MICROSEC

e-Szignó Certification Authority

eIDAS conform
Qualified Certificate for Electronic Signature
Certification Practice Statement

ver. 2.2

Date of effect: 30/10/2016

OID	1.3.6.1.4.1.21528.2.1.1.92.2.2
Version	2.2
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	30/09/2016
Date of effect	30/10/2016

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	eIDAS conformity. OID: 1.3.6.1.4.1.21528.2.1.1.92.2.0	01/07/2016	Csilla Endrődi, Szabóné Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments. OID: 1.3.6.1.4.1.21528.2.1.1.92.2.1	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.
2.2	Changes according to the auditor comments.	30/10/2016	Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document is the *Certification Practice Statement* concerning the qualified signing service of e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or *Provider*).

The *Provider* provides its services for its *Client*s those have contractual relationship.

The present *Certification Practice Statement* describes the framework of the provision of the aforementioned services and includes the detailed procedures and miscellaneous operating rules.

It makes recommendations for the *Relying Parties* for the verification of the electronic signatures and *Certificate*s created by the services.

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

Microsec asked for its registration as a trust service proider at the National Media and Infocommunications Authority on the 1st of July 2016.

1.1 Overview

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

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

Furthermore the role of present document is to help the users and acceptors of *Certificate*s, *Certificate* revocation lists and online *Certificate* status responses issued by the *Provider* in the clear identification of the ways of managing them, the level of security guaranteed by them as well as the relevant technical, commercial, financial guarantees and legal responsibility related to them. The content and format of the present document complies with the requirements of the RFC 3647 [24] framework. It consists of 9 sections that contain the security requirements, processes defined by the *Provider* and the practices to be followed during the provision of services. To strictly preserve the outline specified by RFC 3647, section headings where the document does not impose a requirement have the statement "No stipulation".

Requirements for end user activity related to the used services can be contained besides the present *Certification Practice Statement* in the General Terms and Conditions the service agreement concluded with the provider, the Certificate Policies applied by the *Provider* (see section 1.2.1), the *Time-Stamping Policy* [37] and other regulation or document independent from the *Provider* as well.

1.2 Document Name and Identification

Issuer	e-Szignó Certification Authority
Document name	eIDAS conform Qualified Certificate for Electronic Signature Certification Practice Statement
Document version	2.2
Date of effect	30/10/2016

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

1.2.1 Certificate Policies

All *Certificate*s issued by the *Provider* refers 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 *Provider* issues *Certificate*s according to the following *Certificate Policies* based on the present *Certification Practice Statement*:

OID	DENOMINATION	SHORT NAME
1.3.6.1.4.1.21528.2.1.1.42.2.2	Qualified, for the generation and verification of electronic signatures, for natural persons issued on *Qualified Electronic Signature Creation Device*, Certificate Policy prohibiting the use of pseudonyms.	MATBN
1.3.6.1.4.1.21528.2.1.1.43.2.2	Qualified, for the generation and verification of electronic signatures, for natural persons issued on *Hardware Security Module*, Certificate Policy prohibiting the use of pseudonyms.	MATHN
1.3.6.1.4.1.21528.2.1.1.44.2.2	Qualified, for the generation and verification of electronic signatures, for natural persons issued as a software token , Certificate Policy prohibiting the use of pseudonyms.	MATSN
1.3.6.1.4.1.21528.2.1.1.48.2.2	Qualified, for the generation and verification of electronic signatures, for natural persons controlling the issuance of Certificates, pseudonymous Certificate Policy.	MATxA

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

- First character [Xxxxx]
  - M: qualified *Certificate Qualified Signature Certificate Policy*
  - N: non-qualified *Certificate Qualified Signature Certificate Policy*
  - H: non-qualified, III. certificate class *Certificate Qualified Signature Certificate Policy*
  - K: non-qualified, II. certificate class *Certificate Qualified Signature Certificate Policy*
  - A: non-qualified, automatic issuance *Certificate Qualified Signature Certificate Policy*
  - x: no stipulation
- Second character [xXxxx]
  - A: Signing purpose *Certificate Qualified Signature Certificate Policy*

  - B: Seal creation purpose *Certificate Qualified Signature Certificate Policy*
  - W: *Website Authentication Certificate Qualified Signature Certificate Policy*
  - K: Code signing *Certificate Qualified Signature Certificate Policy*
  - x: no stipulation

- Third character [xxXxx]
  - T: *Certificate* issued to a natural person *Qualified Signature Certificate Policy*
  - J: *Certificate* issued to a legal person *Qualified Signature Certificate Policy*
  - x: no stipulation

- Fourth character [xxxXx]
  - B: *Certificate* issued on *Qualified Electronic Signature Creation Device Qualified Signature Certificate Policy*
  - H: *Certificate* issued on *Hardware Security Module Qualified Signature Certificate Policy*
  - S: *Certificate* issued by software *Qualified Signature Certificate Policy*
  - x: no stipulation

- Fifth character [xxxxX]
  - A: pseudonymous *Certificate Qualified Signature Certificate Policy*
  - N: pseudonym excluding *Certificate Qualified Signature Certificate Policy*
  - x: no stipulation

The detailed requirements of the listed *Qualified Signature Certificate Policy*(s) are in "e-Szignó Certification Authority - eIDAS conform Qualified Electronic Signature Certificate Policies ver. 2.2." [36]

In case of *Certificate Policies* concerning *Certificate*s issued to natural persons, the *Subject* is always a natural 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*)

In case of *Certificate Policies* prohibiting the use of pseudonyms, the real name of the *Subject* is indicated on the *Certificate*, while in case of pseudonymous *Certificate Policies* the alias is indicated on the *Certificate* in all cases.

In case of *Certificate Policies* ([xxxBx]) requiring the usage of a *Qualified Electronic Signature Creation Device*, the *Provider* shall make sure that the private key associated with the *Certificate*

is located in a *Qualified Electronic Signature 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 *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 Signature Creation Device*;
- Common Criteria [31] certification according to CEN SSCD PP [33], at least at level EAL4;
- FIPS 140-2, Level 2 (or higher) certification [30]

or

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

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

*Certificate*s that comply with *Certificate Policies* that require the usage of a *Qualified Electronic Signature Creation Device* or *Hardware Security Module* can be issued within the confines of the key storage service, if the technical solution used has the required *Qualified Electronic Signature Creation Device* or the *Hardware Security Module* certification.

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

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

A document, with a qualified electronic signature or with advanced electronic signature based on a qualified *Certificate* under paragraph 196 Act III of 1952 on Civil Procedure [2] is representing conclusive evidence.

The qualified *signing Certificate*s issued in accordance with the [MATBN], [MATHN], [MATSN] *Certificate Policies* fully comply with the requirements of the related legislation, so that the private keys belonging to them can be used for the generation of the electronic signatures made by the client as well as by the administration contributor, a person who is not entitled to issue documents (clerk).

The *Provider* provides the validation possibilities of the data necessary for personal identification according to legislative requirements (see Section 4.13) in case of these *Certificate*s.
Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [QCP-n] *Certificate Policy* defined in the ETSI EN 319 411-2 [14] standard;
- the [MATBN] *Certificate Policy* complies with the [QCP-n-qscd] *Certificate Policy*.

Compliance with the ETSI Certificate Policies

	[QCP-n]	[QCP-n-qscd]
MATBN	X	X
MATHN	X	
MATSN	X	
MATxA	X	

1.2.2 Effect

Subject Scope

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

Temporal Scope

The present version of the *Certification Practice Statement* is effective from the 30/10/2016 date of effect, until withdrawal. The effect automatically terminates at the cessation of services.

Personal Scope

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

Geographical Scope

The present *Certification Practice Statement* includes specific requirements for services primarily provided for Hungarian *Client*s, operating by the Hungarian law in Hungary in Hungarian language. The *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.

1.2.3 Security Levels

The *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 Signature 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 *Provider* established the following aggregated order in descending order of security:

- qualified *Certificate*s issued on *Qualified Electronic Signature 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 *Provider* supports the use of electronic channels and enables the use of electronic signature during the administration in most cases possible.

