e-Szignó Certification Authority

eIDAS conform
Qualified Certificate for Electronic Seal
Certificate Policies

ver. 2.4

Date of effect: 30/09/2017

OID	1.3.6.1.4.1.21528.2.1.1.181.2.4 , 1.3.6.1.4.1.21528.2.1.1.182.2.4 , 1.3.6.1.4.1.21528.2.1.1.183.2.4
Version	2.4
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	31/08/2017
Date of effect	30/09/2017

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1031 Budapest, Záhony u. 7. D

Version	Description	Effect date	Author(s)
2.0	New policies according to the eIDAS requirements.	01/07/2016	Csilla Endrődi, Szabóné Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments.	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.
2.2	Changes according to the auditor comments.	30/10/2016	Sándor Szőke, Dr.
2.4	Yearly revision.	30/09/2017	Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document contains the *Qualified Seal Certificate Policy* defined by e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or *Trust Service Provider*) concerning the issuance of qualified certificate for electronic seal service.

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

1.1 Overview

The *Qualified Seal 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 RFC 3647 [27] 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 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 Policies 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 *Qualified Seal 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 or not fully in this sense used in other areas. The terms to be used in this sense are indicated by capitalization and italicization throughout this document.

1.2 Document Name and Identification

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

Issuer	e-Szignó Certification Authority
Document name	eIDAS conform Qualified Certificate for Electronic Seal Certificate Policies
Document version	2.4
Date of effect	30/09/2017

The listing 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* based on which they were issued. The first seven numbers of the *Certificate Policy* identifier OID 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 following numbers was allocated within Microsec own competence, interpretation as follows:

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

The present document defines the following *Certificate Policies*:

OID	DENOMINATION	SHORT NAME

1.3.6.1.4.1.21528.2.1.1.181.2.4	Qualified, for the generation and verification of electronic seals, for legal persons issued on *Qualified Electronic Seal Creation Device*, Certificate Policy prohibiting the use of pseudonyms.	MBJBN
1.3.6.1.4.1.21528.2.1.1.182.2.4	Qualified, for the generation and verification of electronic seals, for legal persons issued on *Hardware Security Module*, Certificate Policy prohibiting the use of pseudonyms.	MBJHN
1.3.6.1.4.1.21528.2.1.1.183.2.4	Qualified, for the generation and verification of electronic seals, for legal persons issued as a software token , Certificate Policy prohibiting the use of pseudonyms.	MBJSN

Formation and interpretation of the *Qualified Seal Certificate Policy* short name happens according to the following rules:

- First character [Xxxxx]
  - M: qualified *Certificate Qualified Seal Certificate Policy*
  - N: non-qualified *Certificate Qualified Seal Certificate Policy*
  - H: non-qualified, III. certificate class *Certificate Qualified Seal Certificate Policy*
  - K: non-qualified, II. certificate class *Certificate Qualified Seal Certificate Policy*
  - A: non-qualified, automatic issuance *Certificate Qualified Seal Certificate Policy*
  - x: no stipulation
- Second character [xXxxx]
  - A: Signing purpose *Certificate Qualified Seal Certificate Policy*
  - B: Seal creation purpose *Certificate Qualified Seal Certificate Policy*
  - W: *Website Authentication Certificate Qualified Seal Certificate Policy*
  - K: *Codesigning Certificate Qualified Seal Certificate Policy*
  - x: no stipulation
- Third character [xxXxx]
  - T: *Certificate* issued to a natural person *Qualified Seal Certificate Policy*
  - J: *Certificate* issued to a legal person *Qualified Seal Certificate Policy*

  - x: no stipulation

- Fourth character [xxxXx]
  - B: *Certificate* issued on *Qualified Electronic Seal Creation Device Qualified Seal Certificate Policy*
  - H: *Certificate* issued on *Hardware Security Module Qualified Seal Certificate Policy*
  - S: *Certificate* issued by software *Qualified Seal Certificate Policy*
  - x: no stipulation
- Fifth character [xxxxX]
  - A: pseudonymous *Certificate Qualified Seal Certificate Policy*
  - N: pseudonym excluding *Certificate Qualified Seal Certificate Policy*
  - x: no stipulation

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

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

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

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

In case of a *Certificate Policy* ([xxxHx]) that requires the usage of *Hardware Security Module*, the *Trust Service Provider*:

a./ guarantees that the private key belonging to the *Certificate* is stored only on such *Hardware Security Module* that has at least one of the following certifications:

- Certificate issued in any of the member states of the European Union certifying that the equipment is a *Qualified Electronic Seal Creation Device*;
- Common Criteria [34] certification according to CEN SSCD PP [36], at least at level EAL4;
- FIPS 140-2, Level 2 (or higher) certification [33]

or

b./ can accept the *Certificate* applicant's written statement to this effect, while preserving its right to discretion.

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

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

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

A document, with a qualified electronic seal or with advanced electronic seal based on a qualified *Certificate* under paragraph 196 Act III of 1952 on Civil Procedure [3] is representing conclusive evidence.

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [QCP-l] *Certificate Policy* defined in the ETSI EN 319 411-2 [16] standard;
- the [MBJBN] *Certificate Policy* complies with the [QCP-l-qscd] *Certificate Policy*.
- the [MBJHN] *Certificate Policy* complies with the [NCP+] *Certificate Policy* defined in the ETSI EN 319 411-1 [15] standard.

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.

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

1.2.2 Effect

This *Certificate Policy* collection is in effect from the 30/09/2017 date of entry into force to withdrawal.

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 *Qualified Seal Certificate Policy* extends each of the participants mentioned in section 1.3.

Present *Certificate Policies* 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 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 [Mxxxx];
- non-qualified III. certification class *Certificate*s [Hxxxx] issued by e-Szignó Certification Authority;
- non-qualified II. certification class *Certificate*s [Kxxxx] issued by e-Szignó Certification Authority;
- non-qualified *Certificate*s issued not by e-Szignó Certification Authority [xxxxx].

Based on the used container in descending order by security:

- *Certificate*s issued on *Qualified Electronic Seal Creation Device* [xxxBx];
- *Certificate*s issued on *Hardware Security Module* [xxxHx];
- otherwise, for example *Certificate*s issued by software [xxxSx], [xxxxx].

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 Seal Creation Device* [MxxBx];
- qualified *Certificate*s issued on *Hardware Security Module* [MxxHx];
- qualified otherwise, for example *Certificate*s issued by software [MxxSx], [Mxxxx];

- non-qualified III. certification class *Certificate*s [HxxHx] issued by e-Szignó Certification Authority on a *Hardware Security Module*;
- non-qualified otherwise, for example by software issued III. certification class *Certificate*s [HxxSx][Hxxxx];
- non-qualified II. certification class *Certificate*s [KxxHx] issued by e-Szignó Certification Authority on *Hardware Security Module*;
- non-qualified otherwise, for example by software issued II. certification class *Certificate*s [KxxSx][Kxxxx] issued by e-Szignó Certification Authority;
- non-qualified *Certificate*s issued not by e-Szignó Certification Authority [xxxxx].

During the communication with the *Client*s the *Trust Service Provider* supports the use of electronic channels and enables the use of electronic seal 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. certificate 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 *Qualified Seal 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.

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 *Subject* is that legal person, whose data is indicated on the *Certificate*.

In case of a *Certificate* for electronic seal purposes, the *Subject* is the *Creator of the Electronic Seal*.

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

There is no other participants.

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 electronic seal creation, with the *Certificate*s the *Creator of the Electronic Seal* can verify the authenticity of the documents sealed by him.

In case of *Certificate Policies* requiring *Qualified Electronic Seal Creation Device* usage ([MBJBN]) the private key belonging to the qualified *Certificate* is protected by the *Qualified Electronic Seal*

Creation Device that was issued within the confines of the electronic seal qualified certificate issuance service. *Certificate*s issued according to these polices are suitable for qualified electronic seal generation.

