evaluation tools too, that are used to monitor the resulting log entries according to preset criteria and, where necessary, alert the operational staff.

The notifications received from the automated evaluation tools are processed and evaluated by the experts of the IT operation within 24 hours.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the online system, the logs are archived and their secure preservation is ensured by the *Trust Service Provider* for the amount of time defined in Section 5.5.2, but at least 10 years from the date of their creation.

For that time period, the *Trust Service Provider* ensures the readability of archived data, and maintains the software and hardware tools necessary for that.

5.4.4 Protection of Audit Log

The *Trust Service Provider* protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

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

The *Trust Service Provider* provides the log records with qualified *Time Stamp*s, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the *Trust Service Provider* makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The *Trust Service Provider* verifies the accesses in a secure way. The *Trust Service Provider* preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

5.4.5 Audit Log Backup Procedures

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

The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups shall be defined in the backup regulations of the *Trust Service Provider*.

5.4.6 Audit Collection System (Internal vs External)

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas are suspended by the *Trust Service Provider* until the incident is resolved.

5.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary the *Trust Service Provider* involves them in the investigation of the event. The Clients affected by triggering the event has the duty to cooperate with the *Trust Service Provider* to explore the event.

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Trust Service Provider* monitor the publicly available information about possible vulnerabilities and the new software patches. They analise the information, classify the vulnerability and if necessary inform the management about the result and propose an action plan to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat within a period of 48 hours after its discovery, but at least once a year the experts of the *Trust Service Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access, and may affect the *Certificate* issuing process, or allow modification of the data stored in the *Certificate*.

Based on the results of the analysis the *Trust Service Provider*

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis for the decision that the residual risk is accepted and the vulnerability does not require remediation.

At first the new software versions and software patches are installed on the test system of the *Trust Service Provider* and only after the successfully finished test are installed on the live system which is used to provide the services.

The new software patches are not installed on the live system if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reasons for not applying any security patches are documented.

5.5 Records Archival

5.5.1 Types of Records Archived

The *Trust Service Provider* is prepared to the proper secure long-term archiving of electronic and paper documents.

The *Trust Service Provider* archives the following types of information:

- every document related to the accreditation of the *Trust 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 *Trust 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;
- every electronic and paper based log entry.

5.5.2 Retention Period for Archive

The *Trust Service Provider* preserves the archived data for the time periods below:

- the *Certificate Policy* for at least 10 years from the date of repeal;
- *Certification Practice Statement* for at least 10 years from the date of repeal;
- General Terms and Conditions for at least 10 years from the date of repeal;
- in the case of video identification, all communications recorded during the identification for at least 10 years from the date of recording;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate;
- all other documents to be archived for at least 10 years from the date of their creation.

5.5.3 Protection of Archive

The *Trust Service Provider* stores all archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper based copy of the document available.
Each of the two locations fulfils the requirements for archiving security and other requirements.
During the preservation of the archived data, it is ensured that:

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

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

5.5.4 Archive Backup Procedures

The *Trust Service Provider* makes an authentic electronic copy of the original paper documents in accordance with the relevant legislation.

Electronic copies are stored according to the same rules as other protected electronic documents.

After archiving the authentic electronic copies the *Trust Service Provider* may destroy the original paper documents.

5.5.5 Requirements for Time Stamping of Records

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

The time value is given by the internal clock of the *Trust Service Provider* which is synchronized to two separate Stratum-1 UTC time sources:

- one accurate time source uses the satellite-based GNSS (GPS and Galileo) system;
- the other accurate time source is based on the longwave time signal service (DCF77).

In order to provide accuracy the *Trust Service Provider* synchronizes its own internal time with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization at least 4 times a day.

This way the *Trust Service Provider* guarantees that the deviation of the time indicated in the time marks from the UTC time base is at most 1 second.

The *Trust Service Provider* provides the daily log files with a qualified *Time Stamp*.

During the preservation of the archived data, if necessary (for example algorithm change expiration of the original *Time Stamp*) the authenticity of the data is ensured.

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *Trust Service Provider*'s protected computer system, and only the log files that are electronically signed and protected with qualified time stamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the *Trust Service Provider* in an inner data storage operated by it.

5.5.7 Procedures to Obtain and Verify Archive Information

The *Trust Service Provider* creates the log files manually or automatically. In case of an automatic logging system, the certified log files are generated daily.

The archived files are protected from unauthorized access.

Controlled access to the archived data is only available to the eligible persons:

- *Client*s 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 *Trust Service Provider* ensures that the used *Certification Unit*s are continuously possessing a valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it generates a new key pair for the *Certification Unit*s and inform its Clients in time. The new provider key is generated and managed according to this regulation.

If the *Trust Service Provider* changes any of its end-user *Certificate*s issuer provider Certificate keys, it complies with the following requirements:

- it discloses the affected Certificates and public keys in accordance with the requirements defined in section 2.2 ;
- after the provider re-key the end-user *Certificate*s to be issued will only be signed with the new provider keys;
- it preserves its old Certificates and public keys, and makes available the seal verification until all of the with the old provider key validity time expire.

5.7 Compromise and Disaster Recovery

In case of a disaster, the *Trust Service Provider* takes all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it takes the necessary amendments, corrective measures to prevent future occurrence of the incident.

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

5.7.1 Incident and Compromise Handling Procedures

The *Trust Service Provider* has a business continuity plan.

The *Trust Service Provider* established and maintains a fully functional backup system, which is at a safe distance from the primary location, geographically located at a different place and is independently capable of supplying the full range of services.

The *Trust Service Provider* annually tests the changeover to a backup system and reviews its business continuity plans.

The *Trust Service Provider* has increased security tools and systems in order to minimize the software and hardware failures and data corruptions. The recoverability of services is guaranteed by the underpinning contracts and own backup tools of the *Trust Service Provider*.

The internal policies of the *Trust Service Provider* define in detail the tasks related to the management of security incidents. Any deviation from normal operation is recorded in the internal task management system after detection. Upon detection of a discrepancy, the *Trust Service Provider* shall immediately begin the investigation of the discrepancy, eliminate the detected discrepancy as soon as possible and, if necessary, take preventive measures to prevent the recurrence of the discrepancy.

In all cases, the *Trust Service Provider* classifies any discrepancy that may affect the availability, integrity or confidentiality of the services as a security incident and prioritizes it (e.g. service interruption).

The *Trust Service Provider* shall officially notify the National Media and Infocommunications Authority of service outages and security incidents deemed serious within 24 hours of the occurrence of the incident.

In the event of a security incident, the *Trust Service Provider* creates an incident report in the Mozilla Bugzilla system in accordance with the requirements of the trusted root certificate programs, in which it describes in detail the circumstances of the security incident, the root causes, the affected Certificates, the immediate measures taken to eliminate the incident and the longer-term measures in order the prevention of further incidents.

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

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

The *Trust Service Provider* makes a full daily backup of its databases and the generated log events.

The *Trust Service Provider* makes full system backups as frequently as necessary to be able to restore the full service in case of a disaster.

The business continuity plan of the *Trust Service Provider* includes accurate requirements for the tasks to be performed in case of critical system component failure.

Once the problem resolved and the integrity restored, the *Trust Service Provider* restarts its services as soon as possible.

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

5.7.3 Entity Private Key Compromise Procedures

The Business Continuity Plan of the *Trust Service Provider* has an action plan in place in case the provider private keys compromise. The action plan reveals the circumstances of the compromise besides the revocation of the provider public key and the *Certificate* accompanying, arranges the notification of all concerned parties, takes the necessary steps against the recurrence of the compromise and, if necessary, provides new key to the service unit and the compromise affected end users. The *Trust Service Provider* immediately ceases to use that particular key in case of certification unit key compromise.

In case another certificate authority also issued *Certificate* for the given certification unit - by law, contract or agreement between CAs based - and over or cross certified this certification unit of the *Trust Service Provider*, the *Trust Service Provider* promptly informs that other Certification Authority for that given key compromise and initiates the certificate revocation belonging to the key in question.

The *Trust Service Provider* publishes a notice about the provider public key revocationaccording to the section 1.3.1

5.7.4 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster are defined in the *Trust Service Provider*'s business continuity plan.

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

The secondary services site is placed so far away from the primary site that a probable disaster cannot reach both locations simultaneously.

The *Trust 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 *Trust Service Provider* restores its devices damaged during the disaster and the original service security level as quickly as possible

5.8 CA or RA Termination

In the event of the planned termination of the service, the *Trust Service Provider* notifies the end users and the National Media and Infocommunications Authority at least 60 days prior to the termination of the service.

The Certification Service and Certificate Status Service Termination

At the same time with the notification about the service termination, the *Trust Service Provider* shuts down the following services:

- registration,
- *Certificate* creation,
- *Certificate* issuance,
- *Certificate* renewal,
- *Certificate* modification
- re-key.