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

On an individual basis in special cases, the *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

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

- the Microsec e-Szignó Certification Authority,
- the *Registration Authority* in a contractual relationship with Microsec e-Szignó Certification Authority,
- the *Client*s of Microsec e-Szignó Certification Authority (*Subscriber*s and *Subject*s),
- *Relying Parties*,
- other participants.

1.3.1 Certification Authorities

Data of the *Provider*

Name	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number	01-10-047218 Company Registry Court of Budapest
Head office	1031 Budapest, Záhony street 7. D. building
Telephone number	(+36-1) 505-4444
Fax number	(+36-1) 505-4445
Internet address	`https://www.microsec.hu`, `https://www.e-szigno.hu`

Contact information of the customer service:

The name of the provider unit	e-Szigno Certification Authority
Customer service	1031 Budapest, Záhony str. 7., Graphisoft Park, D building
Office hours of the customer service	on workdays between 8:30-16:30 by prior arrangement
Telephone number of the customer service	(+36-1) 505-4444
E-mail address of the customer service	info@e-szigno.hu
Service related information access	`https://www.e-szigno.hu`
Place for registering complaints	Microsec zrt. 1031 Budapest, Záhony str. 7., Graphisoft Park, D building
Relevant Consumer Protection Inspectorate	Budapest Capital Authority for Consumer Protection 1052 Budapest, Városház str. 7. 1364 Budapest, Pf. 144.
Relevant Arbitration Board	Arbitration Board of Budapest 1016 Budapest, Krisztina krt. 99. III. em. 310. 1253 Budapest, Pf.: 10.

Introduction of the *Provider*

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

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [3] (hereinafter: Eat.):

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

On the 1st of July, 2016. the whole system of services related to electronic signatures changed uniformly on a European basis with eIDAS and its complement Act CCXXII of 2015. [6] coming into force. Microsec continuously migrates its services in accordance with the new eIDAS requirements.

From the 1st of July, 2016 :

- starts the issuance of eIDAS qualified signing certificates for natural persons;

- starts the issuance of eIDAS non-qualified signing, seal and webserver certificates;
- in accordance with the transitional provisions, it provides on a national qualified level until obtaining the final eIDAS certificate the issuance of signing certificates for organizations, time stamping and long term preservation services.

Quality and Information Security

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

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

Business Providing Certification Services

Operating as an independent business unit within the organization of Microsec, the e-Szignó Certification Authority provides the *Certificate* creation and management, the *Certificate* revocation information issuance, the *Electronic Signature Creation Device* and the provision of the online certificate status service. The tasks related to the management of the regulations is provided by this unit too. The e-Szignó Certification Authority has its own *Registration Authority*, but does not exclude the cooperation with an external *Registration Authority* either.

Services

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

- Issuance of Qualified Certificates for Electronic Signatures

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

The Issuance of Qualified Certificates for Electronic Signatures Service

The *Provider* to provide the Issuance of Qualified Certificates for Electronic Signatures service signs a service agreement with the *Subscriber* , within the confines of it issues a qualified *Certificate* suitable for electronic signature generation to the *Subject*s specified by the *Subscriber*. The

Certificate provides a certified connection between the data of the identified *Subject* and the public signature verifier data of the signature generation data that the *Subject* holds. Within the framework of a service agreement, multiple *Certificate*s can be issued to the *Subject*.

In case of using a qualified *Certificate* issued based on present *Certification Practice Statement*, if the electronic signature was created by a *Qualified Electronic Signature Creation Device*, the electronic signature is a qualified electronic signature. If the electronic signature was not created by a *Qualified Electronic Signature Creation Device* then the electronic signature is an advanced electronic signature based on qualified certificate. A document verified by a qualified electronic signature or an advanced electronic signature based on a qualified certificate under the 196. § of the Act 1952 - III on Civil Procedure [2] considered as a private document providing a full probative value.

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

- *Subject* may apply for a *Certificate* (and a *Electronic Signature Creation Device* in addition) from the *Provider*, the *Certificate* issuance is performed according to a *Certificate Policy* or policies;
- the *Subject* may request the revocation of its *Certificate*;
- the *Subject* may request the suspension and reinstation of its *Certificate*.

The *Subscriber* may also request the revocation, suspension or reinstation of the belonging *Subject*'s *Certificate*. These actions may also be requested by the organizational administrator authorized by the *Subscriber* and registered by the *Provider*.

The *Provider* makes the revocation lists publicly available, containing the revocation status of the issued *Certificate*s. The *Provider* also makes the *Certificate* public, according to the *Subject*'s consent. The suspended, revoked or expired *Certificate* is invalid. Signatures created with an invalid *Certificate*s do not have any legal effect.

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

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

Certificate Types

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

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

- *Organizational Certificate* means a *Certificate*

  wherein the *Subject* is an *Organization*, a device under the control of the *Organization* or the *Certificate* attests the relationship of a natural person *Subject* with the *Organization*. In this case, the name of the *Organization* is indicated in the "O" field of the *Certificate*. This type of a *Certificate* can only be used as specified by the *Organization*.

  In case of an *Organizational Certificate* issued to a natural person, further restrictions can be indicated in the "Title" field, related to the usage of the *Certificate*.

- *Certificate for Automatism* means a *Certificate* wherein the denomination of the IT device (application, system) is indicated amongst the *Subject* data in the *Certificate*, by the help of the *Subject* uses the *Certificate*.

- Pseudonymous *Certificate* means a *Certificate* wherein not the official denomination of the *Subject* is in the *Certificate*. In the pseudonymous *Certificate*s the requested name is indicated in the "Pseudonym" field, and it is stated in the "CN" field that the *Certificate* contains a pseudonym.

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

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

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

Test Certificates

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

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

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

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

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

Device Service

Within the confines of the device service *Provider* puts the *Certificate* related signature-creation data of the *Subject* on an *Electronic Signature Creation Device* which complies with the *Qualified Electronic Signature Creation Device* requirements defined in eIDAS regulation [1]. The usage of these *Qualified Electronic Signature Creation Device*s is prerequisite for the creation of qualified electronic signatures.

Certification Units

The following contains a list of *Certification Unit*s appearing in the system of the e-Szignó Certification Authority under the effect of this *Certification Practice Statement*. Further information can be found in the the certificate hierarchy of the *Provider* at the following address: `https://e-szigno.hu/en/pki-services/ca-certificates.html`

The following certification units of the *Provider* issue *Certificate*s:

- "Microsec e-Szigno Root CA 2009" – Root certification unit, that issues SHA-256 based *Certificate*s for the *Certification Unit*s of the *Provider*. This *Certification Unit* has a self certified (SHA-256 based) certificate.
- "Qualified e-Szigno CA 2009", productive qualified *Certification Unit*, certified by the "Microsec e-Szigno Root CA 2009". This certification unit issues *Certificate*s according to pseudonym excluding qualified ([MATB] OID:1.3.6.1.4.1.21528.2.1.1.42.2.2) *Certification Unit*.
- "Qualified e-Szigno QCP CA 2012", productive qualified *Certification Unit*, certified by the "Microsec e-Szigno Root CA 2009". This *Certification Unit* issues *Certificate*s according to certificate policies that do not require that the private key belonging to the *Certificate* shall reside inside of a *Qualified Electronic Signature Creation Device*.
  - OID:1.3.6.1.4.1.21528.2.1.1.43.2.2 [MATHN];

  - OID:1.3.6.1.4.1.21528.2.1.1.44.2.2 [MATSN];
  - OID:1.3.6.1.4.1.21528.2.1.1.82.2.2 [MBJHN];
  - OID:1.3.6.1.4.1.21528.2.1.1.83.2.2 [MBJSN];

  This *Certification Unit* issues pseudonymous and non-pseudonymous *Certificate*s for natural and non-natural persons.