If a *Certificate Policy* does not require the usage of a *Qualified Electronic Seal Creation Device*, then the electronic seal based on a certificate issued according that policy can be considered a qualified certificate based advanced electronic seal.

A document, with a qualified electronic seal under the paragraph 99. of Act CCXXII. [8] of 2015. on general rules about electronic administration and trust services shall be considered a document representing conclusive evidence.

1.4.2 Prohibited Certificate Uses

Provider Certificates

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

End-User Certificates

*Certificate*s issued in accordance with the present *Certificate Policies*, and the private keys belonging to them using for other purposes than the generation and verification of electronic seal is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Organization name	Microsec e-Szignó Certification Authority
Organization address	Hungary, H-1037 Budapest, Záhony street 7. building D
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
E-mail address	info@e-szigno.hu

1.5.2 Contact Person

Questions related to the present *Qualified Seal Certificate Policy* can be directly put to the following person:

Contact person	Process management department leader
Organization name	Microsec ltd.
Organization address	Hungary, H-1037 Budapest, Záhony street 7. building D
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
E-mail address	info@e-szigno.hu

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

The provider that issued the *Certification Practice Statement* is responsible for its conformity with the *Qualified Seal Certificate Policy* referenced in it and for the provision of the service according to 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 *Qualified Seal 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	A person with an identity or attribute verified by the *Trust Service Provider* with the *Certificate*, so the seal creator especially in case of an electronic seal certificate.
Certificate for Automatism	A *Certificate* in which the name of the IT device (application, system) that is applied by the *Subject* to use the *Certificate* is to be recorded among the *Subject*'s data.
Creator of a Seal	"A legal person who creates an electronic seal." *(eIDAS [1] article 3. point 24.)*
Trust Service Supervisory Body	"The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [8] 91.§ 1. paragraph)*
Trust Service	"Means an electronic service normally provided for remuneration which consists of: • the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or • the creation, verification and validation of *Website Authentication Certificate*; or • the preservation of electronic signatures, seals or certificates related to those services; " *(eIDAS [1] 3. article 16. point)*
Trust Service Policy	"A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common security requirements." *(Act CCXXII. of 2015. [8] 1. § 8. point)*

Trust Service Provider	"A natural or a legal person who provides one or more *Trust Service*s either as a qualified or as a non-qualified *Trust Service Provider*." *(eIDAS [1] 3. article 19. point)*
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. *(eIDAS [1] 3. article 25. point)*
Qualified Certificate for Electronic Seal	A *Certificate* for an electronic seal issued by a *Qualified Trust Service Provider* and meets the requirements laid down in eIDAS Annex III [1]. *(eIDAS [1] 3. article 30. point)*
Certificate for Electronic Seal	An electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person. *(eIDAS [1] 3. article 29. point)*
Electronic Seal Creation Data	"Means unique data, which is used by the creator of the electronic seal to create an electronic seal." *(eIDAS [1] 3. article 28. point)* Typically cryptographic private key.
Electronic Seal Creation Device	"Means configured software or hardware used to create an electronic seal." *(eIDAS [1] 3. article 31. point)*
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.
Relying Party	Recipient of the electronic document, who acts relying on the electronic seal based on a given certificate.

Validation	"Means the process of verifying and confirming that an electronic signature or a seal is valid. " *(eIDAS [1] 3. article 41. point)*
Validation Chain	The electronic document or its hash, and the series of information assigned to one another (especially those certificates, information related to certificates, data used for signature or seal creation, the current status of the certificate, information on the withdrawal, as well as information on the validity data of the certificate issuer provider and its revocation information), with the help of which it can be established that the advanced or qualified electronic signature, seal or time-stamp placed on the electronic document was valid at the time of the signature, seal or time-stamp placement. *(Act CCXXII. of 2015. [8] 1. § point 21.)*
Validation Data	"Means data that is used to validate an electronic signature or an electronic seal." *(eIDAS [1] 3. article 40. point)*
Suspension	The temporary termination 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.
Advanced Electronic Seal	"Means an advanced electronic seal that meets the following requirements: a/ it is uniquely linked to the creator of the seal; b/ it is capable of identifying the creator of the seal; c/ it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and d/ it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable. " *(eIDAS [1] 3. article 26. point)*

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 the Signature-Verification Data – indicated on the certificate.
HSM: Hardware Security Module	A hardware-based secure tool that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions.
Certification Authority	A *Trust Service Provider*, who/which identifies the requester within the confines of the certification service, issues *Certificate*s, keeps a record, receives the *Certificate* related data changes, and publishes the regulations belonging to the *Certificate* and the information on the current state (especially on possible revocation) of the *Certificate*.
Certification Unit	A unit of the *Trust Service Provider*'s system that signs the *Certificate*s. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a *Certification Unit*. It is possible that a Certification Authority simultaneously operate several *Certification Unit*s.
Certificate Policy	"A *Trust Service Policy* which concerns the *Certificate* issued within the framework of the *Trust Service*." *(Act CCXXII. of 2015. [8] 1. § 24. point)*
Applicant	That natural person who acts during the application for the given *Certificate*.

Represented Organization	If the *Certificate* is issued to the *Applicant* for the purpose of using it for its activities or for sealing on behalf of the *Organization* then the *Represented Organization* is the *Organization* in question, which is also specified in the *Certificate*.
Compromise	A cryptographic key is compromised, when unauthorized persons might have gained access to it.
Intermediate Certification Unit	A *Certification Unit* whose *Certificate* was issued by another *Certification Unit*.
Cryptographic Key	An individual digital signal series controlling cryptographic transformation, the knowledge of which is required for encryption, decryption, electronic signature creation and verification.
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.
Hash	"A specific length bit string assigned to the electronic document, during the creation of which the used procedure (hashing procedure) fulfils the requirements defined in Act CCXXII. of 2015. [8] at the time of the creation." *(Act CCXXII. of 2015. [8] 1. § 34. point)* The hash in practice a fixed-length bit string that is clearly dependent on the electronic document, from which it is derived from, with a very small probability that two different documents would have the same hash, and it is practically impossible given the hash prepare a document, which has the same hash.

Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair for an actor that the *Subject* shall keep strictly secret. In case of electronic seals the *Creator of the Electronic Seal* generates the seal with the help of the private key. 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.
Qualified Trust Service	"A *Trust Service* that meets the applicable requirements laid down in the eIDAS Regulation." *(eIDAS [1] article 3. point 17.)*
Qualified Trust Service Provider	"A *Trust Service Provider* who provides one or more *Qualified Trust Service*s and is granted the qualified status by the supervisory body." *(eIDAS [1] article 3. point 20.)*
Qualified Electronic Seal	An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal. *(eIDAS [1] article 3. point 27.)*
Qualified Electronic Seal Creation Device	"Means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II of eIDAS" *(eIDAS [1] article 3. point 32.)*
Qualified Electronic Time Stamp	An electronic Time-Stamp which meets the requirements laid down in Article 42 of the eIDAS Regulation [1]. *(eIDAS [1] article 3. point 34.)*
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to an actor, 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 an electronic seal, the public key of the seal creator party is needed to verify the seal authenticity (this is the Certificate-Verifier Data). 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 provider contract 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.
Organization	Legal person.
Organizational Certificate	A *Certificate*, the *Subject* of which is the *Organization*, or which presents that the natural person *Subject* belongs to a *Organization*. In this case the name of the *Organization* is indicated in the "O" field of the *Certificate*. Every seal certificate is a *Organizational Certificate*.