The *Trust Service Provider* at least 20 days before the planned termination, but at least 14 days after the notification of the *Client*s :

- revokes all valid enduser *Certificate*s;
- stop processing the revocation requests;
- terminates the regular issuance of the *Certificate Revocation List*s;
- issues a closing *Certificate Revocation List*, in wich the value of the "nextUpdate" field is "99991231235959Z".

At the same time of the termination, the *Trust Service Provider* shuts down the following services:

- *Certificate* publishing,
- *Certificate* revocation status publishing,
- OCSP service.
- technical support.
- information provision.

Before a planned termination, the *Trust Service Provider* engages in negotiations about the taking over of its services with other Trust Service Provider whose rating is identical to its own. Under section 9.3 , it will hand over its records, including confidential user data, to such a Trust Service Provider or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.

The *Trust Service Provider* takes measures concerning the revocation of provider *Certificate*s (and destroying private keys) during the 60 day period – depending on the outcome of the negotiations.

The *Trust Service Provider* informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The *Trust Service Provider* is to inform its *Client*s by electronic mail, and *Relying Parties* by means of a publication on its website.

The *Trust Service Provider* will publish an announcement about the shutdown of active root certification units at least 5 days before the termination in accordance with chapter 2.1.

The *Trust Service Provider* destroys the private keys of the terminated root certification units within 5 working days after the termination in a documented manner.

Upon termination the service, the *Trust Service Provider* produces a full scope backup of its data contained in its IT system, protected by a qualified *Time Stamp*.

The *Trust Service Provider* provides for authorised *Relying Parties* the possibility to interpret the data appearing in its revoked *Certificate*s records if necessary.

In order to make the handing over of its data to another Trust Service Provider possible, the *Trust Service Provider* places data on media and in a format which the new Trust Service Provider can receive or provides the new Trust Service Provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this.

6 Technical Security Controls

The *Trust Service Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Trust Service Provider* manages the provider cryptographic private keys during their whole life-cycle within a *Hardware Security Module* that has appropriate Certification.

Both the *Trust Service Provider* and the system supplier and execution contractors have significant experience with deployment of PKI based systems and trust services and they use internationally recognized technology.

The *Trust Service Provider* continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

6.1 Key Pair Generation and Installation

The *Trust Service Provider* makes sure that the generation and management of all the private keys generated by it – for itself and for some of its departments (for example *Certificate Repository*, *Registration Authority*) – is secure and complies with the regulatory requirements in force and with industry standards.

6.1.1 Key Pair Generation

The *Trust Service Provider* uses key generation algorithms for the key pair generation, which comply with the requirements set out in the following normatives:

- ETSI TS 119 312 [19];
- CABF Baseline Requirements recommendation [42];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [8] 92. § (1) b) .

Generation of Service Provider's key pairs

The *Trust Service Provider* in case of the generation of a key pair of its own ensures:

- 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 *Trust 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 [24], or
  - meets the requirements of FIPS 140-2 [44] level 3 or higher, or
  - meets the requirements of FIPS 140-3 [45] level 3 or higher, or
  - meets the requirements of CEN 419 221-5 [21], or
  - is a reliable system that is evaluated in accordance with ISO/IEC 15408 [23] 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 *Trust 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 generatin key pairs for Service Provider's root and intermediate *Certificate* the *Trust 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 *Trust Service Provider* responsible for key management and a trusted person independent from the operation of the *Trust 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.

Generation of Service Provider's infrastructure key pairs

In case of generating the infrastructure keys used in its own IT systems, the *Trust Service Provider* ensures that:

- the generation of the *Trust 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

The *Trust Service Provider* never generates keypairs for the enduser *Certificate*s.
In case of an *Applicant* generated key pair:

- the production of keys shall be done in a properly secure environment that is under the supervision of the *Applicant*;
- the *Applicant* shall ensure the proper protection of the generated private key;
- the *Trust 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 *Trust 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 *Trust Service Provider* is aware of a demonstrated or proven method that exposes the *Applicant*'s private key to compromise;
- the *Trust Service Provider* has previously been made aware that the *Applicant*'s private key has suffered a key compromise, such as through the provisions of Section 4.9.1;
- the *Trust Service Provider* is aware of a demonstrated or proven method to easily compute the *Applicant*'s private key based on the public key (such as a Debian weak key, see `https://wiki.debian.org/SSLkeys`).

6.1.2 Private Key Delivery to Subscriber

The *Trust Service Provider* never generates keypairs for the enduser *Certificate*s.

6.1.3 Public Key Delivery to Certificate Issuer

When the key pair is generated by the *Applicant*, the following provisions shall be complied with:

- the public key shall be sent to the *Trust Service Provider* in a manner that it can be unambiguously assigned to the *Applicant*;
- the *Certificate Application* process shall prove that the *Applicant* really owns the private key corresponding to the public key.

When the end user keys generated by the *Applicant*, the *Applicant* sends the *Trust Service Provider* a PKCS#10 formatted *Certificate Application* which he or she signs with the private key belonging to the public key to be indicated on the *Certificate*. The PKCS#10 formatted *Certificate Application* contains the public key generated by the *Applicant* and the *Subject* data to be indicated on the *Certificate*, so both requirements are met.

6.1.4 CA Public Key Delivery to Relying Parties

The *Trust Service Provider* discloses the status information related to the provider Certificates for the Relying Parties by the following methods:

- The *Trust Service Provider* publishes the full provider certificate hierarchy containing every root and intermediate provider certificate from which every current provider Certificate is downloadable (see at the Provider certificates point at the

  `https://e-szigno.hu/en/pki-services/ca-certificates.html`

  url).
- The denomination of the root and intermediate certification units and the *Root Certificate*s' hash is in the 1.3.1 section of the *Certification Practice Statement*.

- The Certificates of the intermediate certification units are published on the certified Hungarian Trust Service Provider List [49] maintained and published by the National Media and Infocommunications Authority within the framework of the European common regulations [48]. The list contains every provider certificate (even the expired and revoked ones).
- For the online certificate status response signer responders the *Trust Service Provider* – according to the best international practice – issues *Certificate*s with very short validity periods, thus eliminating the necessity of checking the revocation status of the *Certificate*s. The current status of the *Certificate*s is continuously available at the webpage of the *Trust Service Provider* at the

  `https://e-szigno.hu/en/pki-services/ca-certificates.html`

  address.

The *Trust Service Provider* discloses for the *Relying Parties* the status information related to the *Certificate* of the certification units operated by it, and of the units that take part in the online certificate status service by the following methods:

- The status information related to the *Certificate* of the root certification units is available on the webpage of the *Trust Service Provider*.
- The status change information of the intermediate (not root) certification units' certificates is disclosed on the *Certificate Revocation List*s, on its webpage and within the confines of the online certificate status response service.
- For the responders signing the online certificate status responses the *Trust 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 *Trust Service Provider* guarantees that in case of key compromise or other problem no new *Certificate* will be issued for the old private key signing the OCSP responses . The *Trust Service Provider* issues the OCSP response *Certificate*s for new, secure private keys.

Regarding the disclosure methods of the status information, also see Section 4.10.

6.1.5 Key Sizes

The *Trust Service Provider* uses cryptographic algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [19];
- CABF Baseline Requirements recommendation [42];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [8] 92. § (1) b) .

The *Certification Authority* uses at least 2048 bit RSA keys or at least 256 bit ECC keys in every currently active root and intermediate provider *Certificate* and even in the *Certificate*s of the *Time Stamping Unit*s and the OCSP responders.

The *Certification Authority* issues the enduser *Certificate*s only for at least 2048 bit RSA keys or at least 256 bit ECC keys.
The *Trust Service Provider* supports only the following RSA keylengths:

- RSA-2048 (2048 bit)
- RSA-3072 (3072 bit)
- RSA-4096 (4096 bit)

The *Trust Service Provider* supports only the following ECC curves:

- ECC NIST P-256 (256 bit)
- ECC NIST P-384 (384 bit)
- ECC NIST P-521 (521 bit)

The ECC key always represents a valid point on the supported elliptic curve.

6.1.6 Public Key Parameters Generation and Quality Checking

The *Trust Service Provider* generates the keys according to the description of the section 6.1.1.

Verification of Compliance of Parameters

A *Certification Authority* verifies the compliance of each service provider's and enduser's key before the *Certificate* issuance to the following parameters:

1. in case of RSA keys
    - RSA keylength is within the supported values
    - RSA exponent is odd
    - the value of the RSA exponent is at least "(2 exp 16)+1" and at most "(2 exp 256)-1"
    - the modulus is odd, not a prime power and it does not have a divider smaller than 752
2. in case of ECC keys
    - the key is a valid point in a supported curve (ECC Full Public-Key Validation Routine as defined in section 5.6.2.3.3 of NIST Special Publication 800-56A Revision 3 [46])

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The *Trust 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' *Certificate*s,

- to sign the OCSP responder *Certificate*,
- to sign CRLs.