- "Qualified Pseudonymous e-Szigno CA 2009", productive qualified *Certification Unit*, certified by the "Microsec e-Szigno Root CA 2009". This *Certification Unit* issues *Certificate*s according to the pseudonymous qualified ([MATxA] OID:1.3.6.1.4.1.21528.2.1.1.48.2.2) certificate policy.

- OCSP responders; every *Certification Unit* with SHA-256 based *Certificate* certifies dedicated OCSP responder *Certification Unit*, which gives responses regarding the revocation status of the Certificates issued by the given certification unit. The OCSP responder units name contains the "OCSP Responder"text besides the given certification unit name. The "OCSPSigning" extended key usage is present in the OCSP responder *Certificate*s.

The following *Certification Unit*s of the *Provider* do not issue *Certificate*s anymore:

- "Qualified KET e-Szigno CA 2009", productive qualified *Certification Unit*, issues *Certificate*s according to public administrative certificate policies certified by KGYHSZ (Public Administration Root).

The aforementioned units have SHA-256 based Certificates, and issue SHA-256 based SHA-256 *Certificate*s, and OCSP responses. Every provider and end-user RSA key is at least 2048 bit in the hierarchy above.

The *Provider* issued SHA-1 *Certificate*s based "Microsec e-Szigno Root CA" *Certification Unit* beforehand. The *Provider* does not issue *Certificate*s according to this hierarchy. The *Provider* keeps the SHA-1 based hierarchy for the verifiability of the previously created signatures and *Time Stamp*s. The following *Certification Unit*s are in the hierarchy:

- "Microsec e-Szigno Root CA" – Root certification unit, which issued SHA-1 based *Certificate*s to the *Certification Unit*s of the *Provider*. This *Certification Unit* has a self-certified certificate.

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

- "Qualified e-Szigno PCA", productive qualified *Certification Unit*, cross-certified by the "Microsec e-Szigno Root CA" root *Certification Unit*. This *Certification Unit* issued certificates according to the pseudonymous qualified certificate policy.
- "Qualified e-Szigno CA7", productive qualified *Certification Unit* cross-certified by the Public Administration Root CA. With this *Certification Unit* the *Provider* issued qualified certificates exclusively according to administrative certificate policies with this certification unit.
- "Microsec e-Szigno Server CA", the "Microsec e-Szigno Root CA" root *Certification Unit*, and the KGYHSZ certifies it. This *Certification Unit* cross-certified the SHA-1 based time stamp issuer time stamp units.
- "e-Szigno OCSP CA" (self-certified) – The OCSP responder certificate issuer *Certification Unit*.
- "e-Szigno OCSP Responder" – OCSP responder – certified by "e-Szigno OCSP CA".

Intermediate *Certification Unit*s in the SHA-1 based hierarchy issue "closing CRLs", with a validity date (`nextUpdate`) that is equal to the expiry date of the issuing *Provider*.

For the uninterrupted verification of formerly created signatures and time stamps SHA-1-based revocation information was available for SHA-1-based *Certificate*s until the 31st of December, 2012. Until this date, the *Provider* used SHA-1-based OCSP responder certificates and issued SHA-1-based OCSP responses for the SHA-1-based hierarchy. Since the 1st of January, 2013, the *Provider* uses SHA-256 based OCSP responder certificates and issues SHA-256 based OCSP responses in its SHA-1 based hierarchy.

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

The hash of the root *Certificate*s belonging to "Microsec e-Szigno Root CA" and "e-Szigno OCSP CA" were published by the *Provider* in the July 21, 2005 edition of Magyar Nemzet (a Hungarian daily newspaper), the *Provider* published the hash of the "Microsec e-Szigno Root CA 2009" *Certificate* in the June 17 2010 issue of Expressz (a Hungarian daily newspaper). These root *Certificate*s are available through the webpage of the e-Szignó Certification Authority.

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

- The "e-Szigno OCSP CA" root *Certificate* SHA-1 hash: `56 2c 85 5b 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68`,
  the SHA-1 hash of the same root *Certificate*: `15 a9 45 a5 e4 92 c8 6c 3e 4e 0e a5 81 4c 9c 43 b0 4f 2e a6 83 1a 64 6c 37 8c d2 b1 82 05 aa 89`
- The "Microsec e-Szigno Root CA 2009" root *Certificate* SHA-1 hash [1] :
  `89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e`,
  the SHA-256 hash of the same root:
  `3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8 e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78`

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

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

The "Microsec e-Szigno Root CA 2009" root *Certificate* is contained and distributed by the following certificate stores:

- Apple iOS from the 7.1.2 version.
- Apple Mac OS X from the 10.9.4 version.

The `https://e-szigno.hu/en/pki-services/browser-compatibilty.html` webpage contains more information on other browsers and certificate stores that contain the root certificates of the *Provider* by default.

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

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

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

Chained Certification Service

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

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

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

1.3.2 Registration Authorities

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

Tasks of the office:

- registration of the *Subject* indicated on end user *Certificate*s,

- administration and registration activity related to the issuing of *Certificate*s and *Electronic Signature Creation Device*s
- maintaining contact with *Client*s (reception of questions, announcements, requests and complaints, and the initiation of their processing),
- performance of certificate actions (revocation, suspension, reinstation, certificate renewal, certificate modification and re-key).

The customer service operated by the *Provider* receives requests pertaining to various certificate actions, and initiates their processing. The *Provider* maintains a continuously available standby service for the initiation of suspension – 24 hours a day, every day of the week.

The *Registration Authority* may perform registration activities at the following locations:

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

The *Provider* may also contract other organizations for the creation of external registration offices, or for the operation of mobile registration units which perform specific tasks of the central office at an external location. These external *Registration Authority*s also operate in a controlled way and in accordance with this *Certification Practice Statement*, the *Provider* supervises the controlling system of these organisations.

1.3.3 Subscribers

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

- *Subscriber*:
  - concludes a service agreement with the *Provider*,
  - defines the scope of the *Subject*s ,
  - responsible for the payment of the fees arising from the usage of the service.
- *Subject*: the *Provider* issues the *Certificate* for the *Subject*.
- *Signatory*: the electronic signature certification service user party, who can create electronic signature with the help of the issued *Certificate*.

The *Subject* is the *Signatory*.

1.3.4 Relying Parties

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

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

1.3.5 Other Participants

If a *Certificate* has been issued to the *Subject* in order to be used representing an *Organization* (*Organizational Certificate*issued to natural person) for signing or for its activity, the *Represented Organization* is the actual *Organization* also indicated within the *Certificate*.

The *Provider* does not necessarily have a contractual relationship with the *Represented Organization*, but the *Provider* shall not issue an *Organizational Certificate* without the approval of that *Organization*. The *Provider* can suspend or revoke the *Certificate* at the request of the *Represented Organization*.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The private keys belonging to the end-user *Certificate*s issued by the *Provider* based on the present *Certification Practice Statement* can be only used for electronic signature creation, with the *Certificate*s the *Signatory* can verify the authenticity of the documents signed by him.

The public key in the *Certificate*, the *Certificate* itself, the *Certificate* revocation lists, the *Time Stamp*s and the online revocation status responses can be used for the electronic signature.

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 signature is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Organization name	Microsec e-Szignó Certification Authority
Organization address	Hungary, H-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 *Certification Practice Statement* 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 Signature Certificate Policy*

The provider that issued the *Certification Practice Statement* is responsible for its conformity with the *Qualified Signature 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 *Provider*s applying these policies.

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

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

1.5.4 Practice Statement Approval Procedures

The writing, the acceptance and the issuance of the new or any modified versions of the *Certification Practice Statement* happens according to unified processes – as defined in detail in section 9.12.1.