Organization Administrator	That natural person who is eligible to act during the application, suspension, reinstatement and revocation of the electronic seal *Certificate*s issued to the *Organization* and to grant the issuance of organization related personal *Certificate*s and the revocation of such *Certificate*. The Organization administrator can be appointed by a person eligible for representing the organization. Designation of an Organization Administrator is not compulsory for every Organization, if not designated, then the person eligible to represent the Organization performs the tasks aforementioned.
Trust Service Practice Statement	"The statement of the *Trust Service Provider* of the detailed procedures or other operational requirements used in connection with the provision of particular *Trust Service*s." *(Act CCXXII. of 2015. [8] 1. § point 41.)*
Service Agreement	"The contract between the *Trust Service Provider* and the *Trust Service* client, which includes the conditions for the provision of the *Trust Service* and for using the services." *(Act CCXXII. of 2015. [8] 1. § point 42.)*
Certificate	"The electronic signature certificate, the electronic seal certificate and the *Website Authentication Certificate*, and all those electronic verifications issued within the framework of the *Trust Service* by the service provider, which includes the certificate related verification data and the certificate usage related information, and which as an electronic document is reliably protected against the available counterfeiting technologies at the time of the issuance and during its validity period." *(Act CCXXII. of 2015. [8] 1. § point 44.)*
Certificate Application	The data and statements given by the *Applicant* to the *Trust Service Provider* for *Certificate* issuance, in which the *Applicant* reaffirms the authenticity of data to be indicated on the *Certificate*.

Certificate Repository	Data repository containing various *Certificate*s. A Certification Authority has a Certificate Repository in which the issued certificates are disclosed, but the system containing Certificates available to the application on the computer of the *Subject* and the *Relying Party* is also called Certificate Repository.
Client	The collective term for the *Subscriber* and every related *Applicant* denomination.
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 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 maintained by the *Certification Authority*.

1.6.2 Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	electronic Identification, Authentication and Signature
LDAP	Lightweight Directory Access Protocol
NMHH	National Media and Infocommunications Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
TSP	Trust Service Provider

2 Publication and Repository Responsibilities

2.1 Repositories

The *Certification Authority* shall publish on its webpage and through LDAP protocol its provider *Certificate*s, and those *Certificate*s to the disclosure of which the *Applicant* consented to.

The *Trust Service Provider* shall publish the *Qualified Seal Certificate Policy*, the *Certification Practice Statement* and other documents containing the terms and conditions its operation is based on.

The *Certification Authority* 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 3 hours in each case.

2.2 Publication of Certification Information

The *Trust Service Provider* shall disclose on its webpage its provider *Certificate*s, and those *Certificate*s for the *Relying Parties* to the disclosure of which the *Applicant* consented to.

Service Provider Certificates

With the following methods the *Certification Authority* shall disclose the *Certificate*s of the time-stamping units, certification units and the online certificate status service units it operates:

- The denomination of the root certification units, and the hash of its root certificates in the *Certification Practice Statement*. 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) shall be disclosed on the revocation lists, its website and within the confines of the online certificate status response services.
- For the signers of the online certificate status responses the *Certification Authority* – compliant to the best international practice – shall issue a *Certificate* with extremely short period of validity thereby eliminating the need for *Certificate* revocation status verification. The revocation status of the OCSP response *Certificate*s shall be disclosed by the *Trust Service Provider* such a way that in case of key compromise, or any other problems there shall not be any more new *Certificate* disclosed for the OCSP response signer old private key later. The *Trust Service Provider* shall disclose OCSP response *Certificate*s for a new, secure private key.

End-User Certificates

With the following methods the *Certification Authority* shall disclose status information related to the end-user *Certificate*s which it had issued:

- on revocation lists,
- within the confines of the online certification status response service.

The end-user *Certificate* revocation and suspension 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.

The *Trust Service Provider* shall disclose the contractual conditions and policies electronically on its website.

The new documents to be introduced shall be disclosed on the website 30 days 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 in printed form at the customer service of the *Trust Service Provider*.

The *Trust Service Provider* shall make available the *Qualified Seal Certificate Policy*, the *Certification Practice Statement* and the Service Agreement to the *Client* on a durable medium following the conclusion of the contract.

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

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The disclosure of the *Qualified Seal Certificate Policy* related new versions is compliant with the methods described in Section 9.12.

The *Trust Service Provider* discloses other regulations, contractual conditions and their new versions if necessary.

The *Trust Service Provider* shall publish extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

2.3.2 Frequency of the Certificates Disclosure

The *Trust Service Provider* regarding the disclosure of some *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 *Certification Authority* shall disclose in case of the *Applicant*'s consent 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 on the certificate revocation lists. The requirements related to the issuance of the certificate revocation lists are discussed in Section 4.10.

2.4 Access Controls on Repositories

Access shall be provided to anyone for reading purposes to public information of the *Certificate*s and status information disclosed by the *Certification Authority* according to the particularities of publication.

The information disclosed by the *Certification Authority* shall only be amended, deleted or modified by the *Certification Authority*. The *Certification Authority* shall prevent unauthorized changes to the information with various defence mechanisms.

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 RCF 5280 [29] and RFC 6818 [30] 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):

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

  The organization's full or shortened name shall be in this field in the same form as in a public registry – or in the absence thereof in the deed of foundation.

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

  Filling is required.

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

  It shall not be filled.

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

  It shall not be filled.

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

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

  Seal *Certificate* shall not be pseudonymous.

- 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 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*.

  The "Serial Number" value that meets the above requirements is the Subject provider unique identifier.

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

  In the "O" field the *Organization*'s full or shortened name shall be indicated according to the deed of foundation or a public register.

  The field shall be filled out.

  In case of a provider *Certificate* issued for a *Trust Service Provider* the "O" field is mandatory to be filled, 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
  The identifier of the *Organization* indicated in the "O" field can be in this field.

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

  Filling out the field is mandatory.

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

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

  Only that data can be indicated here that the *Trust Service Provider* verified and that the *Organization* has the right to use.

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

  Optional field.

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

  The two-letter country code - according to ISO 3166-1 [23] - of the place of incorporation of the *Organization* indicated in the "O" field.

  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

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

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

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

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

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

  Optional field.

- Postal Code – OID: 2.5.4.17 – Zip code

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

  Optional field.

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

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

  Shall not be filled.

- E-mail Address (EMAIL) – OID: 1.2.840.113549.1.9.1 – The e-mail address of the *Subject*

  Optional to fill.

  If filled, it shall be the same as the e-mail address indicated in the "RFC822name" field of the *Subject* alternative names field.

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 " ").

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.

- In case of *Organizational Certificate*s, for the request of the *Applicant* the trademark, trade name or DBA (Doing Business As) name or product name legitimately used by the *Organization* can be indicated (possibly supplemented by a unique identifier) in this field. The *Trust Service Provider* is entitled to denote the nature of the name indicated.

  The *Trust Service Provider* shall verify the names to be indicated in the "Subject Alternative Names" field.

- The *Subject*'s e-mail address can be given in the subject alternative names "rfc822Name" field. If there's an e-mail address indicated on the *Certificate*, then this field definitely shall be filled out. The same e-mail address might be displayed in the "EMAIL" field of the *Certificate*.

  Further *Subject* alternative names field usage is permitted.

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 name of the *Organization* in the *Certificate* shall be indicated the same way as the notation in public registers – or in the absence thereof like in the deed of foundation.

3.1.3 Anonymity or Pseudonymity of Subscribers

Seal certificate shall not be pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

In order to interpret the identifiers it is recommended 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.

The *Trust Service Provider* can indicate other unique identifier (for example, identity card number, tax number, and identification within the organization) on request.

Procedures to Resolve Disputes Relating the Names

The *Trust Service Provider* shall make sure of the *Client*'s credentials to use the indicated names. The *Trust Service Provider* is entitled to revoke the *Certificate* in question for the illegal use of the name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

In the fields of the end-user *Certificate* required by the *Subscriber* trademarks may occur, and the *Trust Service Provider* shall make sure of their legitimate use, and in case of a complaint it is entitled to revoke the *Certificate*.

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 refuse the issuance of the required *Certificate* at its sole discretion, without any apparent 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 *Certificate* requester owns and has it under his control 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*.

