# e-Szignó Certificate Authority

# eIDAS conform
# Certificate for Website Authentication
# Certificate Policies

**ver. 3.3**

**Date of effect: 2022-11-30**

| | |
|---|---|
| OID | 1.3.6.1.4.1.21528.2.1.1.159,<br>1.3.6.1.4.1.21528.2.1.1.161,<br>1.3.6.1.4.1.21528.2.1.1.162 |
| Version | 3.3 |
| First version date of effect | 2016-07-01 |
| Security classification | PUBLIC |
| Approved by | Gergely Vanczák |
| Date of approval | 2022-11-24 |
| Date of effect | 2022-11-30 |

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. |
| 2.4 | 2017-09-30 | - Yearly revision. |
| 2.6 | 2018-03-24 | - Global revision.<br>- Changes in the domain validation methods.<br>- Introducing identity validation by state notaries.<br>- 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.<br>- 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.<br>- Identity validation rules.<br>- Certificate modification.<br>- HSM requirements.<br>- Smaller improvements of wording. |
| 2.14 | 2020-05-26 | - Smaller improvements.<br>- Add High Risk Certificate Report to Section 1.5.2.<br>- Restructuring Chapter 2.<br>- Adding more information for revocation in chapter 4.9.<br>- Improve section 9.4. |
| 2.16 | 2020-08-14 | - Smaller improvements.<br>- Remove OCSP Signing EKU from ICA certificates.<br>- Certificate lifetime is 398 days. |
| 2.17 | 2020-10-28 | - Smaller improvements.<br>- New domain validation possibility.<br>- Improvements according to the auditor's and the supervisory body's findings. |

| Version | Effect date | Description |
|---|---|---|
| 2.19 | 2020-12-28 | - Smaller improvements.<br>- More detailed rules for the Certificate renewal initiated by the Service Provider. |
| 2.20 | 2021-03-03 | - Smaller improvements.<br>- Introduction of video-based natural person identification in Section 3.2.3.<br>- Upgrading the rules for the generation of service provider's key pairs in the section 6.1.1.<br>- Upgrading the description of the CRL profile in the section 7.2. |
| 2.22 | 2021-06-30 | - Smaller improvements.<br>- Certificate types.<br>- Who can initiate revocation.<br>- Reporting key compromise.<br>- Publication of conformity assessment results. |
| 2.24 | 2021-11-30 | - Smaller improvements.<br>- subjectAltName, commonName and Organizational Unit fields requirements.<br>- Change in BR 3.2.2.4.18 Validation method.<br>- HSM certification. |
| 2.25 | 2022-03-31 | - Revision.<br>- Specifying term dual control.<br>- Introducing new SN fields.<br>- KASZ based identity validation.<br>- Upgrade the rules of electronic signature acceptance.<br>- QWAC policy change.<br>- Depreciating OU field. |
| 3.1 | 2022-08-31 | - Global revision.<br>- Change in policy OID generation rules.<br>- Managing revocation reasons.<br>- ETSI TS 119 461 conformity. |

| Version | Effect date | Description |
|---|---|---|
| 3.3 | 2022-11-30 | - Global revision.<br>- Contact person.<br>- Customer Portal.<br>- Change in policy OID generation rules. |

# Table of Contents

# 1 Introduction

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

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

## 1.1 Overview

The *Certificate Policy* is a "set of rules that specify a *Certificate*'s usability for a community and/or a class of applications with common security requirements". The content and format of this document complies with the requirements of the IETF RFC 3647 [25] framework. It consists of 9 sections that contain the security requirements, processes and the practices defined by the *Trust Service Provider* to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, section headings where the *Certificate Policy* does not impose a requirement have the statement "No stipulation".

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

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

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

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

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

## 1.2 Document Name and Identification

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

| | |
|---|---|
| Issuer | e-Szignó Certificate Authority |
| Document name | eIDAS conform<br>Certificate for Website Authentication<br>Certificate Policies |
| Document version | 3.3 |
| Date of effect | 2022-11-30 |

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

### 1.2.1 Certificate Policies

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

The first seven numbers of the OID identifying the *Certificate 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 |

The present document defines the following *Certificate Policies*:

| OID | DENOMINATION | SHORT NAME |
|---|---|---|
| 1.3.6.1.4.1.21528.2.1.1.159 | certification class III., for website authentication certificates, prohibiting the use of pseudonyms. | HWJSN |
| 1.3.6.1.4.1.21528.2.1.1.161 | certification class II., for website authentication certificates, prohibiting the use of pseudonyms. | KWJSN, KWTSN |
| 1.3.6.1.4.1.21528.2.1.1.162 | Issued during automatic issuance, controlling website authentication certificate issuance, Certificate Policy 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.

Based on these *Certificate Policies* the *Trust Service Provider* can issue *Certificate*s used for webserver authentication.

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.

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [LCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [13] standard;
- each *Certificate Policy* complies with the [DVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [13] standard;
- each *Certificate Policy* complies with the [OVCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [13] 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 [13] 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

This *Certificate Policy* collection is in effect from the 2022-11-30 date of entry into force to withdrawal. The effect automatically terminates at the issuance of the newer version of the *Certificate Policy*.

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

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

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

### 1.2.3 Security Levels

The *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

### 1.3.1 Certification Authorities

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

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

### 1.3.2 Registration Authorities

See the definition in section 1.6.

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

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

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

### 1.3.3 Subscribers

*Subscriber*s define the scope of *Applicant*s using the service, and *Subscriber*s also cover the service fees related to the usage of these services.

The *Applicant* is that natural person, who acts during the application for *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* and the other policies mentioned in it contain the recommendations related to its operation.

### 1.3.5 Other Participants

The independent auditor who makes the conformity assessment audit.

The supervisory authority.

## 1.4 Certificate Usage

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

### 1.4.1 Appropriate Certificate Uses

The private keys belonging to the end-user *Certificate*s issued by the *Trust Service Provider* based on one of the present *Certificate Policies* 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.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

The data of the organization administering the present *Certificate Policy* can be found in the following table:

| | |
|---|---|
| Organization name | Microsec e-Szignó 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 *Certificate Policy* 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* shall maintain a continuous 24x7 ability to respond internally to a High Piority Certificate Problem Report. The *Certification Practice Statement* shall contain the way how to issue the report.

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

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

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

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

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

| | |
|---|---|
| II. certification class | A group of non-qualified *Certificate Policies*, that make possible the *Certificate* issuance based on the *Applicant*'s remote registration. |
| III. certification class | A group of non-qualified *Certificate Policies*, that bound the *Certificate* issuance to the *Applicant*'s personal registration. |
| 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. |
| Trust Service Supervisory Body | "The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [7] 91.§ 1. paragraph)* |

| | |
|---|---|
| Trust Service | "Means an electronic service normally provided for remuneration which consists of:<br>• 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<br>• the creation, verification and validation of *Website Authentication Certificate*; or<br>• the preservation of electronic signatures, seals or certificates related to those services;<br>" *(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. [7] 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 [34], 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 [34], 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. [7] 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<br>*Applicant* shall keep strictly secret.<br>In case of webserver authentication the webserver shall use its private key during its authentication procedure.<br>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.<br>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. [7] 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. [7] 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. [7] 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.<br>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.)*<br>The webserver domain name or IP address<br>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 |
| 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* shall disclose the contractual conditions and policies electronically on its website.