1.6 Definitions and Acronyms

1.6.1 Definitions

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 safety systems.
Subject	"A person with an identity or attribute verified by the *Trust Service Provider* with the *Certificate*, so the signatory especially in case of an electronic signature certificate. " *(Act CCXXII. of 2015. [6] 1. § point 43.)*
Subject Unique Identifier	The globally unique identifier of the *Subject*, given by the *Provider*. The identifier is in the "Subject DN Serial Number" field of the *Certificate*, according to the requirements of section 3.1.1.
Signatory	"A natural person who creates an electronic signature." *(eIDAS [1] article 3. point 9.)* " A person with an identity or attribute verified by the *Trust Service Provider* with the certificate of the electronic signature. " *(Act CCXXII. of 2015. [6] 1. § point 43.)*
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.
Trust Service Supervisory Body	"The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [6] 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 safety requirements." *(Act CCXXII. of 2015. [6] 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 Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign *(eIDAS [1] 3. article 10. point)*
Certificate for Electronic Signature	"Means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person." *(eIDAS [1] 3. article 14. point)* In case of *Certificate*s issued by the *Provider*, it can be clearly concluded from the *Certificate Policy* related to the *Certificate*s, whether the given *Certificate* is pseudonymous or not. The reference of the *Certificate Policy* is in the *Certificate*.

Qualified Certificate for Electronic Signature	A *Certificate* for electronic signatures issued by a *Qualified Trust Service Provider* and meets the requirements laid down in Annex I of eIDAS [1]. *(eIDAS [1] 3. article 15. point)*
Electronic Signature Creation Data	"Means unique data which is used by the signatory to create an electronic signature." *(eIDAS [1] 3. article 13. point)* Typically, cryptographic private key, formerly known as the signature creation data.
Electronic Signature Creation Device	"Means configured software or hardware used to create an electronic signature." *(eIDAS [1] 3. article 22. point)* Formerly known as signature-creation device (ALE).
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 *Provider* in order to use some of its services.
Relying Party	Recipient of the electronic document, who acts relying on the electronic signature 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. [6] 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 Signature	"Means an electronic signature which meets the following requirements: a/ it is uniquely linked to the signatory; b/ it is capable of identifying the signatory; c/ it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and d/ it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. " *(eIDAS [1] 3. article 11. 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*, the Certificate-Verifier Data and the information on the current state (especially on possible revocation) of the *Certificate*.
Certification Unit	A unit of the *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. [6] 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 *Subject* for the purpose of using it for its activities or for signing 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. [6] at the time of the creation." *(Act CCXXII. of 2015. [6] 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 signatures the *Signatory* generates the signature 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 Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. *(eIDAS [1] article 3. point 12.)*
Qualified Electronic Signature Creation Device	"Means an electronic signature creation device that meets the requirements laid down in Annex II of eIDAS [1]." *(eIDAS [1] article 3. point 23.)* Previously known as Secure Signature Creation Device (BALE).
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 signature, the public key of the signature creator party is needed to verify the signature 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 *Provider* by the *Client* in which the Client authorizes the *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 *Provider*, when the continuation of the normal operation of the *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*.
Organization Administrator	That natural person who is eligible to act during the application, suspension, reinstatement and revocation of the *Certificate*s issued to the *Organization* and to grant the issuance of organization related personal electronic signature *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. [6] 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. [6] 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. [6] 1. § point 44.)*
Certificate Application	The data and statements given by the *Applicant* to the *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 (certificate manager system) on the computer of the *Subject* and the *Relying Party* is also called Certificate Repository.
Server-Based Signature Service	A service in which the Signatory's private key can be found on a properly protected server in a secure cryptographic module that can be used by the Signatory after a properly secured authentication step.
Client	The collective term for the *Subscriber* and every related *Subject* 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* publishes on its webpage (`https://www.e-szigno.hu`) and through LDAP protocol (`ldap://ldap.e-szigno.hu`) its provider *Certificate*s, and those *Certificate*s to the disclosure of which the *Subject* consented to.

The *Provider* publishes the *Qualified Signature Certificate Policy*, the *Certification Practice Statement* and other documents containing the terms and conditions its operation is based on.

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

2.2 Publication of Certification Information

The *Provider* discloses on its webpage its provider *Certificate*s, and those *Certificate*s for the *Relying Parties* to the disclosure of which the *Subject* consented to.

Service Provider Certificates

With the following methods the *Certification Authority* discloses 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*. (see section: 1.3.1.) The information related to their change of status are available at the website of the *Certification Authority*.
- The status change of *Certificate*s of intermediate (non-root) and the *Time-Stamping Unit*s is 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 – issues a *Certificate* with extremely short period of validity (for 10 minutes) thereby eliminating the need for *Certificate* revocation status verification. The revocation status of the OCSP response *Certificate*s is only to be disclosed by the *Provider* such a way that in case of key compromise, or any other problems there won't be any more new *Certificate* disclosed for the OCSP response signer old private key later. The *Provider* discloses OCSP response *Certificate*s for a new, secure private key. For the detailed description of the OCSP response validation see section 4.5.2.

End-User Certificates

With the following methods the *Certification Authority* discloses 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 is disclosed by the *Provider*, and the *Subject*'s consent is not required for it. For status information disclosing methods, see Section 4.10.

The *Provider* discloses the contractual conditions and policies electronically on its website.

The new documents to be introduced are disclosed on the website 30 days before coming into force.

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

The actual version of policies and contractual conditions is readable in printed form at the customer service of the *Provider*.

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

The *Provider* notifies 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 *Certification Practice Statement* related new versions is compliant with the methods described in Section 9.12.

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

The *Provider* publishes 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 *Provider* regarding the disclosure of some *Certificate*s follows the practices below:

- the *Certificate*s of the root certification units operated by it are disclosed before commencing the service;
- the *Certificate*s of the intermediate certification units operated by it are disclosed within 5 workdays after issuance;
- the *Certification Authority* discloses in case of the *Subject*'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 *Provider* and the provider *Certificate*s are available immediately within the confines of the online certificate status service.

The information related to the status of the *Certificate*s are disclosed in the Certificate Repository on the certificate revocation lists. The practices related to the issuance of the certificate revocation lists are discussed in Section 4.10.

2.4 Access Controls on Repositories

Access is 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 applied *Certificate Policies*.

The indicated Issuer ID and the Subject ID amongst the basic fields of the Certificate comply with the RCF 5280 [26] and RFC 6818 [27] recommendations name-specific format requirements, in addition the *Provider* supports the Subject Alternative Names and Issuer Alternative Names fields located amongst the extensions.

3.1.1 Types of Names

Denomination of the *Subject*

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

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

  In case of natural persons, the name of the natural person is in this field in the same form as in a public registry. 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*)

  If pseudonym is indicated on this field in the *Certificate*, then the "pseudonymous certificate" text (or the equivalent in a foreign language), and the pseudonym itself is in the pseudonym (PSEUDO) field.

  Always filled out.

- Surname – OID: 2.5.4.4 – Surname of the natural person
  The surname of the *Subject* is in this field , where the *Provider* generates the surname from the full name in the CN field.

  In case of pseudonymous certificate, the *Provider* does not fill this field.

  Always filled out.

- Given Name – OID: 2.5.4.42 – The first name of the natural person.
  The first name of the *Subject* is in this field

  , where the *Provider* generates the first name from the full name in the CN field.

In case of pseudonymous certificate, the *Provider* does not fill this field.

Always filled out.

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

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

  The pseudonym freely chosen by the *Subject* is indicated in this field.

  The *Provider* does not verify the pseudonym. The usage of the pseudonym only affects the PESUDO field, every other field is filled with real values verified by the *Provider*.

  If the Pseudonym field is filled, then in the "CN" field, it is indicated that the certificate contains a pseudonym.

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

  The indication of at least one filled out "Serial Number" field is in the *Certificate* which complies with the following requirements, so that it is able to form a part of the *Subject* permanent unique identifier in case of the usage of "Permanent Identifier" extension according to the RFC 4043 [25] recommendation:

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

  – the *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.

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

  The unique identifiers issued by the *Provider* to the *Subject* are OID formatted: "1.3.6.1.4.1.21528.2.x.y.z".