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

3.2.2 Authentication of an 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 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 trade marks indicated in the *Certificate* see the chapter 3.1.6.

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

The *Trust Service Provider* shall guarantee that the registration and verification of the personal data can not be carried out by the same person.

3.2.3 Authentication of an Individual Identity

The natural person's identity shall be verified:

- if a natural person is acting on behalf of an *Organization* for *Organizational Certificate* application.

When issuing a qualified *Certificate*, the identity of the natural person shall be verified according to (1) paragraph of Article 24 of the eIDAS regulation [1] by the physical presence or by a method providing equivalent security. The *Trust Service Provider* shall use the identification methods described in the (1) paragraph of article 24. as follows.

The method of the identification of the natural person is:

1. During personal identification.

   - the natural person shall appear in person at the *Registration Authority* to perform the personal identification;
   - 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. [4]) official cards appropriate for verifying identity defined in Nytv. in accordance with Eüt. 85.§ (3) [8];
     – in case of natural persons outside the scope of Nytv. [4] on the basis of a travel document defined in the Act on the entry and residence of persons enjoying the right of free movement and residence or the law on entry and residence of third-country nationals [5] in accordance with Eüt. 85.§ (4) [8];
     – in case of identifying natural persons abroad none on the basis of the above documents the *Trust Service Provider* applies identity verification in accordance with Eüt. 82. (5) [8] only in the case of identifying European citizens. In such case, accepts a personal identity card with a photo issued by the European country of nationality accepted as a trusted document for identity verification.
   - the natural person shall verify the accuracy of the data for the registration and identity verification with a statement signed with a handwritten signature;
   - the *Trust Service Provider* verifies, whether any alteration or counterfeiting happened to the presented identity cards.

2. Remotely using an electronic identification device, with respect to that the physical presence of a natural person or a representative entitled to represent the legal person before issuing qualified certificates has been guaranteed, and which complies with the substantial or high security levels defined in Article 8 of eIDAS regulation [1].

   In these cases:

   - In addition, during identification besides subject's name an identification number or other data accepted on a national level that enables that natural persons can be distinguishable from others of the same name shall be supplied.

3. By identification traced back to an electronic signature certificate. In this case:

   - The *Applicant* submits the *Certificate Application* in electronic format with an electronic signature based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate* (see section 1.2.3.).
   - The electronically signed *Certificate Application* shall contain the data needed for the definit identification of the natural person.
   - The authenticity and confidentiality of the *Certificate Application* shall be verified on the whole certification chain.
   - The *Trust Service Provider* may accept only those electronic signatures, which are based on a *Certificate* issued by a Trust Service Provider which is listed on the Trusted List of one of the EU member states and was valid at the time of the signature creation.

4. By using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

   In this case the *Trust Service Provider* processes the identity verification the same way as in case of the personal identification. The only difference is that the face to face identification is replaced by a remote validation process which shall ensure that

   - the identity of the natural person can be securely verified;
   - the identity of the natural person and the official proof of identity card used for the verification can be connected with high relaibility by using biometrical identification data;
   - the natural person can be connected to the received *Certificate Application*.

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*.

The *Trust Service Provider* shall guarantee that the registration and verification of the personal data can not be carried out by the same person.

3.2.4 Non-Verified Subscriber Information

Only that data can be in the *Certificate* issued by the *Trust Service Provider*, which was verified by the *Trust Service Provider* or on the authenticity of which the *Applicant* made a statement with recognition of their criminal liability.

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*.

In case of Organizational Certification applications the *Organization* may appoint an organization administrator, who is eligible to act during the application, suspension, reinstatement and revocation of the *Certificate*s issued to the *Organization* .

An Organization administrator can be appointed by a person eligible for representing the *Organization*. The designation of an Organization 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 validity of the affected *Certificate*.

Details related to the re-key process can be read in section 4.7.

3.3.1 Identification and Authentication for Routine Re-key

For the submission of the re-key applications, the following options shall be provided:

- on paper signed manually by the *Applicant* at the customer service of the *Trust Service Provider*, to the mobile registration associate of the *Trust Service Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed upon,
- in an electronically submitted request with a electronic seal based on the *Certificate* to be renewed;
- in electronic form with an electronic signature of the *Applicant* based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- signed manually, sent by post to the Customer service.

In case of a personal application the applicant identification takes place as described in section 3.2.3.

In case of a *Certificate* application according to the aforementioned, signed with an electronic signature or with an electronic seal, there is no need for further verification of the applicant's identity, or the authenticity of the application.

3.3.2 Identification and Authentication for Re-key After Revocation

The *Trust Service Provider* can accept re-key requests only during the service provision time, in case of *Certificate*s suspended, revoked or expired due to key compromise too. The identity of the person submitting the request shall be verified according to the process defined 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

For submitting *Certificate* renewal requests the following options are enabled by the *Trust Service Provider*:

- on paper signed manually by the *Applicant* at the customer service of the *Trust Service Provider*, to the mobile registration associate of the *Trust Service Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed,

- in an electronically submitted request with a electronic seal based on the *Certificate* to be renewed;
- in electronic form with an electronic signature of the *Applicant* based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- signed manually, sent by post to the Customer service.

In case of a personal application, then the *Applicant*'s identification takes place according to as described in section 3.2.3.

In case of a *Certificate* application according to the aforementioned, signed with an electronic signature or with an electronic seal there is no need for further verification of the applicant's identity, or the authenticity of the application.

In case the renewal request is submitted on paper by post, the identification of the applicant and the verification of the application is performed during a personal meeting after receiving the application. .

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 *Subject* with an unchanged public key, but with different *Subject* identification data.

In this case, the changed *Subject* information shall be verified by the *Trust Service Provider* as defined in section 3.2. before the *Certificate* issuance.

3.5.1 Identification and Authentication in Case of a Valid Certificate

For submitting *Certificate* modification applications the following options are enabled by the *Trust Service Provider*:

- on paper signed manually by the *Applicant* at the customer service of the *Trust Service Provider*, to the mobile registration associate of the *Trust Service Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed,
- in an electronically submitted request with a electronic seal based on the *Certificate* to be renewed;

- in electronic form with an electronic signature of the *Applicant* based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- signed manually, sent by post to the Customer service.

In case of a personal application, then the *Applicant*'s identification takes place according to as described in section 3.2.3.

In case of a *Certificate* application according to the aforementioned, signed with an electronic signature or with an electronic seal, there is no need for further verification of the applicant's identity, or the authenticity of the application.

In case the modification request is submitted on paper by post, the identification of the *Applicant* and the verification of the application is performed during a personal meeting after receiveing the application. .

3.5.2 Identification and Authentication in Case of an Invalid Certificate

Invalid *Certificate* shall not be modified.

3.6 Identification and Authentication for Revocation Request

The *Trust Service Provider* shall receive and process the requests related to the suspension and 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 identity of the person submitting the requests and the authenticity of the requests shall get verified.

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

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 name of *Organization* name of organizational unit, city, country, e-mail address);
- the personal identification information of the person entitled to represent the *Subject* (full name, number of the identity document);
- the contact of the person entitled to represent the *Subject* (telephone number, e-mail address);
- 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 person entitled to represent the *Subject* according to Section 3.2.3;
- the documents for the identification of the *Organization* according to Section 3.2.2;
- the certification or procuration delivered by the *Organization*, that the *Applicant* is entitled to represent the *Organization* ;
- if the *Certificate* requested contains a trademark or a brand name, then a certification about the usage rights of the *Applicant* .