The private key of the *Trust 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' *Certificate*s,
- to sign the end user *Certificate*,
- to sign the *Time Stamping Unit Certificate*,
- to sign the OCSP responder Certificate,
- to sign CRLs.

The *Trust Service Provider* includes the "Key Usage" extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [39] compatible applications technically restrict the usage of the *Certificate*s. The requirements set out for the value of the field are in Section 7.1.2.

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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The *Trust Service Provider* ensures the secure management of the private keys held by it and prevents the private key disclosure, copy, deletion, modification and unauthorized usage. The *Trust Service Provider* may only preserve the private keys as long as the provision of the service definitely requires.

The *Trust Service Provider* stores and uses the Root CA private keys physically isolated from normal operations such that only designated trusted personnel have access to the keys for use.

The *Trust Service Provider* private keys used for the certification organization *Certificate* issuance are stored at a physically secure location, in a secure *Hardware Security Module*.

The *Trust Service Provider* deletes the signing private keys stored on the *Hardware Security Module*s which are out of order in as defined in the device's manual so that it is practically impossible to restore the keys.

The *Trust Service Provider* doesn't generates keypairs for the *Applicant*, eliminating the need to ensure the preservation of the end-user private keys.

6.2.1 Cryptographic Module Standards and Controls

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

- the requirements of ISO/IEC 19790 [24], or
- the requirements of FIPS 140-2 [44] level 3 or higher, or
- the requirements of FIPS 140-3 [45] level 3 or higher, or
- the requirements of CEN 419 221-5 [21], or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to ISO/IEC 15408 [23] 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 *Trust Service Provider* stores the provider private keys outside of the *Hardware Security Module* only in encrypted form. Only those algorithms and key parameters are used for encoding wichs fizs to the actual algorithmic decision of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [8] 92. § (1) b) and that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The *Trust Service Provider* provider private keys are stored in a physically secure site even in an encrypted form, in the safe of the *Data Centre* , where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the *Trust Service Provider* destroys the coded keys or recodes them again using algorithm and key parameters that ensure higher protection.

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

The *Trust Service Provider* implements the "n out of m" at the activation of the private key related key management functions. The parameters are determined so that the simultaneous presence of at least two; trusted role holder employees is needed for the critical operations carried out with its provider private keys.

6.2.3 Private Key Escrow

The *Trust Service Provider* does not escrow its provider or enduser private keys.

6.2.4 Private Key Backup

The *Trust Service Provider* makes security copies of its provider private keys, before putting the provider private key into service as described in section 6.2.1. in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 6.2.2..

The *Trust Service Provider* stores the backup copy in duplicate, and at least one copy of those is stored at a different place from the service provider location.

The same strict security standards are applied to the management and preservation of backups as for the operation of the production system.

The *Trust Service Provider* does not make any copy of the end-user private keys.

6.2.5 Private Key Archival

The *Trust Service Provider* does not archive its private keys and the end-user private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Trust Service Provider* are created in a *Hardware Security Module* that meets the requirements.

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

The *Trust Service Provider* only exports the private key from the *Hardware Security Module* for the purpose of making a secure copy.

The export and loading of the provider private keys is performed according to section 6.2.2.

6.2.7 Private Key Storage on Cryptographic Module

The *Trust Service Provider* keeps its private keys used for service provision in *Hardware Security Module*s according to section 6.2.1.

Private keys are stored and used in the *Hardware Security Module* as specified in the certification of the device with full compliance with the related operating instructions.

6.2.8 Method of Activating Private Key

The *Trust Service Provider* keeps its provider private keys in a secure *Hardware Security Module* and complies with its user guide and the requirements outlined in the certification documents. The *Hardware Security Module* can only be activated by the corresponding operator cards and the private keys within the *Hardware Security Module* can not be used before activating the module. The *Trust Service Provider* keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the *Trust Service Provider*.

The *Trust Service Provider* ensures that signatures can only be created with the private key of the root unit certificate in case of commands issued directly by the trust official duly authorized to do so.

In case of *Applicant* generated private key the protection of the private key is the *Applicant*'s full responsibility.

6.2.9 Method of Deactivating Private Key

Provider Private Keys

The private key used by the *Trust Service Provider*, and managed by the cryptographic devices becomes deactivated if (in a regular or irregular way) the device is removed from active status. This can happen in the following cases:

- the user deactivates the key,
- the power supply of the device is interrupted (switched off or power supply problem),
- the device enters an error state.

The private key deactivated like this can not be used until the module is in active state again.

End-User Private Keys

The proper usage of the private keys is the responsibility of the *Applicant*.

6.2.10 Method of Destroying Private Key

Provider Private Keys

The discarded, expired or compromised *Trust Service Provider*'s private keys are destroyed in a way that makes further use of the private keys impossible.

The *Trust Service Provider* destroys the provider private keys stored in the secure *Hardware Security Module* of the certification organization according to the procedures, requirements defined in the user guide and in the certification documents of the used *Hardware Security Module*, in the simultaneous presence of two *Trust Service Provider* employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

The *Trust Service Provider* destroys each backup copy of the private key in a documented way in such a way that its restoration and usage becomes impossible.

End-User Private Keys

The discarded website authentication private keys of the end-users are recommended to be destroyed.

6.2.11 Cryptographic Module Rating

According to the requirements of Section 6.2.1 every provider private key of the *Trust Service Provider* is stored in a cryptographic module that

- has a certificate according to ISO/IEC 19790 [24], or
- has a certificate according to FIPS 140-2 Level 3 [44], or
- has a certificate according to FIPS 140-3 Level 3 [45], or
- has an at least EAL-4 level Common Criteria [47] based certificate attesting compliance with the requirements of the CEN 419 221-5 [21], 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 *Trust Service Provider* archives every issued *Certificate* for ten years after the end of the validity period or until the completion of the incurred dispute related to the *Certificate*.

For the same time period, the *Trust Service Provider* preserves devices, with which the content of the *Certificate* can be established.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Keys and Certificates of the Root Certification Units

The validity period of the *Trust Service Provider* root certification unit certificates and the private keys belonging to them shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority.

The validity period of the *Trust Service Provider* root certification unit certificates and the private keys:

- the key of the "Microsec e-Szigno Root CA" root certification unit was valid until 2017-04-06
- the key of the "e-Szigno OCSP CA" root certification unit was valid until 2017-04-26
- the key of the "Microsec e-Szigno Root CA 2009" root certification unit is valid until 2029-12-30

  Due to the planned phase out of the use of 2048-bit RSA keys - 2025-12-31 according to the currently valid cryptographic requirements - the entire hierarchy will be shut down on schedule.
- the key of the "e-Szigno Root CA 2017" root certification unit is valid until 2042-08-22
- the key of the "e-Szigno TLS Root CA 2023" root certification unit is valid until 2038-07-17
- The validity period of root certificates created after 2023-09-15 shall be
  - minimum 2.922 days (≙8 years)
  - maximum 9.132 days (≙25 years)

The Keys and Certificates of the Intermediate Certification Units

The validity period of the *Trust Service Provider* intermediate certification unit certificates and the private keys belonging to them:

- shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority;

- shall not exceed the validity period of the issuer root or intermediate provider *Certificate* that issued the intermediate provider *Certificate*.

The intermediate (not root) certification unit keys of the *Trust Service Provider* are valid until the expiration time of the *Certificate*s belonging to them.

End-User Certificates

The validity period of the end user *Certificate*s issued by the *Trust Service Provider* is

- maximum 398 days (≙13 months) from the date of issuance;
- shall not exceed the date until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority;
- shall not exceed the expiration date of the provider *Certificate* that issued the *Certificate*.

Taking into account the above aspects, the *Trust Service Provider* issues end-user *Certificate*s with the following validity periods by default:

- 396 days (≙13 months) from the date of issuance;

If the *Trust Service Provider* deviates from the specified values, it will inform the *Client*s in advance.
During the Certificate renewal and Certificate modification the *Trust Service Provider* may issue the new *Certificate* for the same end-user private key.

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.
If this happens, the *Trust Service Provider* revokes the related *Certificate*s.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The *Trust Service Provider*'s private keys are protected in accordance with the procedures, requirements defined in the used *Hardware Security Module* user guide and the certification documents.
In case of password based activation data usage, the passwords are sufficiently complex in order to ensure the required level of protection.
The *Trust Service Provider* never generates software based private keys for the end user *Certificate*s.
The creation and installation of the activation data of the *Applicant* created private keys is the duty of the *Applicant*.

6.4.2 Activation Data Protection

The employees of the *Trust Service Provider* manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

The protection of the activation data of the private keys created by the *Applicant*, is the duty and responsibility of the *Applicant*.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the *Trust Service Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *Trust Service Provider* are sufficiently protected from unauthorized access;
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

6.5.2 Computer Security Rating

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, Microsec has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

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

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

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

Based on the results of the risk assessment the *Trust Service Provider*

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The *Trust Service Provider* only uses applications and devices in its production IT system that are:

- commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by the *Trust 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 *Trust Service Provider* during which design structured development methods and controlled development environment were used, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

Procurement of IT tools is performed in a way that excludes changes to the hardware and software components using reliable, regularly qualified suppliers.