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

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

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

After concluding the contract, the *Trust Service Provider* shall make the individual Service Agreement, the General Terms and Conditions, the *Disclosure Statement*, the *Certificate Policy* and the *Certification Practice Statement* available to the *Client* on a durable medium, or in a way that can be downloaded to the *Client*.

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

## 2.2 Publication of Certification Information

The *Trust Service Provider* shall disclose on its webpage

- its provider *Certificate*s;

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

**Service Provider Certificates**

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

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

**End-User Certificates**

With the following methods the *Trust Service Provider* shall disclose 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

shall be 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. For status information disclosing methods, see Section 4.10.

The *Trust Service Provider* shall guarantee, 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 99.9% per year, while service downtimes may not exceed at most 3 hours in each case.

The *Trust Service Provider* shall publish through known Certificate Transparency Log providers those *PreCertificate*s, the publication of which is consented by the *Applicant*.

## 2.3 Time or Frequency of Publication

### 2.3.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the service are contained in the service contract to be signed by the *Client* during the conclusion of the contract, or in the General Terms and Conditions [44] 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, shall follow the practices below:

- the *Certificate*s of the root certification units operated by it shall be disclosed before commencing the service;
- the *Certificate*s of the intermediate certification units operated by it shall be disclosed within 5 workdays after issuance;
- the *Trust Service Provider* shall publish the *PreCertificate* corresponding to the enduser *Certificate* before the issuance of the *Certificate* through CT Log providers;
- the *Trust Service Provider* shall disclose the end-user Certificates in its *Certificate Repository* after issuance without delay.

### 2.3.3 The Changed Revocation Status Publication Frequency

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

The information related to the status of the *Certificate*s shall be disclosed in the Certificate Repository and on the *Certificate Revocation List*s. The requirements related to the issuance of the *Certificate Revocation List*s are discussed in Section 4.10. The requirements 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 shall be 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* shall prevent 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 present *Certificate Policies*.

The indicated Issuer ID and the Subject ID amongst the basic fields of the Certificate shall comply with the ITU X.520 standard [39], the RCF 5280 [29] and IETF RFC 6818 [32] recommendations name-specific format requirements, in addition the *Trust Service Provider* shall support the "Subject Alternative Names" and "Issuer Alternative Names" fields located amongst the extension.

### 3.1.1 Types of Names

**Denomination of the *Subject***

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

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

  If present, this field shall contain exactly one entry that is one of the values contained in the *Certificate*'s "Subject Alternative Names" extension.

  The value of the field shall be encoded as follows:

  **IPv4 address** :
  If the value is an IPv4 address, then the value shall be encoded as an "IPv4Address" as specified in RFC 3986 [27], 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 [30], Section 4. pg. 81

  **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 "subjectAltName" 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.

  Usage is optional.

  Only that domain name or IP address can be 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* shall be in this field.

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

- 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* shall be in this field.

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

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

  It shall not be filled.

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

  It shall not be filled.

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

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

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

  The indication of at least one filled out "Serial Number" field is compulsory, in the *Certificate* which complies with the following requirements, so that it is able to form a part of the *Subject* permanent unique identifier in case of the usage of "Permanent Identifier" extension according to the IETF RFC 4043 [28] recommendation:

  – the identifier value belongs to the *Subject* named in the *Certificate*, identified by the *Trust Service Provider*, and it is unique within the system of the *Trust Service Provider*;
  – the *Trust Service Provider* guarantees that the identifier value of any two *Certificate*s it issued only matches with each other, if both of the *Certificate*s belong to the same *Subject*.

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

- 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* shall be 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 shall not be filled.

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

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

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

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

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

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

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

  This field shall 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 [21] - of the country belonging to the domain or IP address , 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 [21] - 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 [21] - of the address of the natural person named in the "SN" and "GN" fields.

  Filling out is required.

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

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

  In case of DVCP *Certificate* it shall not be filled.

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

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

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

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

  In case of DVCP *Certificate* it shall not be filled.

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

  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 shall not be filled.

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

  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 shall not be filled.

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

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

  Shall not be filled.

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

  Shall not be filled.

The *Certificate*s issued in accordance with the present *Certificate Policies* might contain further "Subject DN" fields. Only verified text values may be indicated on these fields (they shall not contain values indicating lack of data for example: ".", "-" or " ").

**Extensions**

- Subject Alternative Names - "Subject Alternative Names"

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

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

  Filling is required.

  Each entry shall be 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" field 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 [29], and thus shall not contain domain name containing underscore ("_") character.

### 3.1.2 Need for Names to be Meaningful

The following rules shall be 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* shall have a unique name in the *Certificate Repository* of the *Trust Service Provider*. In order to ensure the uniqueness, the *Trust Service Provider* shall give 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.

#### Procedures to Resolve Disputes Relating the Names

The *Trust Service Provider* shall ensure 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

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

## 3.2 Initial Identity Validation

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

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

### 3.2.2 Authentication of an Organization Identity or a Domain

#### 3.2.2.1 Authentication of organization identity

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

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

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

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

The *Certification Practice Statement* shall determine the detailed procedural rules.

#### 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* shall ensure 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* shall ensure that, the *Applicant* is the authorized user of the entire domain namespace covered by the wildcard domain name. The *Trust Service Provider* shall not issue a *Certificate*, in which the domain name space to be covered by the wildcard domain name is a registered gTLD or ccTLD (for example: "*.com", "*.co.uk"), or a subdomain under these TLDs under which public domain name registration is directly possible.

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

The *Trust Service Provider* shall support the usage of the Internationalized Domain Names according to the IDNA2003 [24] requirements.

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 [40].

#### 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 Random Value shall be sent 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 shall be 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 shall remain valid for use in a confirming response for no more than 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 shall be 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 shall remain valid for use in a confirming response for no more than 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 Random Value or Request Token either in a DNS CNAME, TXT or CAA record for either

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

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

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

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 must be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set must be found using the search algorithm defined in IETF RFC 8659 [35] Section 3.

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 shall be unique in each email. The Random Value shall remain valid for use in a confirming response for no more than 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 must be 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 [31] 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 shall be unique in each email. The Random Value shall remain valid for use in a confirming response for no more than 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 shall remain valid for use in a confirming response for no more than 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 [26] 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 shall remain valid for use in a confirming response for no more than 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 [35] 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 [26] section 5.1.4, or it cannot be used. Global Numbers shall have a preceding + and a country code and may contain visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

$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 shall remain valid for use in a confirming response for no more than 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* shall not accept redirects (3xx HTTP status code).
The Random Value included in the Request Token:

- shall be unique to each *Certificate Application*;
- may remain valid for use in a confirming response for no more than 30 days from its creation.

The *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* shall verify 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.
   - during the personal identification the identity of the natural person shall be verified based on a suitable official proof of identity card;

     The identification can be based on the following official documents:
     - in case of natural persons within the scope of Act LXVI. of 1992. (henceforth: Nytv. [3]) official cards appropriate for verifying identity defined in Nytv. in accordance with Eüt. 82.§ (3) [7];
     - 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 [4] in accordance with Eüt. 82.§ (4) [7];
     - 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) [7] only in the case of identifying European citizens. In such case a personal identity card with a photo 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 shall verify, 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 identification data shall be checked by the *Registration Authority* with the help of a trusted third party or an authentic public register.
- The *Registration Authority* shall verify the authenticity of the presented cards. The *Trust Service Provider* shall verify that the *Certificate Application* was really sent by the identified *Applicant* through a trustable communication channel.