  – In it, the first numbers are fixed (1.3.6.1.4.1.21528.2.2: is the unique identifier of the *Provider*),

  – "x" is the inner identifier used by the *Provider*,

  – "y" is the inner identifier used by the *Provider*,

  – "z" is an automatically issued, a unique identifier within a specific "x.y" value pair.

  So the "x.y.z" value pair is the the Subject unique identifier within the system of the Certification Authority.

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

This identifier is part of the "Permanent Identifier" according to RFC 4043 [25] recommendation if the *Certificate* "Subject Alternative Names" field contains the "assigner" but not the "identifierValue" according to RFC 4043 recommendation.

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

The *Provider* only issues a pseudonymus Certificate for a fresh OID.

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

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

In case of *Certificate*s issued to lawyers, the *Provider* indicates the name of the Bar Association that the lawyer is a member of, and the ID assigned to the lawyer by the Bar Association (registration number, KASZ (Bar Association identification number)).

In the Serial Number the *Provider* – compliant with the standards – does not indicate accents.

These other fields can be considered as the *Subject*'s unique identifiers, but the forefront OID formatted identifier fulfils the identifier role according to RFC 4043.

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

  In case of an *Organizational Certificate* the *Organization*'s full or shortened name is indicated in the "O" field according to the deed of foundation or a public register.

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

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

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

- Organization Identifier (OrgId) – OID: 2.5.4.97 – Identifier of the organization
  In case of an organizational certificate the identifier of the *Organization* indicated in the "O" field is in this field.

  Only that data can be in it, which was verified by the *Provider*.

  In case of an organizational certificate filling out the field is optional.

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

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

  In case of an organizational certificate the name of the certification unit related to the organization named in the "O" field, or the trademark, or other information is in this field.

  Only that data is indicated here that the *Provider* verified and that the *Organization* has the right to use.

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

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

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

  In case of an *Organizational Certificate* the two-letter country code of the place of incorporation of the *Organization* indicated in the "O" field.

  In case of a natural person *Subject* not related to an *Organization* the two-letter code of the country of the *Subject*'s permanent address.

  Always filled out.

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

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

  Not filled.

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

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

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

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

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

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

- Postal Code – OID: 2.5.4.17 – Zip code

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

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

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

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

  In case of organizational certificates it determines the *Subject*'s title associated with that organization in what he creates the signature.

  The field contains values only in case of a *Organizational Certificate*, so only when the "O" field is filled.

  The *Provider* verifies – based on the official document presented by the Represented Organization – the authenticity and genuineness of the value to be indicated on this field.

  Since the "Title" field contains the title of the *Subject*, it can contain further restrictions on the *Certificate* usage.

- 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 is 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 *Certification Practice Statement* might contain further – in accordance with the referenced *Certificate Policies* – "Subject DN" fields. Only verified text values may be indicated on these fields (they shall not contain values indicating lack of data for example: ".", "-" or " ").

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 natural person *Subject*s, for the *Subject*'s request, his name written in different notation than in the field "Subject DN / Common Name" can be indicated here (typically in the "CN" field of the "Subject Alternative Names"). That name can be written with or without accent marks. The *Provider* is entitled to denote the nature of the name indicated.

  The *Provider* verifies the names to be indicated on "Subject Alternative Names" field. It takes a decision based on whether the name requested by the *Client* is indeed the name of the *Subject*, and that it does not mislead others. If the *Subject* in the exercise of its profession does not use its name indicated on its document used for identification, then it can request the *Provider* to use that alternative name 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 is definitely filled out. The same e-mail address might be displayed in the "EMAIL" field of the *Certificate*.

- Furthermore the RFC 4043 [25] "Permanent Identifier" can be included in the subject alternative names field. This is a different name forms that only contains the "assigner" field, in this the unique OID of the *Provider* is indicated. Then according to the RFC 4043 recommendation, this "assigner" OID together with the first "Serial Number" value – containing the OID allocated by the *Provider*– of the "Subject" field makes up the *Subject* permanent identifier.

The Denomination of the Certificate Issuer Certification Unit

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

- Common Name (CN) – OID: 2.5.4.3
  The name of the *Certificate* issuer certification unit in English (see section: 1.3.1.).

- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  (The name of the *Provider* in English without accents.)

- Organization Identifier (OrgId) – OID: 2.5.4.97
  "VATHU-23584497-2-41"
  Filling out is optional.

- Organizational Unit (OU) – OID: 2.5.4.11
  "e-Szigno CA"
  (The name of the *Provider* organization unit's name without accents; not filled in SHA-256 based provider *Certificate*s.)

- Locality (L) – OID: 2.5.4.7
  "Budapest"
  (Domicile city of the *Provider* without accents.))

- Country (C) – OID: 2.5.4.6
  "HU"
  (Two letter abbreviation of the domicile country of the *Provider*))

- E-mail address (EMAIL) – OID: 1.2.840.113549.1.9.1
  "info@e-szigno.hu"
  Filling out is optional.

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

The Alternate Names of the Certificate Issuer Certification Unit

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

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

3.1.2 Need for Names to be Meaningful

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

- the identifier shall be meaningful;
- the personal name in the *Certificate* shall be indicated the same way as the notation in public registers ;
- 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.

In case of a Pseudonymous *Certificate*, only the "Pseudonym" field can contain pseudonym, the other fields are verified the same way by the *Provider*as applied in the non-pseudonymous *Certificate*s.

3.1.3 Anonymity or Pseudonymity of Subscribers

See Section 3.1.1.

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 *Provider*. In such case, the *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.

The *Provider* ensures the possibility to electronically verify the data for the identification of the person if the *Provider* issued the *Certificate* based on a *Certificate Policy* which requires that. The details thereof are written in section 4.13.

3.1.5 Uniqueness of Names

The *Subject* has a unique name in the *Certificate Repository* of the *Provider*. In order to ensure the uniqueness, the *Provider* gives each *Subject* an identifier (OID), – unique in the *Provider*'s register – , which is indicated on the *Subject*'s unique identifier "Subject DN Serial Number" field.

The *Subject*s' unique identifiers (OID) are distributed in accordance with the order of the received certification applications examination, ensuring the uniqueness of the "Subject" field in the *Certificate*.

The *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 *Provider* makes sure of the *Client*'s credentials to use the indicated names. The *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 *Provider* makes sure of their legitimate use, and in case of a complaint it is entitled to revoke the *Certificate*.

If the *Client* requests a *Certificate*, and asks for brand name or trademark indication, then the *Client* shall provide evidence of the legitimacy of its use, which the *Provider* verifies before *Certificate* issuance.

The *Provider* uses the e-Szignó trademark during its service provision. The trademark is the property of E-Szignó LP., for the usage of the trademark, the consent is given by the holder.

3.2 Initial Identity Validation

The *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 *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 *Provider* ensures and makes sure that the *Certificate* requester owns and has it under his control the private key belonging to the public key of the *Certificate* .

If the *Provider* generates within its organization the private key belonging to the qualified *Certificate* of the *Subject* – typically on *Qualified Electronic Signature Creation Device* or on other, *Hardware Security Module* in case of *Certificate Policies* requiring such – , then it does not have to specially verify that the *Subject* owns the private pair of the public key to be verified.

If the *Subject* requests the *Certificate* issuance for a key provided by it – typically in case of software certificates –, then the *Provider* accepts the *Certificate Application* in PKCS#10 format, which at the same time confirms, that the owner of the private key asked for the *Certificate* indeed.

The *Provider* considers equivalent evidence that the *Subject* submits the *Certificate Application* with the public key to be included in the requested *Certificate* signed with the use of a valid qualified *Certificate* based qualified electronic signature.

If the *Subject* private key is generated and managed by another *Trust Service Provider*, then the *Trust Service Provider* verifies that, the referred *Trust Service Provider* owns the private key, and is under the sole control of the *Subject*. The *Provider* may accept the authentic statement of the referred *Trust Service Provider* about this. The format of the statement may be electronic. The *Provider* verifies the authenticity of the statement. The verification of the ownership might happen with the acceptance of a PKCS#10 formatted *Certificate Application* too.