The hardware and software components applied for the provision of services are not used for other purposes by the *Trust Service Provider*.

The *Trust Service Provider* prevents the malicious software from entering into the devices used for certification services with appropriate security measures.

The hardware and software components are checked regularly for malicious software prior the first usage, and subsequently.

The *Trust Service Provider* acts with the same carefulness in case of program update purchases as at the acquisition of the first version.

The *Trust Service Provider* employs reliable, adequately trained staff over the course of installing software and hardware.

The *Trust Service Provider* only installs softwares to its service provider IT equipment necessary for the purpose of service provision.

The *Trust Service Provider* has a version control system where every change of the IT system is documented.

The *Trust Service Provider* operates automatic monitoring system to record all unauthorized changes, which records all changes in every file and in case of changes in the monitored files it generates a log entry or sends an alert to the system operators.

6.6.2 Security Management Controls

The *Trust Service Provider* implements processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system detects any kind of unauthorized changes, data entry that affects the system, the firewall, the routers, programs and other components used in the service. Installing the program used in the service the *Trust Service Provider* ensures that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Trust Service Provider* regularly checks the integrity of the software in its system used in the service.

Each *Hardware Security Module* applied by the *Trust Service Provider* has been verified, tested and evaluated. The *Trust Service Provider* verifies the integrity of the modules:

- following the acquisition of the devices during the takeover,
- immediately before the first usage,
- regularly during operation.

The *Trust Service Provider* deletes the provider keys from the *Hardware Security Module*s permanently or temporarily withdrawn from use.

The *Trust Service Provider* stores the unused *Hardware Security Module*s at a physically protected location.

6.6.3 Life Cycle Security Controls

The *Trust Service Provider* ensures the protection of the used *Hardware Security Module*s during their whole life cycle.

During the operation of the IT equipment and systems used for the provision of the services, the *Trust Service Provider* takes into account the security aspects related to the life cycle of the equipment, according to which:

- it uses properly certified *Hardware Security Module*s in its systems;
- ensure, upon receipt of the *Hardware Security Module*s, that the quality control ensures that that the protection of the *Hardware Security Module*s against tampering was ensured during transportation;
- it stores the *Hardware Security Module*s in a safe place, and ensure the protection of the *Hardware Security Module*s against tampering during storage;
- continuously complies with the requirements set out in the *Hardware Security Module*'s security target, instructions for use and certification report during operation;
- deletes the private keys stored in their decommissioned *Hardware Security Module*s in such a way that it becomes practically impossible to restore the keys;
- handle and dispose of decommissioned *Hardware Security Module*s in accordance with the requirements of its security target, instructions for use and certification report.

6.7 Network Security Controls

The *Trust Service Provider* follows industry best practices for securing their networks. It conforms to the CA/B Forum's Network and Certificate System Security Requirements [41].

The *Trust Service Provider* keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too.

The *Trust Service Provider* implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system.

The *Trust Service Provider* checks the authenticity and integrity of every software component at their first loading.

The *Trust Service Provider* applies proper network security measures for example:

- divides its IT system into well separated security zones;
- separates dedicated network for administration of IT systems and the *Trust Service Provider*'s operational network;
- separates the production systems for the TSP services from systems used in development and testing;
- establishes communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- operates the IT systems used for the live operational network in secure network zones;
- restricts access and communications between zones to those necessary for the operation of the service;
- disables the not used protocols and user accounts;
- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .
- reviewes the established rule set on a regular basis.

The *Trust Service Provider* undergoes or performs a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least every three (3) months.

The *Trust Service Provider* checks the compliance of the local network components (e.g. routers) configuration with the requirements specified by the *Trust Service Provider* at least every three months.

The *Trust Service Provider* orders a penetration test from an external independent expert who has the necessary skills, tools, proficiency and code of ethics to provide a reliable report yearly and in case of a significant change in the IT network.

6.8 Time stamping

For the protection of the integrity of the log files and other electronic files to be archived the *Trust Service Provider* uses qualified electronic *Time Stamp*s issued by the e-Szignó Certificate Authority.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The end-user *Certificate*s issued by the *Trust Service Provider* and all the provider's root and intermediate *Certificate*s which are in the *Certificate* Chain used to issue the *Certificate*s comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [39]
- IETF RFC 5280 [30]
- IETF RFC 6818 [33]
- IETF RFC 6962 [35];
- ETSI EN 319 412-1 [15]
- ETSI EN 319 412-4 [18]
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [42]

7.1.1 Version Number(s)

The provider certification unit (root and intermediate) *Certificate*s used by the *Trust Service Provider* and the end-user *Certificate*s issued by the *Trust Service Provider* are "v3" *Certificate*s according to the X.509 specification [39].

The *Certificate*s have the following basic fields:

- Version
  The *Certificate* complies with "v3" *Certificate*s according to the X.509 specification, so the value "2" is in this field. [30]
- Serial Number
  The unique identifier generated by the *Certificate* issuer certification unit.

  In case of the end-user *Certificate*s the "Serial Number" field contains a random number generated by a CSPRNG conformant *Hardware Security Module*, with at least 8 bytes (64 bits) entropy.

- Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for the creation of the electronic seal certifying the *Certificate*.

  The *Certification Authority* uses 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
  Electronic seal made by the *Certification Authority* certifying the *Certificate*, that has been created with an Algorithm set defined in the "Algorithm Identifier" field.

- Issuer
  The unique name of the *Certificate* issuer *Certification Unit* according to the ITU X.501 [38] 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
    - earliest the real issuance time of the *Certificate* minus 48 hours
    - latest the real issuance time of the *Certificate* plus 48 hours

  The *Trust Service Provider* never backdates *Certificate*s.

  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 [38] name format (see in section 3.1).

  Always filled out.

- Subject Public Key Algorithm Identifier

  The *Trust Service Provider* supports the RSA and the ECC algorithms in the end-user *Certificate*s.

  The value to be included in this field:

  - "rsaEncryption" (1.2.840.113549.1.1.1)

  - "ecPublicKey" (1.2.840.10045.2.1)

- Subject Public Key Value
  The public key of the Subject.
- Issuer Unique Identifier
  Not filled out.
- Subject Unique Identifier
  Not filled out.

7.1.2 Certificate Extensions

the *Trust Service Provider* only uses the following certificate extensions according to the X.509 specification [39]:

Certificate of the Root Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field is not indicated.
- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the *Certificate*.

  The field value: the SHA-1 hash of the provider public key.

  In case of the self-signed root certification unit certificate the value is identical with the value of the *Subject* key identifier field.
- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key. The field value: the SHA-1 hash of the public key.

  Always filled in.
- Subject Alternative Names – not critical
  OID: 2.5.29.17

  It is filled in according to section 3.1.1.
- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" field is not present in the root *Certificate*.

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

  The used values are:

  - "keyCertSign",
  - "cRLSign".

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

The above fields are always filled out. There is no any more *Certificate* extension.

Certificate of the Intermediate Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32

  This field may limit the *Certificate Policy*s which can be used in the Enduser *Certificate*. The intermediate CAs below this CA may issue only that type of Enduser *Certificate*s which fit to at least one of the *Certificate Policy*s listed here.

  It is always filled.

  In case of *Certificate*s issued to the intermediate certification units of the *Trust 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 *Certificate*s issued to other *Certification Authority*, only that identifier can be in this field, which relates to a *Certificate Policy* which complies to the *Certificate Policy* implemented by the issuer *Certification Authority*, and there can be no "anyPolicy" Identifier.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the *Certificate*.

  It is always filled.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key.
  The field value: the SHA-1 hash of the public key.

  It is always filled.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  It is filled in according to section 3.1.1.
- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" is not present in the *Certificate*.
- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The field contains the following values:

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

  The Intermediate Certification Unit *Certificate*s issued after 2019-01-01 for issuing *Website Authentication Certificate*s

  – contains the following EKU value:
    * Server Authentication (1.3.6.1.5.5.7.3.1)
  – may contain the following EKU value:
    * Client Authentication (1.3.6.1.5.5.7.3.2)
- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL accessibility through http protocol.
  It is always filled.
- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the *Certificate* provided by the *Trust 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 *Trust Service Provider* provides online certificate status service. The availability of this service is indicated here.
  – To facilitate the certificate chain building the *Trust Service Provider* gives the access path through http protocol of the *Certificate* of the *Certificate* issuer certification unit.

The above fields are always filled out. There is not 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 *Trust Service Provider* fills in this field in all cases by providing the following data:

  - the identifier of the *Certificate Policy* (OID according to section 1.2.1);
  - the availability of the *Certification Practice Statement*;
  - The identifier specified by ETSI EN 319 411-1 [14] 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,
    - in case of IVCP *Certificate* OID 0.4.0.2042.1.8.
  - The Certificate policy defined by the CA/Browser Forum as follows:
    - in case of DVCP *Certificate* OID 2.23.140.1.2.1,
    - in case of OVCP *Certificate* OID 2.23.140.1.2.2,
    - in case of IVCP *Certificate* OID 2.23.140.1.2.3.