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

   In this case:

   - The *Applicant* submits the *Certificate Application* in electronic form with 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 [11], 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" [45] 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" [45] 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 [7] 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* can provide opportunity for new *Certificate* issuance based on the reconciled data of the *Applicant* in the case of a *Certificate Application* during the validity period

of the service agreement. The authenticity of the *Certificate Application*, the accuracy of the data to be in the *Certificate* and the identity of the person making the application shall also be checked. The verification process shall be precisely determined in the *Certification Practice Statement*.

### 3.2.4 Non-Verified Subscriber Information

Only that data can be in the *Certificate* issued by the *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.

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

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

### 3.2.6 Criteria for Interoperation

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

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

The collaborating *Trust Service Provider*s shall define the method of the collaboration in the *Certification Practice Statement*s.

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

The *Trust Service Provider* shall disclose its entire cross-certified *Certificate*s it sought or accepted.

## 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* may accept 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* shall take place as described in section 3.2.3.

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

### 3.3.2 Identification and Authentication for invalid Certificate

The *Trust Service Provider* can accept re-key requests only during the service provision time. The identification of the *Applicant* shall take place as described in section 3.2.3.

## 3.4 Identification and Authentication in Case of Certificate Renewal Requests

*Certificate* renewal is the process when the *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* shall take 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* shall not 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* shall take place as described in section 3.2.3.

If the modified *Certificate* expires on the same time as the original *Certificate*, during the procedure, the *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* shall not be renewed.

### 3.6 Identification and Authentication for Revocation Request

The *Trust Service Provider* shall receive and process 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* shall ensure that the besides the rapid processing of the suspension and revocation requests , the requests only get accepted from authorized parties.

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

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

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

## 4 Certificate Life-Cycle Operational Requirements

### 4.1 Application for a Certificate

For each new *Certificate* issuance, *Certificate Application* submission is required. Prior to submitting the first *Certificate Application*, the *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* shall not 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* may prepare the *Subscriber*'s service agreement based on the information given in the *Registration Application*.

The *Trust Service Provider* shall inform 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 shall also be given to the *Applicant*.

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

The *Certificate Application* shall at least include the data below:

- 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);
- the contact of the *Applicant* (telephone number, email address);
- in case of *Organizational Certificate* application, the data of the *Organization* (official name);
- the *Subscriber*'s data (billing information);

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

- documents necessary to identify the *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* ;

### 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* shall ascertain the identity of the person submitting the *Certificate Application* (see section 3.2.3).

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

In case of *Organizational Certificate* application the *Organization* shall be identified too, and it shall be ensured, that the person appeared is entitled to represent the *Organization* and to request a *Certificate* related to the *Organization* (see section: 3.2.2.).

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

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

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

- a confirmation, that the data provided in the *Certificate Application* are accurate;
- a consent, that the *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 aforementioned records shall be kept 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 the *Subject*'s association to the *Represented Organization* can not be verified without a doubt, or any of the indicated data on the *Certificate Application* form is incorrect, then the *Certificate Application* procedure is aborted. Then the *Client* has the opportunity to correct incomplete or erroneous data, and hand over the missing documents.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

The *Trust Service Provider* shall identify the *Applicant* according to Section 3.2.

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

### 4.2.2 Approval or Rejection of Certificate Applications

To avoid any conflicts of interests, the *Trust Service Provider* shall ensure 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* shall verify the authenticity of all the information provided in the *Certificate Application* to be indicated in the *Certificate* before issuing the *Certificate*.

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

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

### 4.2.3 Time to Process Certificate Applications

The *Trust Service Provider* shall define in the *Certification Practice Statement* the time limit within which it undertakes the evaluation of the *Certificate Application*.

## 4.3 Certificate Issuance

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

### 4.3.1 CA Actions During Certificate Issuance

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

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

### 4.3.2 Notification of the Subscriber about the Issuance of the Certificate

The *Trust Service Provider* shall inform the *Applicant* and the *Subscriber* about the issuance of the *Certificate* and shall enable 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* before 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

The *Trust Service Provider* shall disclose the issued *Certificate* after handing over the *Certificate*.
The condition for disclosure is the consent of the affected *Subject*.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

In case of an Organizational *Certificate* the contact of the *Represented Organization* shall be notified on the *Certificate* issuance.

## 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 and to meet the requirements described in the *Certification Practice Statement*, particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- 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 *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

The *Trust Service Provider* shall make 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.
The *Trust Service Provider* can limit the types of *Certificate*s involved in the Certificate renewal in its *Certification Practice Statement*.

### 4.6.1 Circumstances for Certificate Renewal

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

- the *Certificate* renewal request was submitted within the validity period of the *Certificate*;
- the *Certificate* to be renewed is not 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.

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

### 4.6.2 Who May Request Renewal

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

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

The *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* shall verify that:

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;

- the submitter of the *Certificate* renewal application stated that the data of the *Subject* to be indicated in the *Certificate* are unchanged and accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;
- the *Certificate* to be renewed is not 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* shall inform the *Applicant* and the *Subscriber* about the *Certificate* issuance.

### 4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

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

### 4.6.6 Publication of the Renewed Certificate by the CA

The *Trust Service Provider* shall disclose the renewed *Certificate* the same method as the original *Certificate*.

### 4.6.7 Notification of Other Entities about the Certificate Issuance

In case of an *Organizational Certificate* the contact of the *Represented Organization* shall be notified on the *Certificate* issuance.

## 4.7 Certificate Re-Key

*Re-key* means the process when the *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* shall be 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 shall also be given to the *Subscriber*.

### 4.7.2 Who May Request Certification of a New Public Key

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

### 4.7.3 Processing Certificate Re-Key Requests

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

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

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

### 4.7.4 Notification of the Client about the New Certificate Issuance

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

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The *Trust Service Provider* shall hand 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* shall disclose the re-keyed *Certificate* the same way as the original *Certificate*.

### 4.7.7 Notification of Other Entities about the Certificate Issuance

In case of an *Organizational Certificate* the contact of the *Represented Organization* shall be notified on the *Certificate* issuance.

## 4.8 Certificate Modification

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

### 4.8.1 Circumstances for Certificate Modification

*Certificate modification* becomes necessary in the following cases:

- change of data indicated in the *Subject*'s *Certificate*;
- in the *Certificate* issuing system of the *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* shall only accept a *Certificate* modification application within the effect of the service agreement.

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

### 4.8.2 Who May Request Certificate Modification

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

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

### 4.8.3 Processing Certificate Modification Requests

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

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the data given in the application are accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;

- based on the currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the *Certificate* to be issued.

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

### 4.8.4 Notification of the Client about the New Certificate Issuance

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

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

### 4.8.6 Publication of the Modified Certificate by the CA

The *Trust Service Provider* shall disclose the modified *Certificate* the same way as the original *Certificate*.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

In case of an *Organizational Certificate* the contact of the *Represented Organization* shall be notified on the *Certificate* issuance.