3.2.2 Authentication of an Organization Identity

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

- if the *Subject* of the *Certificate* to be issued is the *Organization*;
- if the *Subject* of the *Certificate* to be issued is the device or system operated by the *Organization*;
- if the *Certificate* is issued to a natural person, but the name of the *Organization* is indicated on the *Certificate* as well.

Furthermore it is verified in these cases, that:

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

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

- the official denomination and registered office of the *Organization*,
- official registration number of the *Organization* (e.g. company registration number, tax identification number), if applicable;

- the name of the organization unit within the *Organization*, if its indication in the *Certificate* is requested,
- in case of an *Organizational Certificate* issuance to a natural person, the role of the *Subject* within the *Organization*, if its indication in the *Certificate* is requested.

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

- the statement with the application submitter's manual signature on that the data given for the *Organization* identification is correct and comply with reality;
- a declaration of the the applicant with his signature that there is no trademark amongst the data to be indicated in the *Organization Certificate*, or if included, proof that the *Organization* is entitled to use the trademark;
- a certificate regarding that on behalf of the organization the *Certificate* application submitter natural person is entitled to submit the application [2];
- in case of an *Organizational Certificate* issuance to a natural person, the certificate regarding that the organization consents to that the name of the organization is indicated on the certificate issued to the natural person [3];
- the specimen signature of the person entitled to represent the *Organization* or other, official document equal to the specimen signature, which contains the name and signature of the persons entitled to represent the *Organization* [4];
- the *Organization* existence, name and the legal status verification document [5].

The *Provider* is bound to verify the validity and authenticity of the presented documents in authentic databases.

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

In respect of data verification, the *Provider* accepts:

- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information is correct;
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the given information is correct.

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

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

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

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

The *Provider* guarantees by the proper usage of the trusted roles and the internal administrative processes that during the registration and verification process of the personal data at least two employees needed by the proper trusted roles.

3.2.3 Authentication of an Individual Identity

The natural person's identity shall be verified:

- if the *Subject* of the *Certificate* to be issued is a natural person;
- if a natural person is acting on behalf of an *Organization* for *Organizational Certificate* application.

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 *Provider* uses the identification methods described in items a), b) - if the technical requirements are appropriate - and c) of 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;
    - the identity of the natural person is verified during personal identification based on a suitable official proof of identity card;
    - 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 validity of the identification data used for personal identification is checked by the *Registration Authority* with the help of a trusted third party or a public register;
    - the *Provider* verifies, whether any alteration or counterfeiting happened to the presented cards.

The *Provider* verifies the identity of foreign citizens with the help of their passport or other, personal identification documents, in this case it performs data reconciliation with the proper records of the country, if such records are available. Additional steps are necessary for verifying the foreign document with appropriate confidence, as well as to access the foreign register. In respect of data verification, the *Provider* accepts:

- certificate issued by the embassy or consulate of the foreign country in Hungary, that the organization exists and the given information are correct;
- certificate issued by a Hungarian embassy or consulate in a foreign country, that the organization exists and the provided information is correct.

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

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

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

2. 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.
   - The identification data used for personal identification is checked by the *Registration Authority* with the help of a trusted third party or a public register.

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

   - The *Subject* submits the *Certificate Application* in electronic format with an electronic signature based on a non-pseudonymous *Certificate* with a safety 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 *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.
- The identification data used for personal identification is checked by the *Registration Authority* with the help of a trusted third party or a public register.

The *Provider* uses the data reconciled during a previous identification procedure, if the *Subject* requests new *Certificate* instead of an expired or a revoked one, or if he requests a new *Certificate* besides the existing one during the validity period of the service agreement. The authenticity of the *Certificate* application, the accuracy of the data to be in the *Certificate* and the identity of the person submitting the application shall also be checked.

The *Provider* guarantees by the proper usage of the trusted roles and the internal administrative processes that during the registration and verification process of the personal data at least two employees needed by the proper trusted roles.

3.2.4 Non-Verified Subscriber Information

Only that data can be in the *Certificate* issued by the *Provider*, which was verified by the *Provider* or on the authenticity of which the *Subject* made a statement with recognition of their criminal liability. The only exception is the pseudonym indicated in the *Certificate*s issued according to a pseudonymous *Certificate Policy* [MATxA] appearing in the "Pseudonym" field.

3.2.5 Validation of Authority

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

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

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

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

An organization administrator is a person who is eligible to act during the application, suspension, reinstatement and revocation of the *Certificate*s issued to the *Organization* and to grant the issuance of organization related personal certificates and the revocation of such *Certificate*s .

The organization administrator can be appointed during *Certificate* application, or anytime later with the help of the corresponding form. The identifier information of the designated person(s) shall be given on the form, by which he/she can be identified in later litigation. The form shall be (manually or qualified electronically) signed by the representative of the *Organization*, which is verified by the registration associate of the *Provider* when received. Appointing an organization administrator is not mandatory, and multiple organization administrators can be appointed too. If there is no appointed organization administrator, then the person entitled to represent the *Organization* can perform this task.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-key Requests

Re-key is the process when the *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 *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 *Provider* ensures the following options:

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

In case of a personal application the applicant 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 there is no need for further verification of the applicant's identity, or the authenticity of the application.

The renewal request is sibmitted 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.

.

In case re-key is necessary because the private key belonging to the *Certificate* became compromised, the *Provider* ensures options for the *Subject* to indicate this fact during the suspension or revocation process. In this case the *Subject* is identified within the confines of the suspension or revocation process, and the details are in section 3.6.

3.3.2 Identification and Authentication for Re-key After Revocation

The *Provider* accepts re-key requests – only during the validity period of the service agreement– in case of *Certificate*s revoked or suspended. The identity of the person submitting the application is verified the same way, as in case of re-key requests for valid *Certificate*s according to the process defined in section 3.2.3, except not all listed options are accessible by the *Client*.

3.4 Identification and Authentication in Case of Certificate Renewal Requests

Certificate renewal is the process when the *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 *Provider*:

- on paper signed manually by the *Subject* at the customer service of the *Provider*, to the mobile registration associate of the *Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed,
- in an electronically submitted request with a electronic signature based on the *Certificate* to be renewed;
- in electronic form with an electronic signature of the *Subject* based on the non-pseudonymous *Certificate* with a safety 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 *Subject*'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 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 *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 is verified by the *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 *Provider*:

- on paper signed manually by the *Subject* at the customer service of the *Provider*, to the mobile registration associate of the *Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed,
- in an electronically submitted request with a electronic signature based on the *Certificate* to be renewed;
- in electronic form with an electronic signature of the *Subject* based on the non-pseudonymous *Certificate* with a safety 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 *Subject*'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, 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 *Subject* 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 *Provider* receives and processes 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 *Provider* ensures that the requests only get accepted from authorized parties besides the rapid processing of the suspension and revocation requests.

The identity of the submitter persons and the authenticity of the applications are verified.

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

4 Certificate Life-Cycle Operational Requirements

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

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

- *Certificate renewal* means requesting a *Certificate* with the same data indicated in it as in the previous one by the *Subject* and both *Certificate*s are issued for the same public key. The details of *Certificate renewal* are discussed in section 4.6.
- *Certificate modification* means requesting the modification of the *Subject*'s *Certificate* considering data change. The *Provider* receives *Certificate modification* requests during

the validity period of the *Certificate*. Over the course of Certificate modification, the new *Certificate* is issued to the same public key. The details of *Certificate modification* are described in section 4.8.

- *Re-key* means a new *Certificate* issuance by the *Provider* for a new public key at the request of the *Subject* during the *Certificate*'s validity period or after expiration. The details of *Certificate renewal* are discussed in section 4.7.

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

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

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

4.1 Application for a Certificate

For each new *Certificate* issuance, *Certificate Application* submission is required. Prior to submitting the first *Certificate Application*, the *Subject* shall submit a *Registration Application* to the *Provider*, this can be done through the website of the *Provider*, for instance. The *Subject* shall specify their data to be indicated in the *Certificate* and shall specify what kind of *Certificate* they request, and they shall authorize the *Provider* for the management of their personal data in the Registration request.