4.1.1 Who May Submit a Certificate Application

Certificate Application may only be submitted by natural persons, to request a *Certificate* for the organization represented. 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 person entitled to represent the *Subject* may submit the *Certificate Application* in the following ways:

- on paper signed manually during the personal identification performed at the customer service of the *Trust Service Provider*, by the mobile registration associate of the *Trust Service Provider* or by some other *Registration Authority*'s registration associate,
- on paper sent by post to the postal address of the *Trust Service Provider* (in this case, the personal identification will take place later)
- in electronic form with an electronic signature based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate*, sent to the *Trust Service Provider*'s e-mail address (see section 1.2.3.);

The *Subscriber* and the person entitled to represent the *Subject* 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* (or the *Registration Authority*) shall ascertain the identity of the person submitting the *Certificate Application* (see section 3.2.3.)

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 *Subscriber* determines which *Applicant* is entitled to request a *Certificate* according to which *Certificate Policy*.

The person entitled to represent the *Subject* 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 person entitled to represent the *Subject* 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 decision about the disclosure of the *Certificate*;
- a statement that there's no brand name or trademark indicated in the requested *Certificate*, or it is indicated and the applicant is entitled to use that.

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 *Applicant* or the *Subscriber* handed in.

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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*.

The *Trust Service Provider* accepts or refuses to fulfil the *Certificate Application* after processing it.

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

4.3.1 CA Actions During Certificate Issuance

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

The *Trust Service Provider* shall guarantee that the whole *Certificate* issuance process can not be carried out by only one person.

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

The person entitled to represent the *Subject* shall verify the accuracy of the data indicated in the *Certificate* before the takeover of the *Certificate* and shall make a written statement on that. The person entitled to represent the *Subject* verifies the reception of the *Certificate* by signing the statement.

If the Certification Authority provides *Qualified Electronic Seal Creation Device* to the *Subject*, after the reception of the *Qualified Electronic Seal Creation Device* containing the private key, the *Certificate* of the *Subject* and the code necessary for activation the *Applicant* can test his/her device. Afterwards the *Applicant* shall sign manually a statement about takeover, in which – amongst others – he/she verifies that the data indicated in the *Certificate* are accurate, he/she received the related activation codes and that he/she is acquainted with the technical and legal requirements of the *Qualified Electronic Seal Creation Device* usage.

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

The person entitled to represent the *Subject* shall be notified about the issuance of the *Certificate*.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The *Subject* shall only use its private key corresponding to the *Certificate* for electronic seal creation, and any other usage is prohibited.

A private key corresponding to an expired, revoked, or suspended *Certificate* shall not be used for electronic seal creation.

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 accepting the electronic seal verified, 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*;
- *Certificate*s for electronic seals and the corresponding public keys shall only be used for electronic seal validation;
- 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.

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 suspended or revoked;
- the private key corresponding to the *Certificate* is not compromised;
- the *Subject* identity information indicated in the *Certificate* is still valid.

The *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 who is entitled to submit an application for a new *Certificate* of the same type on behalf of the *Subject* 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 the service signatory key used for the issuance of 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 suspended or revoked;
- based on currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the *Certificate* to be issued.

The method used for identification and authentication during the Certificate renewal is stated in Section 3.4.

4.6.4 Notification of the Client about the New Certificate Issuance

The *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

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

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 suspended or 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

The person entitled to represent the *Subject* 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 process when the *Trust Service Provider* temporarily ceases the validity of the *Certificate* before expiration is called *Certificate* suspension. The *Certificate* suspension is a temporary state; the suspended *Certificate* can be revoked, or before the end of the validity, with the withdrawal of the suspension it can be made valid again. In case of the withdrawal of suspension the *Certificate* becomes valid retroactively, as if it has not been suspended.

4.9.1 Circumstances for Revocation

The *Trust Service Provider* shall revoke the end-user *Certificate* in the following cases:

- *Certificate* modification because of data change referring to the *Subject*;
- the *Trust Service Provider* becomes aware that the data in the *Certificate* do not correspond to reality;
- the *Applicant* or the *Subscriber* notifies the *Trust Service Provider* that the *Certificate Application* is not approved and subsequently the approval is not given;
- the *Applicant* or the *Subscriber* requests the revocation of the *Certificate* in writing;
- the *Trust Service Provider* becomes aware that the private key is not in the exclusive possession of the *Applicant* ;
- the *Trust Service Provider* becomes aware that the certificate was used illegally;
- the *Trust Service Provider* becomes aware that the *Subscriber* failed to fulfil any of its financial obligations according to the service agreement;
- the *Trust Service Provider* 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 *Trust Service Provider* becomes aware that the *Certificate* was not issued according to the related *Qualified Seal Certificate Policy* and the *Certification Practice Statement*;
- the *Trust Service Provider* becomes aware that the private key of the *Certificate* issuer certification unit might be compromised;
- 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 *Trust Service Provider* is no longer entitled to issue *Certificate*s, and maintenance is not provided for the existing CRL and OCSP services;
- the supervisory body enacts (smth.) in a legally binding and executable decision;
- the *Trust Service Provider* has terminated its activities;
- the law makes revocation mandatory.

The *Certification Practice Statement* may include additional conditions on which the *Trust Service Provider* revokes the *Certificate*.

The *Trust Service Provider* shall revoke is bound to take action on the revocation of the *Certificate* of the intermediate certification unit in the following cases:

- *Certificate* modification because of data change relating to the certification unit or the *Trust Service Provider*;
- the *Trust Service Provider* becomes aware that it is not in the exclusive possession of the private key;
- the *Trust Service Provider* becomes aware that the *Certificate* is used illegally;
- the *Trust Service Provider* 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 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 *Certificate* was not issued according to the relevant *Qualified Seal Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit does not comply with the relevant *Qualified Seal Certificate Policy* or *Certification Practice Statement*;
- the *Trust Service Provider* 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 *Trust Service Provider* has ended its activities;
- the law makes the revocation mandatory.

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

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:

- *Certificate* modification because of data change relating to the certification unit or the other *Certification Authority*;
- the issuer *Certification Authority* becomes aware that the data indicated in the *Certificate*s do not correspond with reality;
- *Certification Authority* operating the intermediate certification unit notifies the issuer *Certification Authority* that the *Certificate Application* is not approved and its consent is not given afterwards either;
- the operator of the intermediate certification unit requests the revocation of the *Certificate* in writing;
- 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 *Certificate* is used illegally;
- 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 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 issuer *Certification Authority* becomes aware that the *Certificate* is not issued according to the related *Qualified Seal Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit operator does not comply with the relevant *Qualified Seal Certificate Policy* or *Certification Practice Statement*;
- 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 *Certification Authority* operating the certification unit or the issuer *Certification Authority* of its *Certificate* has ended its activities;
- the law makes the revocation mandatory.

The *Certification Practice Statement* can 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 initiated by:

- the *Subscriber*;
- the contact person specified in the service agreement;
- the *Trust Service Provider*.

4.9.3 Procedure for Revocation Request

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

- on paper signed manually at the customer service of the *Trust Service Provider* during office hours in person;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be revoked (see section 1.2.3.);
- in an electronic form with an electronic seal created by the *Certificate* of the *Subscriber* with a security classification not lower than the *Certificate* to be revoked (see section 1.2.3.);
- signed manually, sent by post to the customer service.

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 a successful revocation the *Trust Service Provider* shall notify the *Subject* and the *Subscriber* about the fact.

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.

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 lists shall be to a maximum of 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 lists shall be to a maximum of 12 months.

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation/Status Checking Availability

The *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

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 *Trust Service Provider* shall provide an opportunity for a temporary cessation of the *Certificate*'s usability to reduce the risk in cases it can be assumed that one of the reasons establishing the revocation of the *Certificate* persists.

4.9.14 Who Can Request Suspension

The same requirements apply to the *Certificate* suspension as to the certificate revocation – see Section 4.9.2.

4.9.15 Procedure for Suspension Request

The *Trust Service Provider* shall enable the initiation of the suspension in each day of the year around the clock.

The *Trust Service Provider* shall enable the submission of the suspension requests the same way as the submission of the revocation requests according to the requirements of the Section 4.9.3, except that in this case the the suspension password is used for the validation of the suspension request.