## 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.

### 4.9.1 Circumstances for Revocation

**Reasons for Revoking a Subscriber Certificate**

*Certification Authority* shall revoke the end-user *Certificate* in the following cases:

- the *Applicant* or the *Subscriber* requests the revocation of the *Certificate* in writing;
- the *Applicant* or the *Subscriber* notifies *Certification Authority* that the *Certificate Application* is not approved and subsequently the approval is not given;
- the *Certification Authority* becomes aware that the private key corresponding to the public key in the *Certificate* has been compromised;

- 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;
- 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 *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;
- 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);
- the *Certification Authority* becomes aware that the wildcard certificate was used for deceptive domain name authentication;
- the *Certification Authority* is made aware of a material change in the information contained in the *Certificate*;
- the *Certificate* modification because of data change referring to the *Subject*;
- 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*;
- the *Certification Authority* becomes aware that any of the data appearing in the *Certificate* is inaccurate;
- the *Certification Authority* is no longer entitled to issue *Certificate*s, and maintenance is not provided for the existing CRL and OCSP services;
- the revocation is required by the *Certification Authority*'s *Certificate Policy* or the *Certification Practice Statement*;
- the *Certification Authority* is made aware of a demonstrated or proven method that exposes the *Subscriber*'s private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see `http://wiki.debian.org/SSLkeys`), or if there is clear evidence that the specific method used to generate the private key was flawed.
- 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* becomes aware that the private key of the *Certificate* issuer certification unit might be compromised;
- the *Certification Authority* becomes aware that the *Subscriber* failed to fulfil any of its financial obligations according to the service agreement;

- the *Certification Authority* has terminated its activities;
- the supervisory body enacts (smth.) in a legally binding and executable decision;
- the law makes revocation mandatory.

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

**Reasons for Revoking a Subordinate CA Certificate**

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

- the CA operating the 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.

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

**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*;
- 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.

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

### 4.9.2 Who Can Request Revocation

The revocation of the *Certificate* may be requested in writing by the *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 shall be able to 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* shall provide clear instructions on how to report suspected Private Key Compromise, *Certificate* misuse, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to *Certificate*s on a publicly available way.

### 4.9.3 Procedure for Revocation Request

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

- **Through the website of the *Trust Service Provider* 24 hours a day**

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

- **Sent by email, with an electronic signature or electronic seal**

  in electronic form with an electronic signature or electronic seal based on a non-pseudonymous *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**

  on paper signed manually at the customer service of the *Trust Service Provider* during office hours in person, or sent by post. In the submitted application, the applicant must select the revocation reason from the list below:

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

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

In case of invalid or incomplete revocation request the *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* shall notify the *Subject* and the *Subscriber* about the revocation.

#### High-Priority Certificate Problem Report

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

### 4.9.4 Revocation Request Grace Period

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

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

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

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

The *Trust Service Provider* shall revoke 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* shall issue a new *Certificate Revocation List* for its end user *Certificate*s at least once a day.

The validity of these *Certificate Revocation List*s shall be maximum 26 hours.

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

### 4.9.8 Maximum Latency for CRLs

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

### 4.9.9 Online Revocation/Status Checking Availability

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

### 4.9.10 Online Revocation Checking Requirements

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

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

### 4.9.12 Special Requirements for Key Compromise

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

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

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

### 4.9.13 Circumstances for Suspension

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* shall provide the following possibilities for the *Certificate* revocation status query:

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

The revoked *Certificate*s shall be listed in the *Certificate Revocation List*s.

The revocation information shall not be removed from the *Certificate Revocation List* until after the expiry date of the revoked *Certificate*.

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

In case of revocation the new status of the *Certificate* shall appear immediately in the revocation records of *Trust Service Provider* after the successful completion of the process.

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

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

OCSP response issued by the *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

No stipulation.

### 4.10.2 Service Availability

The *Trust Service Provider* shall ensure 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 99.9% per year, and the length of downtime shall not exceed at most 3 hours.

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

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

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

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

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

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

## 5.1 Physical Controls

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

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

Services that process critical and sensitive information shall be implemented at secure locations.

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

### 5.1.1 Site Location and Construction

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

### 5.1.2 Physical Access

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

*Trust Service Provider* shall ensure 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 should be physically out of reach;
- the logged-in terminals shall not be left without supervision;
- no work process should be carried out during which confidential information may be revealed.

When leaving the computer room the administrator shall verify that:

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

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

### 5.1.3 Power and Air Conditioning

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

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems;
- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other;
- in 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 shall be ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system should provide the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

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

Cooling systems with proper performance should be used to provide the necessary operating temperature, to prevent overheating of IT devices.

### 5.1.4 Water Exposures

The *Data Centre* of the *Trust Service Provider* shall be adequately protected from water intrusion and flooding.

### 5.1.5 Fire Prevention and Protection

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

### 5.1.6 Media Storage

The *Trust Service Provider* shall protect its media storages from unauthorized access and accidental damage. All audit and archive data shall be created in duplicate. The two copies should be stored separately from each other physically, at locations in a safe distance from each other. The stored media storages shall be protected from damaging environmental influences such as low or high temperatures, dirt, moisture, sunlight, strong magnetic fields, strong radiation.

### 5.1.7 Waste Disposal

The *Trust Service Provider* shall take care of the destruction of its devices, media storages becoming superfluous in compliance with environmental regulations.

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

### 5.1.8 Off-Site Backup

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

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

## 5.2 Procedural Controls

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

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

The *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 shall be 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* shall create trusted roles (in the wording of the regulation, scope of activities) according to the requirements of decree 24/2016. [8] for the performance of its tasks. The rights and functions shall be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

Trusted roles to be implemented:

- manager with overall responsibility for the provider's IT system;
- security officer: individual with overall responsibility for the security of the service;
- system administrator: individual performing the IT system installation, configuration and maintenance;
- operator: individual performing the IT system's continuous operation, backup and restore;
- independent system auditor: individual who audits the logged, as well as archived dataset of the provider , responsible for verifying the enforcement of control measures the provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.
- registration officer: responsible for the approval of production, issuance and revocation of end-user certificates

For the provision of trusted roles the manager responsible for the security of the *Trust Service Provider* shall formally appoint 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 shall be kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority shall be notified without delay.

### 5.2.2 Number of Persons Required per Task

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

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

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

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

### 5.2.4 Roles Requiring Separation of Duties

Employees of the *Trust Service Provider* can hold multiple trusted roles at the same time, but the *Trust Service Provider* is bound to ensure that:

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

## 5.3 Personnel Controls

The *Trust Service Provider* shall take 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* shall address personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants shall have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties who get in contact with the *Trust Service Provider*'s services shall sign a non-disclosure agreement.

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

### 5.3.1 Qualifications, Experience, and Clearance Requirements

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

Trusted roles can be held at the *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* shall only hire employees for trusted or leading roles, who

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

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

### 5.3.3 Training Requirements

The *Trust Service Provider* shall train the newly recruited employees, over the course of which they acquire

- basic PKI knowledge;
- the specifics and the way of handling the *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* shall train the employees concerned with registration about the dangers and risks related to the verification of the data to be indicated on the Certificate.

The employees concerned with registration shall take and pass an exam on the knowledge of the related requirements and procedures for data verification before their appointment, and this fact shall be documented.

Only employees having passed the training shall gain access to the he production IT system of the *Trust Service Provider*.

### 5.3.4 Retraining Frequency and Requirements

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

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

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

The training shall be adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Actions

The *Trust Service Provider* shall regulate the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *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.

### 5.3.7 Independent Contractor Requirements

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

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

### 5.3.8 Documentation Supplied to Personnel

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

## 5.4 Audit Logging Procedures

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

### 5.4.1 Types of Events Recorded

The *Trust Service Provider* shall log every security-related event that can provide information on events, changes happened in the IT system or in its physical environment according to the generally accepted information security practice. In case of every log entry, the following data shall be stored:

- the time of the event;
- the type of the event;
- the identification of the user or the system who/what triggered the event;
- the success or failure of the audited event.