  The end-user *Certificate*s that do not contain the "Certificate Policies" field shall be considered test certificates. The test *Certificate* can only be used for testing purposes, and they shall be declined in case of real transactions.

  The reference to the related Certification Practice Statement may be given in this field.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the *Certificate*.

  It is always filled in.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key. The field value: the SHA-1 hash of the public key.

  It is always filled in.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  See section: 3.1.1.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the end-user *Certificate*s.

  The "pathLenConstraint" field is not present in the end-user *Certificate*s.

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

  In the *Website Authentication Certificate*s 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"

  The same key usage values are used in the Server Authentication *Certificate*s, like the CISCO VPN Server, the Domain Controller or the VPN Server Authentication *Certificate*.

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

  In the *Website Authentication Certificate*s the set value is:

  - "serverAuth (1.3.6.1.5.5.7.3.1)"

  In the *Website Authentication Certificate*s the following further value is included by default, but may be left out in case of the request of the *Applicant*:

  - "clientAuth (1.3.6.1.5.5.7.3.2)"

  In the Server Authentication *Certificate*s the following extended key usage bits are indicated:

Certificate Type	ExtKeyUsage
Cisco VPN Server	serverAuth (1.3.6.1.5.5.7.3.1), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
DomainController	clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)
RDP Gateway	serverAuth (1.3.6.1.5.5.7.3.1)

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL availability relevant to the *Certificate* through http protocol. The CRL availability related to the *Certificate* is present here (URL).

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the *Certificate* provided by the *Trust Service Provider*.

  In case of end-user certificates the field contains the following data:

  – For the purpose of the fast and reliable verification of the current *Certificate* revocation status, the *Trust Service Provider* provides online certificate status service on the default HTTP port (port 80). The availability of this service is indicated here.
  – To facilitate the certificate chain building the *Trust Service Provider* gives the access path through http protocol of the *Certificate* of the *Certificate* issuer certification unit.

  The *Trust 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 *Certificate*s, but it has a field, that can be used in case of a non-qualified *Certificate* too.

  The QCType field may be filled according to the usage purpose.

- 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.

  Filling out is optional and depends on the approval given by the *Applicant*.

The above fields are always filled out according to the given rules, except the List of embedded Signed Certificate Timestamps (SCT).
Other certificate extensions will not be filled out.

7.1.3 Algorithm Object Identifiers

The denomination of the cryptographic algorithm that has been used to certify the *Certificate*. The following cryptographic algorithms are used by the *Certification Authority* for sealing the end-user *Certificate*s:

- "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)

7.1.4 Name Forms

The *Trust Service Provider* uses a distinguished name – composed of attributes defined in the standards IETF RFC 5280 [30], ETSI EN 319 412-2 [16], ETSI EN 319 412-3 [17] and ETSI EN 319 412-4 [18] – for the Subject identification in the *Certificate*s issued based on this *Certification Practice Statement*.

The *Certificate* contains the globally unique identifier of the *Subject* (OID), filled out as defined in Section 3.1.1.

The value in the "Issuer DN" field of the *Certificate* is identical to the value in the "Subject DN" field of the issuer *Certificate*.

7.1.5 Name Constraints

The *Trust Service Provider* does not use name constraints with the use of the "nameConstraints" field.

7.1.6 Certificate Policy Object Identifier

The *Trust Service Provider* includes the not critical (*Certificate Policy*) extension in the *Certificate*s 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 *Trust Service Provider* can put short information related to the *Certificate* usage into the *Certificate Policy* extension Policy Qualifier field.

The field contains the online availability of the *Certification Practice Statement* (URI).

7.1.9 Processing Semantics for Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

The *Certification Authority* issues version "v2" certificate *Certificate Revocation List*s according to the IETF RFC 5280 [30] specification.

7.2.2 CRL and CRL Entry Extensions

The *Certificate Revocation List*s 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 *Certificate*s.
   The entire field is signed with the *Trust Service Provider*'s private key.

   (a) Version
   For the *Certificate Revocation List* version "v2" according to the IETF RFC 5280 [30] 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 [30]. In the case of *Certificate Revocation List*s issued by the *Certification Authority*, this is the same as the time of issue.

   (e) Next issuance (nextUpdate)
   Date of issuance of the next *Certificate Revocation List* (see Chapter 4.10). UTC value with "UTCTime" encoding according to IETF RFC 5280 [30].

   (f) Revoked Certificates
   The list of revoked *Certificate*s is sorted in ascending order by the Certificate Serial Number. If there is no 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 [30].

   Optional *Certificate Revocation List* Entry Extensions (crlEntryExtensions) that can be used by the *Certification Authority*:

   - Revocation Reason (reasonCode) – not critical
     OID: 2.5.29.21
     The reason for revocation is entered in this field.
     Mandatory field in case of subordinate CA *Certificate*s, including a meaningful reason code.

- Invalidity Date (InvalidityDate) – not critical
  OID: 2.5.29.24
  This field can contain the time the private key became untrusted.
  This field is not necessarily filled by the *Certification Authority*.
  When it is filled, the time value is equal to the time encoded in the "revocation-Date" field of the CRL entry.
- Guide to Suspended *Certificate*s (holdInstruction) – not critical
  OID: 2.5.29.23
  This field may contain the guide for managing the suspended *Certificate*.
  This field is not filled by the *Certification Authority*.

(g) CRL Extensions

- Provider Key Identifier (AuthorityKeyIdentifier)
  OID: 2.5.29.35
  The ID of the public key which belongs to the private key used to authenticate the *Certificate Revocation List* in the form of an "SHA1" hash.
- CRL Serial Number (cRLNumber) – not critical
  OID: 2.5.29.20
  This field contains the monotonically increasing serial numbers of the *Certificate Revocation List*s.

Certificate Revocation List Extension conditionally used by the *Certification Authority*:

- Expired Certificates on the CRL (expiredCertsOnCRL) – not critical
  OID: 2.5.29.60
  The *Certification Authority* indicates with this standard field according to the X.509 specification that it does not remove expired *Certificate*s from the CRL. (See: chapter 4.10.)

2. Signing Algorithm ID (signatureAlgorithm)
   The cryptographic algorithm set identifier (OID) used to create the electronic seal that authenticates the *Certificate Revocation List*. Name and OID of the cryptographic algorithm sets supported by the *Certification Authority*:

   - "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 seal of the *Certification Authority* certifying the *Certificate Revocation List*.

   The *Certificate Revocation List* is authenticated by the *Certification Authority* using the same key as used to seal the issued *Certificate*.

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

7.3 OCSP Profile

The *Trust Service Provider* operates an online certificate status service according to the IETF RFC 6960 [34] and IETF RFC 8954 [37] standard.

The OCSP responses issued by *Certification Authority* contain the following fields:

- Algorythm identifier (signatureAlgorithm)
  The identifier of the cryptographic algorithm used for signing the OCSP response (OID).

  The *Trust Service Provider* supports 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 *Trust Service Provider*.

- Identifier of the Responder (responderID)
  The unique identifier of the OCSP Responder which issues the OCSP Response.

- 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 [30].

- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response. Value according to UTC with encoding according to IETF RFC 5280 [30].

  Mandatory, the value is equal to the the time of the issuance + 12 hours.

- *Certificate* Status Response (SingleResponse)
  The field contains the ID of the *Certificate* (CertID) and the revocation status of the *Certificate* (CertStatus).

  The *Trust 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 *Trust Service Provider* and its revocation status is not revoked.

7.3.1 Version Number(s)

The *Trust Service Provider* supports the online certificate status requests and responses conforming to the "v1" version according to the standard IETF RFC 6960 [34] The default value of the (Version) field is "v1", so this field is not included in the OCSP response.

7.3.2 OCSP Extensions

The *Trust 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 [34] specification that it retain revocation information beyond the *Certificate*'s expiration. (See Section 4.10.)

The *Trust Service Provider* may include the following OCSP registration extension:

- Reason Code – not critical
  The reason of the revocation is in this field.

  Mandatory field in case of subordinate CA *Certificate*s, including a meaningful reason code.

8 Compliance Audit and Other Assessments

The *Trust Service Provider* has its operation periodically examined by independent external auditor. During the audit it is examined that the operation of the *Trust 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 [13]
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [14]
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [20]

The result of the screening is a confidential document accessible only to authorized persons.

The conformity certificate issued in accordance with the conformity assessment report is published on the webpage of the *Trust Service Provider*.

The *Trust Service Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Trust Service Provider* has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The *Trust Service Provider* keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

In addition to the external audit, the *Trust Service Provider* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Trust Service Provider* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation(see section: 1.3.1)

8.1 Frequency or Circumstances of Assessment

The *Trust Service Provider* has the conformance assessment carried out annually on its IT system performing the provision of the services .