In case of the acceptance of the suspension request, the status change shall be recorded in the *Certificate* status records of the *Trust Service Provider* without delay.

The requirements of Sections 4.9.3 and 4.9.5 regarding Certificate revocation apply to the evaluation of the suspension requests received through other communication channels.

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

The *Trust Service Provider* shall provide the following possibilities for the *Certificate* status query:

- OCSP – online *Certificate* revocation status query service,
- CRL – certificate revocation lists.

The revoked and suspended *Certificate*s shall be listed in the revocation lists.

The suspended *Certificate*s shall be taken out of the revocation list in case of a reinstatement (withdraw of the suspension).

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

The *Trust Service Provider* shall indicate this fact in the revocation list with the use of the optional "expiredCertsOnCRL" extension.

The new status of the *Certificate* shall appear instantly in the revocation records of *Trust Service Provider* in case of suspension, reinstatement and revocation 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 revocation list, the status change shall be disclosed in the next 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 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 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 seal *Certificate*.

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Symmetric Encryption Key Encapsulation and Recovery Policy and Practices

The private key belonging to the seal *Certificate* shall not be escrowed, so regarding that the symmetric encryption keys do not have to be managed.

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;
- entry to the *Data Centre* may happen after the simultaneous identification of two authorized staff members with trusted roles – and at least one of the staff members shall be a system administrator;
- 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* that automatically alert the fire brigade. Manual fire extinguishers of the appropriate type and amount compliant with the relevant regulations should be placed in a visible place in each room.

Automatic fire extinguishers shall be applied in the *Data Centre*.

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.

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. [9] 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, revocation and suspension 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*.

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.

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

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:

- 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, loading, saving, 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 , suspension and revocation;
  - events related to the request processing;
  - every verification activity performed related to the *Certificate* issuance.
  - refusal of the certificate applications;
  - *Certificate* issuance or status change.

- DATA FLOWS:
  - any kind of security-critical data manually entered into the system;
  - security-relevant data, messages received by the system;

- CA CONFIGURATION:
  - re-parameterization , any change of the settings of any component, of the CA;
  - user admission, deletion;
  - changing the user roles, rights;
  - changing the Certificate profile;
  - changing the CRL profile;
  - generation of a new CRL list;
  - generation of an OCSP response;
  - *Time Stamp* generation;
  - exceeding the required time accuracy threshold.
- HSM:
  - installing an HSM;
  - removing an HSM;
  - disposing, destructing an HSM;
  - delivering HSM;
  - clearing (resetting) an HSM;
  - uploading keys, certificates to the HSM.
- CONFIGURATION CHANGE:
  - hardware;
  - software;
  - operating system;
  - patch;
- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the CA components;
  - access to a CA system component;
  - 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 *Qualified Seal Certificate Policy* or 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.

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 on-line 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* and *Certification Practice Statement*s;
- all issued versions of the 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;
- information related to the impersonation of the *Electronic Seal Creation Device*;
- 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:

- *Certification Practice Statement*: 10 years after the repeal;
- All electronic and / or paper-based information relating to Certificates for at least:
  - 10 years after the validity expiration of the Certificate;
  - until the completion of the dispute concerning the electronic seal generated with the certificate;

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 timestamps 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 are top priority.

5.7.3 Entity Private Key Compromise Procedures

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

- all of the affected Certificates of the *Trust Service Provider* shall be revoked;
- new provider private key shall be generated for the restoration of the services;
- the revoked provider Certificates' data shall be disclosed according to the regulated method in Section 2.2 ;
- 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 [22];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [8] 92. § (1) b) .

The *Trust Service Provider* in case of the generation of a key pair of its own shall ensure:

- The creation of the private key of the provider shall be carried out in a protected environment (see section 5.1), with two trusted role holder (see section 5.2.1) authorized person simultaneously, excluding the presence of other unauthorized persons.
- The creation of the provider private key is carried out in a device, that:
  - meets the requirements of ISO/IEC 19790 [25] , or

  - meets the requirements of FIPS 140-2 [33] level 3 or higher, or
  - meets the requirements of CEN 14167-2 [35] workshop agreement,
  - is a reliable system that is evaluated in accordance with MSZ/ISO/IEC 15408 [24] 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.

- The production of provider private key is performed based on a key generation script.
- For the generation of the provider root certification unit private key, an independent auditor is present or video recording is made of the event. The independent auditor certifies that the key generation occurred according to the script.

In case of the generation of the key pair generated for other parties (for example for its trusted role holder employees and for the *Subjects*) by the *Trust Service Provider*, it 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.

In case of provider root and intermediate *Certificate* creation the *Trust Service Provider* should 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 provider root certification unit private key the trusted officer of the *Trust Service Provider* responsible for key management and as a witness a trusted person independent from the operation of the *Trust Service Provider* (eg. notary, auditor) who verify that the record corresponds to the performed process;
- in case of the generation of the provider intermediate certification unit private key the trusted officer of the *Trust Service Provider* responsible for key management who verifies that the record corresponds to the performed process.

6.1.2 Private Key Delivery to Subscriber

If the *Trust Service Provider* generated the *Subject*'s private key, 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

If 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 revocation lists, 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 algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [22];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [8] 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 the *Time-Stamping Unit 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 [32] 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 seal private key may only be used for electronic seal creation by the *Creator of the Electronic Seal*, any other uses of the key are specifically prohibited.

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 store the private keys used for the electronic seal creation in such secure hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [25], or
- the requirements of FIPS 140-2 [33] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [35] task force agreement, or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to MSZ/ISO/IEC 15408 [24] 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 coded 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 [8] 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* shall not escrow its own provider private keys. The end-user seal private keys shall not be escrowed or copied, and multiple usage is not allowed.

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 end-user seal private keys.

6.2.5 Private Key Archival

The *Trust Service Provider* shall not archive its private keys and the end-user seal 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 the end-user private keys generated by the *Trust Service Provider* it shall ensure that the private keys and the private key activation data are generated and managed in a properly secure way that excludes the possibility of the unauthorized usage of the private key.

The *Qualified Electronic Seal Creation Device*s prepared for the *Creator of the Electronic Seal* shall be configured and handled over to the *Applicant* so that:

- it can be clearly established that the device has not been used before the handover;
- before the usage of the private key the *Applicant* shall identify itself towards the *Hardware Security Module*.

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

In case of *Certificate Policies* requiring the use of *Hardware Security Module* the private keys shall be used in accordance with the requirements defined in the used cryptographic module's user guide and in the certification documents.
The *Hardware Security Module* handled over to the *Subject* shall ensure that the private keys become deactivated in the following cases:

- the power supply of the device ceases for any reason ;
- the *Applicant* exits the application
- the *Applicant* gives a deactivation (exit) instruction from the application to the device.

The deactivated key and the *Qualified Electronic Seal Creation Device* may only be used for electronic seal creation after the re-identification of the *Applicant*.
In case of *Certificate Policies* not requiring the use of a *Hardware Security Module* 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 destruction of the discarded signer private keys issued on a *Qualified Electronic Seal Creation Device* is possible by the physical destruction of the *Qualified Electronic Seal Creation Device*, which is the responsibility of the *Applicant*.

For the request of the *Client* in its presence the *Trust Service Provider* is bound to destroy the *Qualified Electronic Seal Creation Device* presented by the *Client* personally free of charge.

In case of *Certificate Policies* requiring the use of a *Qualified Electronic Seal Creation Device* the obsolete private keys shall be destroyed in accordance with the requirements defined in the used cryptographic module user guide and the certification documents. The compliant destruction of the private keys is the responsibility of the *Applicant*.

In case of *Certificate Policies* requiring the use of a *Hardware Security Module* the obsolete private keys shall be destroyed in accordance with the requirements defined in the used cryptographic module user guide and the certification documents. The compliant destruction of the private keys is the responsibility of the *Applicant*.