The audit records shall not be modified or deleted.

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

The following events shall be logged at minimum:

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- LOGGING:
  - the shutdown, restart of the logging system or some of its components;
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
  - the modification or deletion of the stored logging data;
  - the activities performed because of the logging system's failure.
- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles;
  - in case of password based authentication:

    - ∗ the change of the number of permitted unsuccessful attempts;
    - ∗ reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
    - ∗ readmission of the user blocked because of the unsuccessful login attempts;
  - changing the authentication technique ( for example from password based to PKI based).

- KEY MANAGEMENT:
  - all events for the entire life cycle of service keys (key generation, saving, loading, destruction etc.);
  - events related to generating, managing the user keys;
  - all events related to the management of private keys stored for any purpose by the *Trust Service Provider*.

- 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 *Trust Service Provider* shall ensure the regular evaluation of the created logs.

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

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

The *Trust Service Provider* can use automatized tools to assist the evaluation of the electronic logs. The notifications received from the automatized monitoring tools shall be processed and evaluated within 24 hours.

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

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

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

### 5.4.3 Retention Period for Audit Log

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

### 5.4.4 Protection of Audit Log

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

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

### 5.4.5 Audit Log Backup Procedures

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

The daily log files shall be archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups shall be defined in the *Certification Practice Statement*.

### 5.4.6 Audit Collection System (Internal vs External)

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

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

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

### 5.4.7 Notification to Event-causing Subject

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

### 5.4.8 Vulnerability Assessments

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

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

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

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

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

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

The *Trust Service Provider* shall archive 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* is bound to preserve the archived data for the time periods below:

- the *Certificate Policy* for at least 10 years from the date of repeal;
- *Certification Practice Statement* for at least 10 years from the date of repeal;
- General Terms and Conditions for at least 10 years from the date of repeal;
- in the case of video identification, all communications recorded during the identification for at least 10 years from the date of recording;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate;
- 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* is bound to store every archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy can be made in accordance with the applicable law from the only authentic paper based copy of the document available.

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

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

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

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

### 5.5.4 Archive Backup Procedures

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

### 5.5.5 Requirements for Time Stamping of Records

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

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

The daily log files shall be provided with a *Time Stamp*.

During the preservation of the archived data, if necessary (for example algorithm change expiration of the original *Time Stamp*) the authenticity of the data shall be ensured.

### 5.5.6 Archive Collection System (Internal or External)

The log entries shall be generated in the *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.

### 5.5.7 Procedures to Obtain and Verify Archive Information

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

The archived files shall be protected from unauthorized access.

Controlled access to the archived data shall be available to the eligible persons:

- *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* shall ensure that the used *Certification Unit*s are continuously having the valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it shall generate a new key pair for the *Certification Unit*s , and inform its Clients in time. The new provider key shall be 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 shall comply with the following requirements:

- it shall disclose the affected Certificates and public keys in accordance with the requirements defined in section 2.2 ;

- after the provider re-key the end-user *Certificate*s to be issued can only be signed with the new provider keys;
- it shall preserve its old Certificates and public keys.

## 5.7 Compromise and Disaster Recovery

In case of a disaster, the *Trust Service Provider* is obliged to take all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it shall take the necessary amendments, corrective measures to prevent future occurrence of the incident.

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

### 5.7.1 Incident and Compromise Handling Procedures

The *Trust Service Provider* shall have a business continuity plan.

The *Trust Service Provider* shall establish and maintain a fully functional backup system, which is at a safe distance from the primary location, geographically located at a different place and is independently capable of supplying the full range of services.

The *Trust Service Provider* shall continually test the operation of the backup system and shall review its business continuity plans annually.

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

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

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

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

The *Trust Service Provider* shall make full backups as frequently as necessary to be able to restore the full service in case of a disaster.

The business continuity plan of the *Trust Service Provider* shall include accurate requirements for the tasks to be performed in case of critical system component failure.

Once the problem resolved and the integrity restored, the *Trust Service Provider* shall restart 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

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

- all of the affected *Certificate*s of the *Trust Service Provider* shall be revoked;
- new provider private key shall be generated for the restoration of the services;
- the revoked provider *Certificate*'s data shall be disclosed according to the regulated method in Section 2.2 ;
- every *Website Authentication Certificate* shall be revoked that were signed by the affected private keys;
- new *Website Authentication Certificate*s shall be issued instead of the revoked *Certificate*s by using the new provider keys.
- the information related to the compromise shall be disclosed for every *Subscriber* and *Relying Party*;

### 5.7.4 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster shall be defined in the *Trust Service Provider*'s business continuity plan.

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

The secondary services site shall be 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* shall restore its devices damaged during the disaster and the original service security level as quickly as possible.

## 5.8 CA or RA Termination

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

During the termination the priority tasks are:

- the National Media and Infocommunications Authority, the Relying parties and the *Subscriber*s shall be notified about the planned termination in time;
- the *Trust Service Provider* shall make every effort to ensure that at the latest by the service termination another provider takes over the records and service obligations;
- new *Certificate* issuance shall be terminated;
- provider *Certificate*s shall be revoked, and provider private keys shall be destroyed;
- after the termination of the service, a full system backup and archiving shall be carried out;
- the archived data shall be handed over to the provider that takes over the services, or to the National Media and Infocommunications Authority.

# 6 Technical Security Controls

The *Trust Service Provider* shall use reliable systems and equipment protected against modification for the management of the cryptographic keys and activation data for the whole life-cycle.

The capacity demands shall be continuously monitored and the future capacity demands shall be estimated, so that the necessary availability of processing and storage needs are ensured.

## 6.1 Key Pair Generation and Installation

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

### 6.1.1 Key Pair Generation

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

- ETSI TS 119 312 [18];
- CABF Baseline Requirements recommendation [40];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [7] 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 shall ensure:

- The production of provider key pair is performed based on a key generation script.
- In case of a CA key pair generation a Qualified Auditor witness the CA key pair generation process or the *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 [23] , or

  - meets the requirements of FIPS 140-2 [41] level 3 or higher, or
  - meets the requirements of FIPS 140-3 [42] level 3 or higher, or
  - meets the requirements of CEN 419 221-5 [20], or
  - is a reliable system that is evaluated in accordance with ISO/IEC 15408 [22] 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* shall ensure 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**

In case of generating the key pair for the *Subject*s, the *Trust Service Provider* shall ensure that:

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

- After the documented handover of the private key to the *Applicant* the *Trust Service Provider* destroys every copy of the handed over private key stored by it, in such a way that its restoration and usage becomes impossible. The *Trust Service Provider* ensures that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6 , and the private key is not one of a known weak key pair.

In case of an *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

If the *Trust Service Provider* generated the the private key intended to be used during the website authentication, then the following requirements shall be met:

- Until the key handover, the *Trust Service Provider* stores the private keys generated by it for the *Subject*s and the activation data securely to prevent the key disclosure, copy, modification, damage and the usage by unauthorized persons.
- The *Trust Service Provider* shall ensure that the private keys and their activation data can only be taken over by the *Applicant*.
- The *Trust Service Provider* shall gain sufficient evidence of the handover of the private key to the *Applicant*, and the exact time of the handover.
- After the handover of the signer private key to *Applicant*, the *Trust Service Provider* shall not reserve any copy of the signer private key.