An audit period never exceeds one year in duration. The successive period-of-time audits cover the entire lifetime of each trusted *Certification Unit*, continuously (without gaps) from cradle to grave.

The *Trust Service Provider* ensures regular monitoring of it internal processes, the details of which is specified in the *Certification Practice Statement* and in its inner regulations. It checks the compliance of the operation during a comprehensive internal audit at least once per every year in accordance with applicable CA/B Forum Guidelines.

Beginning in 2023, the *Trust Service Provider* shall perform an annual self-assessment evaluating the conformance of this *Certification Practice Statement* against CA/B Forum Baseline Requirements and the applicable Root Program Policies.

Completed self-assessments shall be submitted to the CCADB within 90 days from the "BR Audit Period End Date" field specified in the root CA's "CA Owner/Certificate" CCADB record (i.e. End Date of the Audit Period).

A random check is performed by the *Trust Service Provider* quarterly on at least 3% of the *Website Authentication Certificate* issued since the previous inspection, whether they comply with the related *Certificate Policies* and *Certification Practice Statement*.

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

8.2 Identity/Qualifications of Assessor

The *Trust Service Provider* performs the internal audits with the help of its employees who hold the independent system auditor role.

The eIDAS and ETSI conformity assessment is performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

8.3 Assessor's Relationship to Assessed Entity

External audit is performed by a person who:

- is independent from the owners, management and operations of the examined *Trust 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 *Trust Service Provider*.

- remuneration is not dependent on the findings of the activities carried out during the audit.

8.4 Topics Covered by Assessment

The review covers the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the *Certification Practice Statement*;
- adequacy of the employed processes;
- documentation;
- physical security;
- adequacy of the personnel;
- IT security;
- compliance with the data protection rules.

The scope of the audit covers all active intermediate *Certification Unit*s in the audited CA hierarchy, under which there is a valid *Certificate* or suitable for issuing a new *Certificate*.

If the *Trust Service Provider* issued a subordinate *Certificate* for the certification unit of another organization then the listed areas are examined at these external organizations as well.

8.5 Actions Taken as a Result of Deficiency

The independent auditor summarizes the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them are recorded in a separate chapter of the report.

The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

- modification suggestions to be optionally taken into consideration;
- derogations to be averted mandatorily.

8.6 Communication of Results

The *Trust Service Provider* publishes the summary report of the assessment on its web page on the following URL:

`https://e-szigno.hu/en/eidas/`

The *Trust Service Provider* doesn't publish the details of the findings, they are treated as confidential information.

The *Trust Service Provider* discloses the audit report in the CCADB operated by Mozilla within three months of the point-in-time date or the end date of the latest audited period.

The *Trust Service Provider* also discloses in the CCADB all CA certificates they issue that chain up to that CA certificate trusted in Mozilla's root store, including those CA certificates that share the same key pair whether they are self-signed, doppelgänger, reissued, cross-signed, or other roots.

The *Trust Service Provider* discloses such CA certificate within one week of certificate creation, and before any such CA is allowed to issue certificates.

9 Other Business and Legal Matters

9.1 Fees

The *Trust Service Provider* publishes fees and prices on its webpage, and makes them available for reading at its customer service.

Price list availability:

- `https://e-szigno.hu/en/price-list`

The *Trust Service Provider* may unilaterally change the price list. The *Trust Service Provider* publishes any modification to the price list 30 days before it comes into force.

The changes favorable for the *Client* may come into force with shorter deadline than 30 days.

Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service agreement and its annexes – the General Terms and Conditions in particular.

9.1.1 Certificate Issuance or Renewal Fees

See section: 9.1.

9.1.2 Certificate Access Fees

The *Trust Service Provider* grants free of charge online access to its *Certificate Repository* for the *Relying Parties*.

9.1.3 Revocation or Status Information Access Fees

The *Trust Service Provider* provides free of charge online CRL and OCSP service for the *Relying Parties* on the status of all end-user and intermediate *Certificate*s it issued.

9.1.4 Fees for Other Services

See section: 9.1.

9.1.5 Refund Policy

See section: 9.1.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage

The *Trust Service Provider* has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

- The *Trust Service Provider* has liability insurance to ensure reliability.
  - The liability insurance covers the following damages caused by the *Trust Service Provider* in connection with the provision of services:
    - damages caused by the breach of the service agreement to the trust service *Client*s;
    - damages caused out of contract to the trust service *Client*s or third parties;
    - damages caused to the National Media and Infocommunications Authority by the *Trust Service Provider* terminating the provision of the trust service;
    - under the eIDAS Regulation [1] 17. article (4) e) point, the legal costs of conformity assessment bodies to perform a conformity assessment by the request of the National Media and Infocommunications Authority if it enforces the costs as legal costs.
  - The liability insurance policy shall cover at least for 3.000.000 Hungarian forints. Coincidental damages occurred for the same reason constitute a single insurance event.
  - The liability insurance provides coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the *Trust 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.

9.3 Confidentiality of Business Information

The *Trust Service Provider* manages clients' data according to legal regulations. The *Trust Service Provider* has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

By applying for a *Certificate*, and signing the service agreement, *Client*s consent to the *Trust Service Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the *Trust Service Provider*'s services go offline; moreover to forwarding such information to the *Trust Service Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

*Applicant*s shall make a declaration whether they consent to the disclosure of a *Certificate* on the *Certificate Application* form that is linked to the service agreement.

The *Trust Service Provider* uses clients' data solely in connection with the provision of its services.

The *Trust Service Provider* discloses *Subject*s' and *Represented Organization*s' data appearing in a *Certificate* together with the *Certificate*. The *Trust Service Provider* stores their data that are not entered in a *Certificate* in a secured manner, for the purpose of providing evidence about the *Subject*s' identity, *Represented Organization*s' organisational identity, and that of its miscellaneous data provision related obligations. The *Trust Service Provider* retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the *Trust Service Provider* sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The *Trust Service Provider* provides for the confidentiality and intactness of information that is not public during the forwarding of *Client*s' data.

9.3.1 Scope of Confidential Information

The *Trust Service Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 9.3.2;
- besides the *Client* data:
  - private keys and activation codes,
  - *Certificate Application*s and Service Contracts,
  - transaction related data and log data,
  - non-public regulations,
  - all data whose public disclosure would have an adverse effect on the security of the service.

9.3.2 Information Not Within the Scope of Confidential Information

The *Trust Service Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

The *Trust Service Provider* treats all of the data it indicates in a *Certificate* as non-confidential information. Such data appear in the *Certificate Application* form linked to the service agreement in a clearly marked way.

The *Trust Service Provider* manages the revocation status of the end-user and intermediate provider *Certificate*s as public information and makes it available without restriction to the *Relying Parties* by publishing a *Certificate Revocation List* (CRL) and by providing online Certificate Status Protocol (OCSP) service. The disclosed information contains the serial number of the *Certificate*, the time of the revocation and optionally the reason for revocation. For more information, see section 7.2. and 7.3.

9.3.3 Responsibility to Protect Confidential Information

The *Trust Service Provider* is responsible for the protection of the confidential data it manages.

The *Trust Service Provider* obliges its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

The *Trust Service Provider* processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following case:

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the *Trust Service Provider* – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the *Trust Service Provider* according to the section (1) of the Eüt. [8] 90. § to investigating authorities and national security services free of charge.

  The *Trust Service Provider* records the fact of data transfers, but does not inform involved clients about it.

- **Provision of information in the scope of litigation**

  In the course of litigation and non-litigious actions under common law, the *Trust Service Provider* may hand over – in case their being affected is certified – *Subject* identity information and the information verified by the *Trust Service Provider*, to an adverse party or its representative, as well as it may disclose them to the inquiring court.

  The *Trust Service Provider* records the fact of data transfers and informs impacted clients about it.

- **Disclosure upon owner's request**

  Upon a *Client*'s personal request to do so or on the basis of its authorisation granted officially, in writing, the *Trust Service Provider* reveals confidential user information pertaining to the *Client* to third parties.

- **Miscellaneous circumstances resulting in the disclosure of information**

  Upon termination of its activity the *Trust Service Provider* is bound to hand over its records subject to the access obligations together with confidential user data to the trusted service provider that takes it over according to section (6) of 88. § Eüt. [8].

9.4 Privacy of Personal Information

The *Trust Service Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Trust Service Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [6] and the 2016/679 EU General Data Protection Regulation [2].

The *Trust Service Provider*:

- preserves,
- upon expiry of the obligation to retain – unless the *Client* otherwise indicates – deletes from the client database

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

The *Trust Service Provider* stores identification data, data about the *Subject* appearing in the *Certificate*, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.

The *Trust Service Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

9.4.1 Privacy Plan

The *Trust Service Provider* has a Privacy Policy and a Privacy Notice document, which contain detailed regulations on the handling of personal data.