In case of *Certificate Policies* not requiring the use of a *Hardware Security Module* the proper destruction of the private keys is the responsibility of the *Applicant*.

The discarded seal 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 certification according to ISO/IEC 19790 [25], or
- has a certification according to FIPS 140-2 Level 3 [33], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [35] workshop agreement, or
- has a verification 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 are:

- 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 2 years from issuance;
- 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 expiration date of the provider *Certificate* that issued the *Certificate*.

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

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.

If this happens, the *Trust Service Provider* revokes the related *Certificate*s.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The *Trust Service Provider*'s private keys 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 *Qualified Electronic Seal Creation Device*s and *Hardware Security Module*s provided by the *Trust Service Provider* for the *Applicant*, the *Trust Service Provider* shall provide for:

- the activation data to be created and installed to the *Qualified Electronic Seal Creation Device*s or to the *Hardware Security Module* is generated in a physically secure environment, with an adequate quality random number generator;
- the activation data to be handed over to the *Applicant* using a safe method.

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.

In case of *Qualified Electronic Seal Creation Device*s, *Hardware Security Module*s issued for *Applicant*s by the *Trust Service Provider*, and the software private keys generated for the *Applicant*:

- the *Trust Service Provider* may only record the activation data for the purpose of delivering them to the *Applicant*;

- the *Trust Service Provider* shall distribute the activation data to the *Applicant*s using a secure method.

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:

- are commercial boxed software, designed and developed by a documented design methodology, 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* used shall have the right certification;
- at the reception of the *Hardware Security Module*, 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* against tampering shall be ensured during storage;
- during the operation the requirements of the *Hardware Security Module* appropriation of security, user guide and the certification report shall be continuously observed;
- the private keys stored in the discarded *Hardware Security Module*s shall be deleted in a way that it is practically impossible to restore the keys.

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 disable unused network ports and services ;
- shall only run network applications unconditionally necessary for the proper operation of the IT system .

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 once per quarter.

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 the provider certification unit (root and intermediate) *Certificate*s used during the service shall comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [32]
- RFC 5280 [29]
- RFC 6818 [30]
- ETSI EN 319 412-1 [17]
- ETSI EN 319 412-3 [19]
- ETSI EN 319 412-5 [21]

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 [32].

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* 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 byte 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 *Trust Service Provider* 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 X.501 name format.
- Valid From & Valid To
  The beginning and the end of the validity period of the *Certificate*. The time is recorded according to UTC and compliant with RFC 5280 encoding.
- Subject
  The unique name of the *Subject* according to the X.501 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 [32] , 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 value shall be: "keyCertSign", "cRLSign".

- Extended Key Usage – not critical
  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 contains the identifier of the valid certification policy (see section 1.2.1.) at the time of the intermediate certification unit *Certificate* issuance and usage, and other information on the other uses of the *Certificate*.

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

  In case of *Certificate*s issued to the intermediate certification units of the *Trust Service Provider*, the "anyPolicy" Identifier can 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
  The further scope definition of the approved key usage. Shall not be present.

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

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1
  The definition of the other services related to the usage of the *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);
  – the availability of the *Certification Practice Statement*;
  – the textual warning in English and Hungarian [1] from which it can be established that:

[1] The same information is also stored in a computer-processable form in the Qualified *Certificate* Statements extension also indicated on the *Certificate*.

    - the *Certificate* is qualified;
    - the private key related to the *Certificate* is protected by a *Qualified Electronic Seal Creation Device* (exclusively in case of policies requiring the usage of *Qualified Electronic Seal Creation Device*);
    - the one-time maximum rate of the obligations that can be undertaken;
    - the preservation time of the data related to the *Certificate*.
  - the identifier (OID) of the certification policy specified by the ETSI EN 319 411-2 [16] , which the *Certificate* complies with too. The certification policies specified by the ETSI EN 319 411-2 are the following:
    - QCP-l: Policy for EU qualified *Certificate* issued to a legal person;
    - QCP-l-qscd: Policy for EU qualified *Certificate* issued to a legal person where the private key and the related *Certificate* reside on a qualified seal creation device.

  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 end-user *Certificate*s the field is mandatory and the value shall be exclusively set to: "nonRepudiation";

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

  Shall not be filled.

- 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.

  Mandatory in case of end-user *Certificate*s.

- 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.

- Qualified *Certificate* Statements – not critical
  OID: 1.3.6.1.5.5.7.1.3
  The field is intended for the indication of statements related to the qualified *Certificate*s, but it has a field, that can be used in case of a non-qualified *Certificate* too.

  The following statements shall be present in every end-user qualified *Certificate*:

- the *Certificate* is an EU qualified *Certificate* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
- the transactional limit related to the *Certificate* – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2) - optional;
- that statement that the *Trust Service Provider* retains the registration data related to the *Certificate* for 10 years after the expiration of the *Certificate* – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
- that statement that the private key related to the *Certificate* resides inside a *Qualified Electronic Seal Creation Device* – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – only in the case of certification policies requiring the use of a *Qualified Electronic Seal Creation Device*;
- the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the end-user *Certificate* – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
- that indication that the *Certificate* was issued for sealing (the value of the field is 'id-etsi-qct-eseal') – 'id-etsi-qcs 6' (0.4.0.1862.1.6);

Other *Certificate* extension shall not be used.

Certificate issued for Time-Stamping Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field contains the identifier of the valid certification policy (see section 1.2.1.) at the time of the *Time-Stamping Unit Certificate* issuance and usage, and other information on the other uses of the *Certificate*.

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

  The reference to the related *Certification Practice Statement* can be given in this field.

- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic signature or seal certifying the *Certificate*. Filling in is mandatory.

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

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

  Filling in is mandatory.

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

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

  The default value of the extension is: CA = "FALSE", so this field shall not be present in the *Certificate* issued for the *Time-Stamping Unit*.

  The "pathLenConstraint" field shall not be present in the *Certificate* issued for the *Time-Stamping Unit*.

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

  In the *Certificate*s issued to the *Time-Stamping Unit* this field shall be mandatory and exclusively set to: "nonRepudiation", "digitalSignature".

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

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

- Extended Key Usage – critical
  The further scope definition of the approved key usage. In the *Certificate*s issued to the *Time-Stamping Unit* this field shall be mandatory and exclusively set to:

  "timeStamping" (1.3.6.1.5.5.7.3.8).

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

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1 The definition of the other services related to the usage of the time-stamping unit *Certificate* provided by *Certification Authority*.

  Mandatory, and the field contains the following data

  - For the purpose of the fast and reliable verification of the current *Certificate* revocation status, the *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 protocol of the *Certificate* of the *Certificate* issuer certification unit.

- Qualified *Certificate* Statements – 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.

  The following statements shall be present in the *Certificate* of the time-stamping unit:

  - the *Certificate* is an EU qualified *Certificate* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
  - the transactional limit related to the *Certificate* – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2) - optional;
  - that statement that the *Trust Service Provider* retains the registration data related to the *Certificate* for 10 years after the expiration of the *Certificate* – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
  - the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the *Time-Stamping Unit Certificate* – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
  - that indication that the *Certificate* was issued for sealing – 'id-etsi-qcs 6' (0.4.0.1862.1.6) (the value of the field is 'id-etsi-qct-eseal' (2));

There shall not be any more *Certificate* extension.

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 RFC 5280 [29], ETSI EN 319 412-2 [18], ETSI EN 319 412-3 [19] and ETSI EN

319 412-4 [20] – 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 on-line 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 revocation lists according to the RFC 5280 [29] specification.