### 6.1.3 Public Key Delivery to Certificate Issuer

When the key pair is generated by the *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.

### 6.1.4 CA Public Key Delivery to Relying Parties

The *Trust Service Provider* shall make available its top-level provider Certificate public keys to the *Relying Parties* in such a way, that makes attacks targeting key modification impossible. Particularly, the *Trust Service Provider* at least shall disclose its provider *Certificate*s on its webpage.

The *Trust Service Provider* shall disclose the status information related to the *Certificate* of the certification units operated by it, and of the units that take part in the online certificate status service by the following methods:

- The name of the root certification units and the hash of its root certificates figure in the *Certification Practice Statement*. Their status change information shall be available on the webpage of the *Trust Service Provider*.
- The status change information of the intermediate (not root) certification units' certificates shall be 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* only discloses that *Certificate*'s revocation status in a way that in case of key compromise or other problem new *Certificate* won't be issued for the old private key signing the OCSP responses . The *Trust Service Provider* shall issue the OCSP response Certificates for new, secure private keys.

Regarding the disclosure methods of the status information, also see Section 4.10.

### 6.1.5 Key Sizes

The *Trust Service Provider* shall only use cryptographic algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [18];
- CABF Baseline Requirements recommendation [40];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [7] 92. § (1) b) .

### 6.1.6 Public Key Parameters Generation and Quality Checking

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

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

### 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The *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* shall include the Key Usage extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [38] compatible applications technically restrict the usage of the Certificates. The requirements set out for the value of the field are in Section 7.1.2.

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* shall ensure the secure management of the private keys held by it and shall prevent the private key disclosure, copy, deletion, modification and unauthorized usage. The *Trust Service Provider* may only preserve the private keys as long as the provision of the service definitely requires.

During the management of the *Hardware Security Module*s the signing private keys stored on the *Hardware Security Module*s which are out of order shall be deleted so that it is practically impossible to restore the keys.

### 6.2.1 Cryptographic Module Standards and Controls

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

- the requirements of ISO/IEC 19790 [23], or
- the requirements of FIPS 140-2 [41] level 3 or higher, or
- the requirements of FIPS 140-3 [42] level 3 or higher, or
- the requirements of CEN 419 221-5 [20], or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to ISO/IEC 15408 [22] or an equivalent security criteria system. The assessment either shall be based on the appropriate security system plan that meets the requirements of the present document, or on security appropriations.

The provider keys may only be stored in encrypted forms outside of the *Hardware Security Module*. For coding only those algorithms and key parameters shall be used by the current order of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [7] 92. § (1) b) that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

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

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

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

The *Trust Service Provider* shall to ensure that the simultaneous presence of at least two; trusted role holder employees is needed for the critical operations carried out with its provider private keys.

### 6.2.3 Private Key Escrow

The *Trust Service Provider* may escrow its own provider private keys only in encrypted form.

### 6.2.4 Private Key Backup

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

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

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

The *Trust Service Provider* shall not make any copy of the website authentication private keys.

### 6.2.5 Private Key Archival

The *Trust Service Provider* shall not archive its private keys and the end-user private keys.

### 6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Trust Service Provider* shall be created in a cryptographic module that meets the requirements.

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

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

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

### 6.2.7 Private Key Storage on Cryptographic Module

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

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

### 6.2.8 Method of Activating Private Key

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

The *Trust Service Provider* shall ensure that signatures can only be created with the private key of the root unit certificate in case of commands issued directly by the trust official duly authorized to do so.

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 *Trust Service Provider*'s private keys shall be deactivated in accordance with the procedures, requirements defined in the used *Hardware Security Module*'s user guide and the certification documents.

#### End-User Private Keys

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 shall be destroyed in a way that makes further use of the private keys impossible.

The provider private keys shall be destroyed according to the procedures, requirements defined in the user guide and in the certification documents of the used *Hardware Security Module*, in the simultaneous presence of two *Trust Service Provider* employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

Each backup copy of the private key shall be destroyed in a documented way in such a way that its restoration and usage becomes impossible.

#### End-User Private Keys

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* shall be stored in a cryptographic module that

- has a certificate according to ISO/IEC 19790 [23], or
- has a certificate according to FIPS 140-2 Level 3 [41], or
- has a certificate according to FIPS 140-3 Level 3 [42], or
- has an at least EAL-4 level Common Criteria [43] based certificate attesting compliance with the requirements of the CEN 419 221-5 [20], 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* shall archive every *Certificate* issued by it.

### 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 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*.

**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*.

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

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

The *Trust Service Provider*'s private keys shall be protected in accordance with the procedures, requirements defined in the used *Hardware Security Module* user guide and the certification documents.

In case of password based activation data usage, the passwords need to be sufficiently complex in order to ensure the required level of protection.

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

The creation and installation of the activation data of the *Applicant* created private keys is the duty of the *Applicant*.

### 6.4.2 Activation Data Protection

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

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 the IT system of the *Trust Service Provider* the compliance with the following requirements shall be ensured:

- the user identity is verified before granting access to the system or the application;
- roles are assigned to users and it shall be ensured that all users only have permissions appropriate for its roles;
- a log entry is created for every transaction, and the log entries shall be archived;
- for the security-critical processes it is ensured that the internal network domains of the *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

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

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

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

- commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by the *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.

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

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

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

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

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

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

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

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

The *Trust Service Provider* shall implement procedures for unauthorized change detection.

### 6.6.2 Security Management Controls

The *Trust Service Provider* shall implement processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system shall detect any kind of unauthorized changes, data entry that affects the system, the firewall, the routers, programs and other components used in the service. Installing the program used in the service the *Trust Service Provider* shall ensure that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Trust Service Provider* shall regularly check the integrity of the software in its system used in the service.

### 6.6.3 Life Cycle Security Controls

The *Trust Service Provider* shall ensure the protection of the used *Hardware Security Module*s during their whole life cycle.

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

- Decommissioned *Hardware Security Module*s shall be handled and disposed of in accordance with the requirements of their security target, instructions for use and certification report.

## 6.7 Network Security Controls

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

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

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

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

- shall divide its IT system into well separated security zones;
- shall separate dedicated network for administration of IT systems and the live operational network;
- shall separate the production systems for the TSP services from systems used in development and testing;
- shall establish communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- shall operate the IT systems used for the live operational network in secure network zones;
- shall restrict access and communications between zones to those necessary for the operation of the service;
- shall disable the not used protocols and accounts;
- shall disable unused network ports and services;
- shall only run network applications unconditionally necessary for the proper operation of the IT system;
- shall review the established rule set on a regular basis.

The *Trust Service Provider* shall undergo or perform a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least every three (3) months.

### 6.8 Time stamping

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

## 7 Certificate, CRL, and OCSP Profiles

### 7.1 Certificate Profile

The end-user *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 shall comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [38]
- IETF RFC 5280 [29]
- IETF RFC 6818 [32]
- IETF RFC 6962 [34];
- ETSI EN 319 412-1 [14]
- ETSI EN 319 412-4 [17]

#### 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* shall be "v3" *Certificate*s according to the X.509 specification [38].

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. [29]
- Serial Number
  The unique identifier generated by the *Certificate* issuer certification unit.