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

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

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

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

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

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

The *Provider* publishes the documents containing this information in a comprehensible manner, made available in an electronically downloadable format as well as upon request in printed form. At the Customer service office, the *Client* has the opportunity for survey and consultation.

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

- data to be indicated in the *Certificate* (for example name, title, name of *Organization*, name of organizational unit, city, country, e-mail address);
- the personal identification information of the *Subject* – in case of an *Organization* the *Organization* representative – (full name, number of the identity document, mother's name, date and time of birth);
- the contact of the *Subject* – in case of an *Organization* the *Organization* representative – (telephone number, e-mail address);
- in case of *Organization Certificate* application, the data of the *Organization* (official name, domicile, optionally: identification data, denomination ot the organization department);
- the *Subscriber*'s data (billing information);

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

- documents necessary to identify the *Subject* – in case of an *Organization*, the *Organization* representative –

  according to Section 3.2.3;
- in case of *Organizational Certificate* application, the documents for the identification of the *Organization* according to Section 3.2.2;
- if the *Subject* is an *Organization*, then the certification or procuration delivered by the *Organization*, that the *Subject* is entitled to represent the *Organization* according to section 3.2.5;
- if the *Subject* is a natural person requesting the indication of belonging to an *Organization*, then the evidence of the consent of the *Organization*, to that according to section 3.2.2.;
- if the *Certificate* requested contains a trademark or a brand name, then a certification about the usage rights of the *Subject* according to section 3.1.6.

4.1.1 Who May Submit a Certificate Application

Certificate Application may only be submitted by natural persons, to request a *Certificate* for themselves or for the organization represented. The precondition of *Certificate* issuance is a valid service agreement (signed by the *Subscriber* and the *Provider*) concerning *Certificate* issuance and maintenance.

The *Subject* – in case of an *Organization* the *Organization* representative – may submit the *Certificate Application* in the following ways:

- on paper signed manually during the personal identification performed at the customer service of the *Provider*, by the mobile registration associate of the *Provider* or by some other *Registration Authority*'s registration associate,
- on paper sent by post to the postal address of the *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 *Provider*'s e-mail address (see section 1.2.3.);

The *Subscriber* and the *Subject* – in case of an *Organization* the *Organization* representative – shall provide their contact information during the *Registration Application*.

4.1.2 Enrolment Process and Responsibilities

During the process of the application the *Provider* (or the *Registration Authority*) ascertains the identity of the person submitting the *Certificate Application* (see section 3.2.3.).

If the *Subject* is an *Organization* and the name of an *Organization* is indicated in the *Certificate* too (Organizational Certificate), then the *Provider* (or the *Registration Authority*) identifies the *Organization* (see section: 3.2.2.) and it ensures, that the *Subject* is entitled to represent the *Organization* (see section: 3.2.5.) and to request a *Certificate* related to the *Organization* (see section: 3.2.2.).

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

The *Subject* – in case of an Organization, its representative – shall provide all the necessary information for the conduct of the identification processes.

The *Provider* performs data reconciliation with public registers (such as the personal data and address register or the company register). In case of a database if it can be arranged, the *Provider* performs the data reconciliation electronically.

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

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

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

The *Provider* registers the *Certificate Application* signed by the *Subject* – in case of an Organization, its representative – which shall contain the following:

- a confirmation, that the data provided in the *Certificate Application* are accurate;
- a consent, that the *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 *Provider* keeps the aforementioned records for the time period required by law.

The *Provider* archives the contracts, the Certificate application form and every attestation that the *Represented Organization*, the *Subject* or the *Subscriber* handed in.

If the identity of the *Subject* – in case of an *Organization*, its representative – or in case of an *Organizational Certificate* the identity of the *Organization* or in case of an *Organizational Certificate* issued to a natural person , the *Subject*'s inherency to the *Represented Organization* can not be verified without a doubt or any of the indicated data on the *Certificate* application form is incorrect, then the *Provider* can, according to its inner regulations give the *Client* the opportunity to correct the missing or incorrect data, and to the hand over the missing attestations within 3 months from the submission of the *Certificate Application*.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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

4.2.2 Approval or Rejection of Certificate Applications

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

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

If the *Subject* requests a *Certificate* containing an e-mail address, the *Provider* verifies the e-mail address to be indicated in the *Certificate*. It ascertains that the e-mail address exists and verifies that it is the *Subject*'s e-mail address indeed.

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

If the identity of the natural person or the organization which is to be identified, or in case of a personal *Certificate*, the *Subject*'s inherency to the *Represented Organization* can not be verified without a doubt or any of the indicated data on the *Certificate Application* form is incorrect, and the *Client* did not correct it for the request of the *Provider*, then the *Provider* rejects the application.

In case of *Certificate Application* refusal the *Provider* informs the *Subject* and the *Subscriber*, but the *Provider* does not have to justify its decision.

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

The *Provider* only issues the *Certificate* to the *Subject* in case of the acceptance of the *Certificate Application*.

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

If the Certification Authority provides the *Electronic Signature Creation Device* to the *Subject* (within the framework of device provision service), as a part of the process, the issued *Certificate* is installed to the *Electronic Signature Creation Device* too. The handover of the *Electronic Signature Creation Device* containing the private key takes place in a controlled environment in accordance with the safety regulations defined in section 6.1.2.

If the takeover of the *Electronic Signature Creation Device* containing the *Subject*'s *Certificate* and private key to the *Subject* do not take place right after the personal identification related to the Certificate application, then the *Subject* (in case of a non-natural person, its representative)

can take over their device after personal identification, in the course of they have to identify themselves with an identification document. The transferring party verifies, that the portrait of the *Subject* matches the one on his/her ID card, and the Signature of the *Subject* fits the one appears on the ID card.

Along with the takeover of the *Electronic Signature Creation Device*, the *Subject* receives the activation codes necessary for activation, generated according to section 6.4. These codes are handed in a closed envelope, and it is mandatory for the *Subject* to open and verify whether the codes are readable.

4.3.1 CA Actions During Certificate Issuance

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

The *Provider* guarantees by the proper usage of the trusted roles and the internal administrative processes that during the *Certificate* issuance process at least two employees needed by the proper trusted roles.

4.3.2 Notification of the Subscriber about the Issuance of the Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The *Subject* – in case of a certificate issued to an Organization, the representative of the *Subject* – shall verify the accuracy of the data indicated in the *Certificate* during the takeover of the *Certificate* and shall make a written statement on that. In the statement the *Subject* or its representative verifies the reception of the *Certificate*.

If the Certification Authority provides *Qualified Electronic Signature Creation Device* to the *Subject*, after the reception of the *Qualified Electronic Signature Creation Device* containing the private key, the *Certificate* of the *Subject* and the code necessary for activation the *Subject* can test his/her device. Afterwards the *Subject* 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 Signature Creation Device* usage.

4.4.2 Publication of the Certificate by the CA

After the *Certificate* receipt – if the *Subject* consents – the *Provider* discloses the *Certificate* in its *Certificate* store.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

If the *Certificate* was issued for the *Subject* to create electronic signature behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

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 signature creation, and any other usage (for example, authorization and encryption) is prohibited.

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

The *Subject* is bound to ensure the adequate protection of the private key and the activation data (password or PIN code).