7.2.2 CRL and CRL Entry Extensions

The revocation lists issued by the *Certification Authority* shall compulsorily include the following fields:

- Version
  The value of the field is compulsorily "1".
- Signature Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for creating the electronic signature or seal certifying the revocation list . The minimal cryptographic algorithm sets to be supported:
  - "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 *Certification Authority* certifying the revocation list. The given certification unit shall certify the revocation list with its key used for signing the *Certificate*s.
- Issuer
  The unique identifier of the revocation list issuer certification unit.
- This Update (thisUpdate)
  The date of the entry into force of the revocation list. Value according to UTC with encoding according to RFC 5280 [29].
- Next Update (nextUpdate)
  The issuance time of the next revocation list (see Section 4.10.). Value according to UTC with encoding according to RFC 5280 [29].
- Revoked *Certificate*s
  The list of the suspended or revoked *Certificate*s with the serial number of the *Certificate* and with the suspension or revocation time.

The revocation list extensions to be filled in by *Certification Authority* as mandatory:

- CRL number – not critical
  The consecutive serial numbers of the revocation lists shall be in this field.

This extension may be used by the *Certification Authority*:

- expiredCertsOnCRL – not critical
  The *Certification Authority* shall indicate with a standard notation according to the X.509 specification that it does not remove the expired *Certificate*s from the CRL. (See Section 4.10.)

The certificate revocation list entry extensions that may be used by the *Certification Authority*:

- Reason Code – not critical
  The reason of the revocation can be in this field.

  In case of suspended certificates, it is a mandatory field, its value is: "certificateHold (6)".

- Invalidity Date – not critical
  The time when the private key became compromised can be in this field.

- Hold Instruction – not critical
  The management of the suspended certificate can be in this field.

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 RFC 2560 [26] and RFC 6960 [31] 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 digital signature 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 RFC 5280 [29].

- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response. Value according to UTC with encoding according to RFC 5280 [29]. Optional.

- *Certificate* Status Response (SingleResponse)
  The field contains the ID of the *Certificate* (CertID) and the revocation status of 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 suspended or revoked.

7.3.1 Version Number(s)

The *Trust Service Provider* shall support the "v1" version according to the standards RFC 2560 [26] and RFC 6960 [31] 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 RFC 6960 [31] 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.

  In case of suspended certificates it is a mandatory field, its value shall be: "certificateHold (6)".

8 Compliance Audit and Other Assessments

The operation of the *Trust Service Provider* is supervised by the National Media and Infocommunications Authority in line with European Union regulations. The National Media and Infocommunications Authority holds site inspections on at least yearly basis at the *Trust*

Service Provider location. Before the site inspection, the *Trust Service Provider* shall have a screening of its operations by an external auditor and shall send the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the *Trust Service Provider* meets the requirements of the eIDAS Regulation [1] and the related Hungarian legislation and the requirements of the applied *Qualified Seal Certificate Policy*(s) and the corresponding *Certification Practice Statement*(s).

The subject and methodology of the screening shall comply with the following normative documents:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [14]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [13]
- ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [15]
- ETSI EN 319 411-2 v2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [16]

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 *Qualified Seal 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.

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 can be 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*, and it issued a provider *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.

The independent auditor shall report the revealed serious derogations without delay to the National Media and Infocommunications Authority that is authorized to take the necessary measures.

The *Trust Service Provider* shall answer the problems stated by the independent auditor in writing, and to report the measures taken to avert them at the occasion of the next authority review.

The independent auditor shall send the assessment report in each case to the National Media and Infocommunications Authority.

8.6 Communication of Results

The *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 on-line 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 on-line 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 comply with the financial and liability requirements below.

9.2.1 Insurance Coverage

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

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

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 injured 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 [6] and the 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 *Applicant*.

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

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

The present *Qualified Seal 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 *Qualified Seal Certificate Policy*, in the related *Certification Practice Statement* and in the service agreement concluded with the *Client*.

- The *Trust Service Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Trust Service Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;
- The *Trust Service Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [7] in relation to the *Client*s which are in a contractual relationship with it.
- The *Trust Service Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [7] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.

- The *Trust Service Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8.).

Certification Authority Obligations

The *Trust Service Provider* shall fulfil the requirements defined in section (2) of article 24. of the eIDAS regulation [1].

The *Trust Service Provider*'s basic obligations is that it shall provide the services in line with the *Qualified Seal Certificate Policy*, this *Certification Practice Statement* and other regulations in the public domain, the contractual 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 to manage and make available smart cards, 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 Certification 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*;
- for the relationship of the *Electronic Seal Creation Device* activation code and the keys uploaded to the device;
- in general for the compliance with its obligations.

9.6.2 RA Representations and Warranties

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

The responsibilities of the *Registration Authority* are:

- to determine the identity of the person authorized to represent the *Applicant*s;
- 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 *Qualified Seal 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 *Qualified Seal 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 *Certificate*;
- to provide immediate information on the changes of its data;
- using its *Electronic Seal Creation Device*, 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 *Qualified Seal 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 suspension or revocation of the *Certificate* and
  - terminate the usage of the *Certificate*;
- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents;
- 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

  any of the electronic seal or 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;
- the *Applicant* shall 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 and/or suspension 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 the *Trust Service Provider* revokes the issued *Certificate* in case it 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*;

- acknowledge that the *Trust Service Provider* has the right to suspend, and revoke *Certificate*s if the *Subscriber* fails to pay the fees of the services by the deadline;
- acknowledge that the *Trust Service Provider* has the right to suspend, and revoke *Certificate* if the *Subscriber* violates the service agreement or the *Trust Service Provider* becomes aware that the *Certificate* was used for an illegal activity.

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 *Qualified Seal Certificate Policy* and the corresponding *Certification Practice Statement*;
- use reliable IT environment and applications;
- verify the the *Certificate* revocation status 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 *Qualified Seal Certificate Policy* and the *Certification Practice Statement*.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The *Trust Service Provider* excludes its liability if:

- *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.

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

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 *Qualified Seal Certificate Policy* is specified on the cover of the document.

9.10.2 Termination

The *Qualified Seal Certificate Policy* is valid without a time limit until withdrawal.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Qualified Seal 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 *Qualified Seal 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 *Qualified Seal 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 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* 30 days prior to the planned entry into force date and it will be sent for review to the National Media and Infocommunications Authority .

The *Trust Service Provider* will accept remarks connected to new regulations published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

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

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

9.12.2 Notification Mechanism and Period

The *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 a new version number in case of even the smallest change to the *Qualified Seal Certificate Policy* , which is part of the document identifier (OID), so any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

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 *Qualified Seal 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 CCXXII of 2015 on electronic administration and the general rules of trust services [8];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [9];
- (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates [10];
- (Hungarian) Ministry of Interior Decree 26/2016. (VI. 30.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body [11];
- (Hungarian) Government Decree 137/2016. (VI. 13.) on the requirements for the use of electronic signatures and seales related to the provision of electronic administration services [12];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [13];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [6];
- (Hungarian) Act V of 2013. on the Civil Code. [7].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

The providers operating according to this *Qualified Seal 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 *Qualified Seal 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 *Qualified Seal 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 *Qualified Seal 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 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 III of 1952 on Civil Procedure .

[4] (Hungarian) Act LXVI of 1992 on the registration of citizens' personal data and address .

[5] (Hungarian) Act II of 2007 on the entry and residence of persons enjoying the right of free movement and residence .

[6] (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information .

[7] (Hungarian) Act V of 2013. on the Civil Code .

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

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

[10] (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates .

[11] (Hungarian) Ministry of Interior Decree 26/2016. (VI. 30.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body .

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

[13] ETSI EN 319 401 V2.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[14] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[15] ETSI EN 319 411-1 V1.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[16] ETSI EN 319 411-2 v2.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[17] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[18] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[19] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[20] ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

[21] ETSI EN 319 412-5 V2.2.0 (2017-08); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[22] ETSI TS 119 312 V1.2.1 (2017-05); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

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

[24] MSZ/ISO/IEC 15408-2002 "Information Technology - Methods and Means of a Security - Evaluation Criteria for IT Security" .

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

[26] IETF RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999.

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

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

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

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

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

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

[35] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

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