The Privacy Policy is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/all-documents.html`

The Privacy Notice is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/privacynotice.html`

9.4.2 Information Treated as Private

The *Trust Service Provider* protects all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from the Certificate or other public data source.

9.4.3 Information Not Deemed Private

The *Trust Service Provider* may disclose the data of the *Subject*s indicated in the *Certificate* based on the written consent of the *Applicant*.

The *Trust Service Provider* may indicate the unique provider identifier assigned to the *Subject* in the *Certificate*.

9.4.4 Responsibility to Protect Private Information

The *Trust Service Provider* stores securely and protects the personal data related to the *Certificate* issuance and not indicated in the *Certificate*. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

9.4.5 Notice and Consent to Use Private Information

The *Trust Service Provider* only discloses personal data indicated in the *Certificate*s with the written consent of the *Client*.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the relevant legislation the *Trust 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 *Trust Service Provider* shall not harm any intellectual property rights of a third person.

The owner of the private and public key issued by the *Trust Service Provider* to clients is the *Subscriber* and the full user is the *Applicant* regardless of the physical media that contains and protects the keys.

The owner of the *Certificate* issued by the *Trust Service Provider* to its clients is the *Trust Service Provider* and its full user is the *Subscriber*.

The *Trust Service Provider* may publish, reproduce, revoke and manage the issued end-user *Certificate*s, 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 *Trust Service Provider* which is disclosed as defined in sections 7.2. and 7.3.

The unique provider identifier issued to the *Client*s by the *Trust Service Provider* is the property of the *Trust Service Provider* which

is disclosed as a part of the *Certificate* by the *Trust Service Provider* in the *Certificate Repository*.

The *Client* is entitled to the use of the identification in the certificate (which identifies the *Certificate* subject).

The present *Certification Practice Statement* is the exclusive property of the *Trust Service Provider*. The *Client*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Certification Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

The present *Certification Practice Statement* may be freely distributed in unchanged form, in full length and with the indication of origin.

The rules of the application of the software provided for the use of the service by the *Trust Service Provider* is accessible in the description of the software and it is included in the user's guide referenced in the description.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the *Trust Service Provider* is in the *Certification Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- the *Trust Service Provider* assumes responsibility that it validated that the *Applicant* either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the *Certificate*;
- The *Trust Service Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Trust Service Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;
- The *Trust Service Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [7] in relation to the *Client*s which are in a contractual relationship with it.
- The *Trust Service Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [7] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Trust Service Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8.).

- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Trust Service Provider* is not responsible:

- for the *Subject* activities related to the private key;
- for the certificate verification and usage activities of the *Relying Parties*;
- for the regulations issued by the *Relying Parties* or others.

Certification Authority Obligations

The *Trust 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 moreover to manage regulations.

The *Trust 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 Certificate Authority is responsible:

- for the authenticity and accuracy of the *Certificate*s it issued;
- for the regulations it has issued, and for their the 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*;
- in general for the compliance with its obligations.

9.6.2 RA Representations and Warranties

The customer service has the task of representing the *Trust Service Provider* at end-users in connection with the services. It performs the following tasks in the scope thereof:

- participates in selling the services;
- performs the registration of *Subject*s;
- receives requests pertaining to various certificate operations (revocation, reinstation, certificate replacement);
- receives and handles data modification related filings;
- participates in revocation status publication;
- offers information provision activity to *Client*s and *Relying Parties* in connection with its activities associated with the services provided by the *Trust Service Provider*;

The *Registration Authority* is responsible:

- for establishing the personal identity of *Applicant*s;
- for establishing the organisational identity of *Represented Organization*s, and in this latter case for establishing the right of representation of an individual acting in the name of a *Represented Organization*;
- for the genuineness of recorded registration data;
- for providing information to those using the services as to the contents and availability of the *Certificate Policy* and the *Certification Practice Statement*, as well as the terms and conditions of using the service prior to concluding the service agreement;
- in general to fully comply with its obligations.

9.6.3 Subscriber Representations and Warranties

Subscriber Responsibility

The responsibility of the *Subscriber* is set by the service agreement and its attachments (including the terms and conditions).

Subscriber Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *Trust Service Provider* while using the service including requesting and applying the *Certificate*s and private keys.

The obligations of the *Subscriber* are determined by this *Certification Practice Statement*, the service agreement, the General Terms and Conditions, as well as the relevant *Certificate Policy*.

When the *Subscriber* is informed about any actual or suspected misuse or compromise of the private key associated with the public key included in a *Certificate* belonging to the *Subscriber*, the *Subscriber* is obliged to

- promptly report this fact to the *Trust Service Provider*,
- promptly request the revocation of the *Certificate*,
- promptly cease using the *Certificate* and its associated private key.

The *Subscriber* may install the *Certificate* and its associated private key only on servers that are accessible at one of the domains or IP addresses listed in the subjectAltName(s) field in the *Certificate*, and to use the *Certificate* solely in compliance with all applicable laws and solely in accordance with the service agreement and the General Terms and Conditions.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *Certification Practice Statement*.
- *Subscriber*s are entitled to specify which *Subject*s should be allowed to receive *Certificate*s, in writing, and *Subscriber*s have the right to request the revocation of such *Certificate*s.
- *Subscriber*s have the right to request the revocation of *Certificate*s.
- *Subscriber*s are entitled to appoint *Organizational Administrator*s.

Applicant Responsibility

The *Applicant* is responsible for:

- the authentication, accuracy and validity of the data provided during registration;
- the verification of the data indicated in the requested *Certificate*;

- to provide immediate information on the changes of its data and the data indicated in the *Certificate*;
- using its private key and *Certificate* according the regulations;
- the secure management of its private key and activation code;
- for the immediate notification and for full information of the *Trust Service Provider* in cases of dispute;
- to generally comply with its obligations.

***Applicant* obligations**

The *Applicant* shall:

- read carefully this *Certification Practice Statement* before using the service;
- completely provide the data required by the *Trust Service Provider* necessary for using the service, and to provide truthful data;
- if the *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 *Trust Service Provider* in writing,
  - request the revocation of the *Certificate* and
  - terminate the usage of the *Certificate*;
- immediately terminate the usage of the private key belonging to the *Certificate*, if the *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;
- install the *Website Authentication Certificate* only to that servers which is accessible on the domain name 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 *Trust Service Provider* in writing and without delay in case a legal dispute starts in connection with the *Certificate*s associated with the service;
- cooperate with the *Trust 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;

- answer to the requests of the *Trust Service Provider* within the period of time determined by the *Trust Service Provider* in case of key compromise or the suspicion of illegal use arises;
- acknowledge that the *Subscriber*s entitled to request the revocation of the *Certificate*;
- acknowledge that the *Trust Service Provider* issues *Certificate*s in the manner specified in the *Certification Practice Statement*, upon the completion of the validation steps described therein;
- acknowledge that the *Trust Service Provider* only displays data that are corresponding to reality in issued *Certificate*s. Accordingly, the *Trust Service Provider* validates data to be entered in *Certificate*s according to the *Certification Practice Statement*;
- acknowledge that in case of requesting an *Organizational Certificate*, the *Trust 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 *Trust Service Provider* is entitled to revoke the issued *Certificate* immediately if
  - the *Trust 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 *Applicant* and in this case, the *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 the CABF Baseline Requirements, the *Trust Service Provider*'s *Certificate Policy* or *Certification Practice Statement*;
  - the *Trust Service Provider* becomes aware that the *Certificate* was used for an illegal activity activity (for example phishing, fraud, malware spreading);
  - the *Subscriber* fails to pay the fees of the services by the deadline.

***Applicant* Rights**

- *Applicant*s have the right to apply for *Certificate*s in accordance with the *Certification Practice Statement*.
- In case this is allowed by the applicable *Certificate Policy*, *Applicant*s are entitled to request the the revocation of their *Certificate*s, according to this *Certification Practice Statement*.

9.6.4 Relying Party Representations and Warranties

The *Relying Parties* decide based on their discretion and/or their policies about the way of accepting and using the *Certificate* . During the verification of the validity for keeping the security level guaranteed by the *Trust 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

Represented Organisation responsibility

The *Represented Organization* is solely responsible for the documents it issues. In particular for document in which it attests that a *Applicant* is a staff member of the *Trust Service Provider*, moreover is entitled to appear in the *Represented Organization*'s *Certificate*. In case the information appearing in any certification made out by the *Represented Organization* is changed, reporting this to the *Trust Service Provider* without delay is the *Represented Organization*'s responsibility.

Represented Organisation rights

- The *Trust Service Provider* only issues *Certificate*s in which the *Represented Organization*'s name is indicated in possession of the *Represented Organization*'s consent.
- The *Represented Organization* is entitled to revoke *Certificate*s in which the *Represented Organization*'s name was also indicated.

9.7 Disclaimers of Warranties

The *Trust Service Provider* excludes its liability if:

- the *Applicant*s do not follow the requirements related to the management 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 the National Media and Infocommunications Authority algorithmic decree.