  In case of the end-user *Certificate*s the "Serial Number" field shall contain a random number with at least 8 bytes (64 bits) entropy.
- Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for the creation of the electronic signature or seal certifying the *Certificate*.
- Signature
  Electronic signature or seal made by the *Certification Authority* certifying the *Certificate*, that has been created with an Algorithm set defined in the "Algorithm Identifier" field.

- Issuer
  The unique name of the *Certificate* issuer *Certification Unit* according to the ITU X.501 [37] name format.
- 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 not be earlier than the real issuance time of the *Certificate*.

  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 [37] name format. Always filled out.
- Subject Public Key Algorithm Identifier

  The Identifier of the Subject Public Key Algorithm.
- Subject Public Key Value
  The public key of the Subject.
- Issuer Unique Identifier
  Not filled out.
- Subject Unique Identifier
  Not filled out.

### 7.1.2 Certificate Extensions

The *Trust Service Provider* may only use certificate extensions according to the X.509 specification [38] , the usage of self-defined critical extensions is not allowed.

Specific requirements concerning certificates extension:

**Certificate of the Root Certification Unit**

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field shall not be indicated.
- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic signature or seal certifying the *Certificate*.

  Filling in is mandatory.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key. The field value: the SHA-1 hash of the public key.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  Filling in is optional.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" field can be present in the *Certificate*.

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

  The field is mandatory and the values shall be:

  – "keyCertSign",
  – "cRLSign".

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

There shall not be any more *Certificate* extensions.

**Certificate of the Intermediate Certification Unit**

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field may limit the *Certificate 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.

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

  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 signature or seal certifying the *Certificate*.

  Filling in is mandatory.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key.
  The field value: the SHA-1 hash of the public key.

  Filling in is mandatory.

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

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The extension is required and its value is: CA = "TRUE".

  The "pathLenConstraint" field may be present in the *Certificate*.

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

  The field is mandatory and the value shall be:

  - "keyCertSign",
  - "cRLSign".

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

  The Intermediate Certification Unit *Certificate*s issued after 2019-01-01 for issuing *Website Authentication Certificate*s shall contain the following EKU values:

  - Server Authentication (1.3.6.1.5.5.7.3.1)
  - 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 and/or ldap protocol.
  It is mandatory to fill.

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the *Certificate* provided by the *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* shall provide online certificate status service. The availability of this service shall be indicated here.
  - To the facilitation of the certificate chain building the *Trust Service Provider* shall give the access path through http or ldap protocol of the *Certificate* of the *Certificate* issuer certification unit.

There may not be any more *Certificate* extensions.

**End-User Certificate**

- *Certificate* Policies – not critical
  OID: 2.5.29.32
  This field contains the denomination of the valid certification policy (see Section 1.2.1) at the time of the *Certificate* issuance and other information on the other uses of the *Certificate*.

  In case of end-user certificates, the *Trust Service Provider* shall fill 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 textual warning in English and Hungarian from which it can be established that it is a II. or III. certification class certificate, namely personal appearance did or did not happen at the registration, and the Subject of the *Certificate* is a natural person.
  - The identifier specified by ETSI EN 319 411-1 [13] 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.

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

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 signature or seal certifying the *Certificate*.

  Filling in is mandatory.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key. The field value: the SHA-1 hash of the public key.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  See section: 3.1.1.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field shall not be present in the end-user *Certificate*s.

  The "pathLenConstraint" field shall not be 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:

  - "digitalSignature" and
  - in case of RSA "keyEncipherment",
  - in case of ECC "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 mandatory value is:

  - "serverAuth (1.3.6.1.5.5.7.3.1)"

In the *Website Authentication Certificate*s the following further value may be set:

- "clientAuth (1.3.6.1.5.5.7.3.2)"

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

  Optional to fill.

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the *Certificate* provided by the *Trust Service Provider*.

  Mandatory in case of end-user certificates 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* shall provide online certificate status service. The availability of this service shall be indicated here.
  - To faciliate the certificate chain building the *Trust Service Provider* shall give 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.

  Only the use of the QCType field is allowed.

- 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*.

Other *Certificate* extension shall not be used.

### 7.1.3 Algorithm Object Identifiers

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

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

### 7.1.4 Name Forms

The *Trust Service Provider* shall use a distinguished name – composed of attributes defined in the standards IETF RFC 5280 [29], ETSI EN 319 412-2 [15], ETSI EN 319 412-3 [16] and ETSI EN 319 412-4 [17] – for the Subject identification in the *Certificate*s issued based on this *Certificate Policy*.

The *Certificate* shall contain the globally unique identifier of the *Subject* (OID), filled out as defined in Section 3.1.1.

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

### 7.1.5 Name Constraints

The *Trust Service Provider* can use name constraints if needed with the use of the "nameConstraints" field. In this case this field shall be marked as critical.

### 7.1.6 Certificate Policy Object Identifier

The *Trust Service Provider* shall include the not critical (*Certificate Policy*) extension in the *Certificate*s issued based on these *Certificate* Policies according to the requirements of the Section 7.1.2..

### 7.1.7 Usage of Policy Constraints Extension

No stipulation.

### 7.1.8 Policy Qualifiers Syntax and Semantics

The *Trust Service Provider* can put short information related to the *Certificate* usage into the *Certificate Policy* extension Policy Qualifier field. The field shall contain the online availability of the *Certification Practice Statement* (URI).

### 7.1.9 Processing Semantics for Critical Certificate Policy Extension

No stipulation.

## 7.2 CRL Profile

### 7.2.1 Version Number(s)

The *Certification Authority* shall issue version "v2" certificate *Certificate Revocation List*s according to the IETF RFC 5280 [29] 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 [29] 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 [29].

   (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 [29].

   (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 [29].

   Optional *Certificate Revocation List* Entry Extensions (crlEntryExtensions) that can be used by the *Certification Authority*:

   - Revocation Reason (reasonCode) – not critical
     OID: 2.5.29.21
     The reason for revocation can be entered in this field.
     Mandatory field in case of subordinate CA *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.

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

(g) CRL Extensions

- Provider Key Identifier (AuthorityKeyIdentifier)
  OID: 2.5.29.35
  The ID of the public key which belongs to the private key used to authenticate the *Certificate Revocation List* in the form of an "SHA1" hash.
- CRL Serial Number (cRLNumber) – not critical
  OID: 2.5.29.20
  This field shall contain the monotonically increasing serial numbers of the *Certificate Revocation List*s.

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

- Expired Certificates on the CRL (expiredCertsOnCRL) – not critical
  OID: 2.5.29.60
  The *Certification Authority* may indicate with this standard field according to the X.509 specification that it does not remove expired *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 to be supported:
   - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
   - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
3. Signature (signatureValue)
   The electronic signature or electronic seal of the *Certification Authority* certifying the *Certificate Revocation List*.
   The *Certificate Revocation List* shall be authenticated by the *Certification Authority* using the same key as used to sign or seal the issued *Certificate*.

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

## 7.3 OCSP Profile

The *Trust Service Provider* shall operate an online certificate status service according to the IETF RFC 6960 [33] and IETF RFC 8954 [36] 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* shall support at least the following cryptographic algorithms:

  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

- (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 [29].
- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response. Value according to UTC with encoding according to IETF RFC 5280 [29]. Mandatory.
- *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* shall support the "v1" version according to the standard IETF RFC 6960 [33] of the online certificate status requests and responses.

### 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 [33] 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 may be 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* shall have its operation periodically examined by independent external auditor. During the audit it shall be 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 [12]
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [13]
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects [19]

The result of the screening is a confidential document accessible only to authorized persons.