9.8 Limitations of Liability

Conditions of liability of the *Trust Service Provider*:

- The *Trust Service Provider* is not responsible for damages that arise from the *Relying Party* failing to proceed as recommended according to effective legal regulations and the *Trust Service Provider*'s regulations in the course of validating and using certificates, moreover its failing to proceed as may be expected in the situation.
- The *Trust Service Provider* shall only be liable for contractual and non-contractual damages connected to its services in relation to third parties with respect to provable damages that occur solely on account of the chargeable violation of its obligations.
- The *Trust Service Provider* is not liable for damages that result from its inability to tend to its information provision and other communication related obligations due to the operational malfunction of the Internet or one of its components because of some kind of external incident beyond its control.
- If The *Trust Service Provider* engages data comparison with an authentic database before the issuance of the *Subject*'s *Certificate*, it relays on the data received from the authentic database. The *Trust Service Provider* will not assume any liability for damages arising out of the inaccuracy of information provided by such authentic databases.
- The *Trust Service Provider* assumes liability solely for providing the services in accordance with the provisions of this *Certification Practice Statement*, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

Administrative Processes

The *Trust Service Provider* logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

Financial Liability

The *Trust Service Provider* has liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

The *Trust Service Provider* limits the obligation for compensation related to services, the extent of this limitation is 4.000.000,-HUF per damage event.

If the valid claim of several entitled parties related to a damage event exceeds the limitation defined for a damage event, then the compensation of the claims takes place in a relative ratio to the limitation.

9.9 Indemnities

9.9.1 Indemnification by the *Trust Service Provider*

The detailed rules of the indemnities of the *Trust Service Provider* are specified in this regulation (see section: 9.8.), the service agreement and the contracts concluded with the *Client*s.

9.9.2 Indemnification by Subscribers

The *Subscriber* and the Subject are liable for damages to the *Trust Service Provider* for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3 Indemnification by Relying Parties

See section: 9.8.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific *Certification Practice Statement* is specified on the cover of the document.

9.10.2 Termination

The *Certification Practice Statement* is valid without a time limit until withdrawal or the issuance of the newer version of the *Certification Practice Statement*.

Section 9. of the *Certification Practice Statement* shall remain effective even after the termination of the *Certification Practice Statement*'s effect (regardless of the manner in which effectiveness is terminated) in connection with any and all *Certificate*s which the *Trust Service Provider* will have issued while the *Certification Practice Statement* was effective.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Certification Practice Statement* the *Trust Service Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

The *Trust Service Provider* guarantees that in case of a the *Certification Practice Statement* withdrawal, requirements for the protection of the confidential data remain in effect.

9.11 Individual Notices and Communications with Participants

The *Trust Service Provider* maintains a customer service in order to contact with its *Client*s.

The *Client*s may make their legal declarations to the *Trust Service Provider* solely in writing, and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

Issued *Certificate*s may also be revoked by sending an SMS. Notifications of other nature may also be given in writing, in the form of electronic mail or fax.

The e-Szignó Certificate Authority informs its *Client*s by means of publication on its webpage or in electronic mail.

9.12 Amendments

The *Trust Service Provider* reserves the right to change the *Certification Practice Statement* in a controlled way in case of the change of normative rules, security requirements, market conditions or other circumstances.

9.12.1 Procedure for Amendment

The *Trust Service Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Trust Service Provider* has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 8.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Trust Service Provider*'s organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certificate Authority.

The team produces internal, non-public working copies of the regulations as it collects changes, and these undergo internal review before being published. The *Trust Service Provider* strives to only issue new regulations at the least frequent intervals possible.

The *Trust Service Provider* reviews the *Certification Practice Statement* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change – or in case of the annual review even if no changes are made to the document – and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document will be published on the webpage of the *Trust Service Provider*.

9.12.2 Notification Mechanism and Period

The *Trust 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 *Trust Service Provider* issues the new version with a new version number even in the case of the smallest change to the *Certification Practice Statement*, in which either the main version number or the sub-version number changes depending on the extent of the change.

In versions 1.x and 2.x, the version number of the *Certification Practice Statement* appeared in the 2 tags at the end of the OID of the document identifier, so two *Certification Practice Statement* with different contents - brought into force - could not have the same OID identifier.

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

9.13 Dispute Resolution Provisions

The *Trust Service Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Trust Service Provider* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The *Client* in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the *Trust Service Provider* or the use of issued *Certificate*s shall be addressed to the customer care centre office in written form. The *Trust Service Provider* notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Trust Service Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Trust Service Provider* may request the provision of information required for giving a response from the submitter. The *Trust Service Provider* investigates complaints within 30 days, and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the *Trust Service Provider* involved, the submitter may initiate consultation with the *Trust Service Provider* and the *Relying Parties*. All participants of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof; and the submission, the *Trust Service Provider*'s response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The *Relying Parties* shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

9.14 Governing Law

The *Trust Service Provider* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Trust Service Provider* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

9.15 Compliance with Applicable Law

The applicable regulations:

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [6];
- (Hungarian) Act V of 2013. on the Civil Code. [7].
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [8];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [9];
- (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 [10];
- (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 [11];

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

Should some of the provisions of the present *Certification Practice Statement* become invalid for any reason, the remaining provisions will remain in effect unchanged.

In case of a conflict between national or EU legislation and the mandatory requirements of the CABF BR [42], the *Trust 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 *Trust 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 *Trust Service Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Certification Practice Statement*, it would waive the enforcement of claims for damages.

9.16.5 Force Majeure

The *Trust 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 *Trust Service Provider*.

9.17 Other Provisions

No stipulation.

A Interpretation of the short policy names

For the simplier handling of the *Certificate Policies* the *Trust Service Provider* defines a five characters long short name (identifier) for each *Certificate Policy*, where each character is meaningful and defines some basic feautures of the given policy according to the following rules:

- First character [?....]
  - M: qualified *Certificate Certificate Policy*
  - H: non-qualified, III. certificate class *Certificate Certificate Policy*
  - K: non-qualified, II. certificate class *Certificate Certificate Policy*
  - A: non-qualified, automatic issuance *Certificate Certificate Policy*
  - x: no stipulation
- Second character [.?...]
  - A: Signing purpose *Certificate Certificate Policy*
  - B: Seal creation purpose *Certificate Certificate Policy*
  - W: *Website Authentication Certificate Certificate Policy*
  - K: *Code Signing Certificate Certificate Policy*
  - S: *Email (S/MIME) Certificate Certificate Policy*
  - E: Other purpose *Certificate Certificate Policy*
- Third character [..?..]
  - T: *Certificate* issued to a natural person *Certificate Policy*
  - J: *Certificate* issued to a legal person *Certificate Policy*
  - x: no stipulation, can be issued to any type of *Subject*
- Fourth character [...?.]
  - B: *Certificate* issued on *Qualified Electronic Signature Creation Device Certificate Policy*
  - H: *Certificate* issued on *Cryptographic Hardware Device Certificate Policy*
  - S: *Certificate* issued by software *Certificate Policy*
  - x: no stipulation, it can be issued on any platforms
- Fifth character [....?]
  - A: pseudonymous *Certificate Certificate Policy*
  - N: pseudonym excluding *Certificate Certificate Policy*

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] 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) .

[3] (Hungarian) Act LXVI of 1992 on the registration of citizens' personal data and address .

[4] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

[5] (Hungarian) Act II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[6] (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information .

[7] (Hungarian) Act V of 2013. on the Civil Code .

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

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

[10] (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 .

[11] (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 .

[12] (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.

[13] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[14] ETSI EN 319 411-1 V1.4.1 (2023-10); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[15] ETSI EN 319 412-1 V1.4.4 (2021-05); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[16] ETSI EN 319 412-2 V2.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[17] ETSI EN 319 412-3 V1.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[18] ETSI EN 319 412-4 V1.2.1 (2021-11); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

[19] ETSI TS 119 312 V1.4.3 (2023-08); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[20] ETSI TS 119 461 V1.1.1 (2021-07) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.

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

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

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

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

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

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

[27] IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.

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

[29] IETF RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environment, September 2007.

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

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

[32] IETF RFC 6532: Internationalized Email Headers, February 2012.

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

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

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

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

[37] IETF RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension, November 2020.

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

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

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

[41] CA/Browser Forum Network and Certificate System Security Requirements, v.1.7. CA/Browser Forum, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Controls-v1. , 2021.

[42] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted tls server Certificates, v.2.0.2. CA/Browser Forum, https://cabforum.org/baseline-requirements-documents/ , 2024.

[43] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates, v.1.0.2. CA/Browser Forum, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.2.pdf , 2023.

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

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

[46] NIST Special Publication 800-56A Revision 3 (April 2018): Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

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

[48] EU Trusted Lists of Certification Service Providers, (https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-provide

[49] Magyarország (Hungary): Trusted List (http://www.nmhh.hu/tl/pub/HU_TL.pdf).

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

[51] e-Szignó Certification Authority - eIDAS conform Certificate for Website Authentication Certificate Policies.

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

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