The conformity certificate issued in accordance with the conformity assessment report shall be published on the webpage of the *Trust Service Provider*.

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

## 8.1 Frequency or Circumstances of Assessment

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

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

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

A random check shall be performed 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*.

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

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

## 8.2 Identity/Qualifications of Assessor

The *Trust Service Provider* can perform 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 can be performed only 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*.

## 8.4 Topics Covered by Assessment

The review shall cover at least the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the *Certification Practice Statement*;
- adequacy of the employed processes;
- documentation;
- physical security;
- adequacy of the personnel;
- IT security;
- compliance with the data protection rules.

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

## 8.5 Actions Taken as a Result of Deficiency

The independent auditor shall summarize the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them shall be recorded in a separate chapter of the report.

The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

- modification suggestions to be optionally taken into consideration;
- derogations to be averted mandatorily.

### 8.6 Communication of Results

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

## 9 Other Business and Legal Matters

### 9.1 Fees

The fees applied by the *Trust Service Provider* shall be publicly disclosed in accordance with the applicable regulations.

#### 9.1.1 Certificate Issuance or Renewal Fees

The *Trust Service Provider* may determine fees for its services related to issuance, renewal, modification or re-keying of the *Certificate*s.

#### 9.1.2 Certificate Access Fees

The *Trust Service Provider* shall grant free of charge online access to its *Certificate Repository* for the *Relying Parties*.

#### 9.1.3 Revocation or Status Information Access Fees

The *Trust Service Provider* shall provide free of charge online CRL and OCSP service on the status of the issued *Certificate*s for the *Relying Parties*.

#### 9.1.4 Fees for Other Services

The *Trust Service Provider* may determine a service fee for other services provided to the *Subscriber*s .

#### 9.1.5 Refund Policy

No stipulation.

### 9.2 Financial Responsibility

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

### 9.2.1 Insurance Coverage

No stipulation.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-entities

- The *Trust Service Provider* shall have liability insurance to ensure reliability.
- The liability insurance policy shall cover 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 shall provide coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the *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* shall manage the data of the Clients in accordance with the respective regulations.

### 9.3.1 Scope of Confidential Information

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

### 9.3.2 Information Not Within the Scope of Confidential Information

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

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

### 9.3.3 Responsibility to Protect Confidential Information

The *Trust Service Provider* is responsible for the protection of the confidential data it manages.

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

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

Such circumstances are, for example:

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

## 9.4 Privacy of Personal Information

The *Trust Service Provider* shall take care of the protection of the personal data it manages. The operation and regulations of the *Trust Service Provider* shall comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [5] and the 2016/679 EU General Data Protection Regulation [2].

The *Trust Service Provider* shall:

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

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

### 9.4.1 Privacy Plan

The *Trust Service Provider* shall have a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing shall be published on the webpage of the *Trust Service Provider*.

### 9.4.2 Information Treated as Private

The *Trust Service Provider* shall protect all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from the Certificate or other public data source.

### 9.4.3 Information Not Deemed Private

The *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* shall store securely and protect the personal data related to the *Certificate* issuance and not indicated in the *Certificate*. The data shall be protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

### 9.4.5 Notice and Consent to Use Private Information

The *Trust Service Provider* shall only disclose 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 may be 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

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

The *Client* is entitled to the use of the identification in the certificate (which identifies the *Certificate* subject).

The present *Certificate Policy* is the exclusive property of the *Trust Service Provider*. The *Client*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Certificate Policy* and any other use for commercial or other purposes is strictly prohibited.

The present *Certificate Policy* may be freely distributed in unchanged form, in full length and with the indication of origin.

The rules of the application of the software provided for the use of the service by the *Trust Service Provider* shall be determined in the *Certification Practice Statement*.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

**Certification Authority's Responsibility**

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

- 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 [6] 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 [6] 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.).

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

- to determine the identity of the *Applicant*s;
- to determine the organizational identity of the *Represented Organization*, the identity and the eligibility of representation of the person acting on behalf of the *Represented Organization*;
- to warrant the authentication of the recorded registration data;
- prior to concluding service agreement to inform the user of the services on the availability and content of the *Certificate Policy* and the *Certification Practice Statement* and the terms and conditions of the service;
- in general to fully comply with its obligations.

### 9.6.3 Subscriber Representations and Warranties

#### *Subscriber* Responsibility

The responsibility of the *Subscriber* is set by the service agreement and its attachments (including the terms and conditions).

#### *Subscriber* Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *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 *Certificate Policy*, the service agreement and its attachments – in particular the general terms and conditions -– and the *Certification Practice Statement*.

#### *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 *Certificate Policy* and *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.

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

### 9.6.4 Relying Party Representations and Warranties

The *Relying Parties* decide based on their discretion and/or their policies about the way of accepting and using the *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

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

## 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

The *Trust Service Provider* can limit its liability for loss.

## 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 the *Certification Practice Statement*, the service agreement, or the contracts concluded with the *Client*s.

### 9.9.2 Indemnification by Subscribers

The *Trust Service Provider* sets the term of claim for damages from *Subscriber*s in the *Certification Practice Statement* and the service agreement.

### 9.9.3 Indemnification by Relying Parties

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

## 9.10 Term and Termination

### 9.10.1 Term

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

### 9.10.2 Termination

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

### 9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Certificate Policy* the *Trust Service Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

## 9.11 Individual Notices and Communications with Participants

The *Trust Service Provider* shall operate a customer service in order to maintain contact with its *Client*s.

## 9.12 Amendments

The *Trust Service Provider* reserves the right to change the *Certificate Policy* in a controlled way in case of the change of normative rules, security requirements, market conditions or other circumstances.

### 9.12.1 Procedure for Amendment

The *Trust Service Provider* reviews the *Certificate Policy* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change – or in case of the annual review even if no changes are made to the document – and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document 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 *Certificate Policy* , in which either the main version number or the sub-version number changes depending on the extent of the change.

In versions 1.x and 2.x, the version number of the *Certificate Policy* appeared in the 2 tags at the end of the OID of the document identifier, so two *Certificate Policy* with different contents - brought into force - could not have the same OID identifier.

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

## 9.13 Dispute Resolution Provisions

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

## 9.14 Governing Law

The *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 present *Certificate Policy* is compliant with the following regulations.

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [5];
- (Hungarian) Act V of 2013. on the Civil Code. [6].
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [7];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [8];
- (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 [9];
- (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 [10];

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

No stipulation.

### 9.16.2 Assignment

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

### 9.16.3 Severability

Should some of the provisions of the present *Certificate Policy* become invalid for any reason, the remaining provisions will remain in effect unchanged.

### 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 *Certificate Policy* , 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*
- 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*
  - 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 II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[5] (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 the general rules of electronic administration and 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] (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.

[12] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[13] ETSI EN 319 411-1 V1.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[14] ETSI EN 319 412-1 V1.4.4 (2021-05); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[15] 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;.

[16] 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.

[17] 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.

[18] ETSI TS 119 312 V1.4.2 (2022-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[19] 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.

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

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

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

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

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

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

[26] IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.

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

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

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

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

[31] IETF RFC 6532: Internationalized Email Headers, February 2012.

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

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

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

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

[36] IETF RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension, November 2020.

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

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

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

[40] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.8.4. CA/Browser Forum, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.4.pdf , 2022.

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

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

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

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

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