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 *Provider*, in the course of accepting the electronic signature verified, the *Relying Party* is recommended to proceed prudentially particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- *Certificate*s for electronic signatures and the corresponding public keys shall only be used for electronic signature validation;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain;
- the electronic signature verification shall be performed with a reliable application, which complies with the related technical specifications, can be resiliently configured, and has been set correctly, and it runs within a virus-free environment;

- in case of personal *Certificate*s related to an organization, it is recommended to verify that the title of the Signatory by which it is entitled to sign the document can be identified by the certificate (for example indicated in the Title field);
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- when accepting a qualified electronic signature it is recommended to verify that the *Certificate* was issued based on a *Certificate Policy* requiring *Qualified Electronic Signature Creation Device*;
- it is recommended to verify the highest value of the obligation undertaken at one time indicated in the *Certificate* (the Certification Authority is not responsible for the claims arising from electronic documents issued and signed concerning transactions in excess of those limits and for the damage caused this way.);
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

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

4.6 Certificate Renewal

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

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

4.6.1 Circumstances for Certificate Renewal

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

- the *Certificate* renewal request was submitted within the validity period of the *Certificate*;
- the *Certificate* to be renewed is not 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 *Provider* shall only accept a *Certificate* renewal application within the effect of the service agreement.

If a previous *Certificate* of the *Subject* is revoked or expired, then new *Certificate* can only be requested in the frame of *Re-key* (see section: 4.7.) or new *Certificate* application (see section: 4.6.).

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

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

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

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

4.6.2 Who May Request Renewal

The Certificate renewal shall be initiated by a person 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 *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.

The *Provider* provides the following possibilities for *Certificate* renewal application submissions:

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

4.6.3 Processing Certificate Renewal Requests

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

- the submitted *Certificate* renewal application is authentic;

- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the submitter of the *Certificate* renewal application stated that the data of the *Subject* to be indicated in the *Certificate* are unchanged and accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;
- the *Certificate* to be renewed is not 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 *Provider* informs the *Subject* and the *Subscriber* about the *Certificate* issuance.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

During the *Certificate* renewal process, there is no key generation, thus there is no need to handover key to the *Subject*. The renewed *Certificate* can be received (downloaded) without personal encounter.

If the private key of the *Subject* is on a *Electronic Signature Creation Device*, then the *Subject* installs the *Certificate* to the device. For that purpose, the *Provider* provides written manuals, and if necessary, provides consultation possibility by telephone.

The subject accepts the *Certificate* by its usage without additional declaration.

4.6.6 Publication of the Renewed Certificate by the CA

The *Provider* discloses the renewed *Certificate* the same method as the original *Certificate*.

4.6.7 Notification of Other Entities about the Certificate Issuance

If the *Certificate* was issued for the *Subject* to create electronic signature behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

4.7 Certificate Re-Key

Re-key means the process when the *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 *Provider* shall only accept *Re-key* applications within the scope of the service agreement.

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

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

4.7.2 Who May Request Certification of a New Public Key

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

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

The *Provider* ensures the following possibilities to submit *Certificate* renewal application:

- on paper signed manually at the customer service of the *Provider*, to the mobile registration associate of the *Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed,
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a safety classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- during the revocation or suspension process of the *Certificate*;
- signed manually, sent by post to the Customer service.

4.7.3 Processing Certificate Re-Key Requests

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

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

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

4.7.4 Notification of the Client about the New Certificate Issuance

The *Provider* informs the *Subject* and the *Subscriber* about the *Certificate* issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

If the new key used is generated on an *Electronic Signature Creation Device* during the *Re-key*, then the issued *Certificate* will be installed to the *Electronic Signature Creation Device* too as part of the *Re-key* process. The handover of the *Electronic Signature Creation Device* containing the private key to the *Subject* takes place in in a controlled environment while in accordance with the safety regulations defined in section 6.1.2. The *Subject* (in case of not natural person *Subject*, its representative) can take over it device following a personal identification, in the course of it shall identify itself with an identification document personal. The transferring party verifies, that the portrait of the *Subject* matches the one on his/her ID card, and the Signature of the *Subject* fits the one appears on the ID card.

Along with the takeover of the *Electronic Signature Creation Device*, the *Subject* receives the activation codes necessary for activation, generated according to section 6.4. These codes are handed in a closed envelope, and it is mandatory for the *Subject* to open and verify whether the codes are readable. After testing the *Electronic Signature Creation Device*, the *Subject* shall sign a statement manually about takeover, in which – amongst others – it verifies that the data indicated in the *Certificate* are valid, it received the *Electronic Signature Creation Device* and the related activation codes, and that it is aware of the technical and legal requirements of the device usage.

If the new key used during the *Re-key* was provided by the *Subject*, then there is no need for key and *Electronic Signature Creation Device* handover. The renewed *Certificate* can be received (downloaded) without personal encounter. By using the *Certificate*, the *Subject* accepts the it without additional declaration and. The *Provider* hands over the *Certificate* issued for the new public key after the identification of the *Subject*.

4.7.6 Publication of the Re-Keyed Certificate

The *Provider* discloses the renewed *Certificate* the same way as the original *Certificate*.

4.7.7 Notification of Other Entities about the Certificate Issuance

If the *Certificate* was issued for the *Subject* to create electronic signature behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

4.8 Certificate Modification

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

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

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

4.8.1 Circumstances for Certificate Modification

Certificate modification becomes necessary in the following cases:

- change of data indicated in the *Subject*'s *Certificate*;
- in the *Certificate* issuing system of the *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 *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 *Provider* only accepts *Certificate* modification application in the scope of the Service Agreement.

If the previous *Certificate* of the *Subject* is revoked or expired, then the new *Certificate* can be requested within the framework of *Re-key* (see section: 4.7.) or new *Certificate* application (see section: 4.6.).

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

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

4.8.2 Who May Request Certificate Modification

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

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

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

The *Provider* ensures the following possibilities to submit *Certificate* renewal application:

- on paper signed manually at the customer service of the *Provider*, to the mobile registration associate of the *Provider* or to some other *Registration Authority*'s registration associate, on a date previously agreed;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a safety classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- during the revocation or suspension process of the *Certificate*;
- signed manually, sent by post to the Customer service.

4.8.3 Processing Certificate Modification Requests

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

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

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

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

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

4.8.4 Notification of the Client about the New Certificate Issuance

The *Provider* informs the *Subject* and the *Subscriber* about the *Certificate* issuance.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

If the private key of the *Subject* is on a *Electronic Signature Creation Device* then the *Certificate* can be installed to the device by the *Subject* too. For that, the *Provider* provides written guidelines, and if necessary, it provides consultation possibilities by telephone. The *Subject* accepts the *Certificate* by its usage, and there is no need for further statement.

4.8.6 Publication of the Modified Certificate by the CA

The *Provider* discloses the modified *Certificate* the same way as the original *Certificate*.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

If the *Certificate* was issued for the *Subject* to create electronic signature behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

4.9 Certificate Revocation and Suspension

The process when the *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 *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.

The usage of the private key belonging to the revoked or suspended *Certificate* shall be eliminated or suspended immediately.

If possible, the private key belonging to the revoked *Certificate* shall be destroyed immediately after revocation.

Responsibility regulations related to revocation and suspension:

- Before the revocation/suspension request is received by the *Provider*, the *Subject* and the *Subscriber* are responsible for the damages arising.
- After the *Provider* accepts the revocation or suspension request, the *Provider* is responsible for the damages arising. The *Provider* forthwith publishes the changed revocation state of the *Certificate* after accepting the request.
- If the *Provider* has already published the invalid revocation state of the *Certificate*, the *Provider* does not take any responsibility, if the *Relying Party* considers the *Certificate* valid.

4.9.1 Circumstances for Revocation

Certification Authority takes action on the revocation of the end-user *Certificate* in the following cases:

- *Certificate* modification because of data change referring to the *Subject*;
- the *Provider* becomes aware that the data in the *Certificate* do not correspond to reality;
- the *Subject* or the *Subscriber* notifies the *Provider* that the *Certificate Application* is not approved and subsequently the approval is not given;
- if the *Provider* issued the *Certificate* based on a document from a third party, and it withdraws that document in writing;
- the *Subject* or the *Subscriber* requests the revocation of the *Certificate* in writing;
- the *Provider* becomes aware that the private key is not in the exclusive possession of the *Subject* , or in case of the Remote Signature Service, does not have sole control over the private key;

- the *Provider* becomes aware that the certificate was used illegally;
- the *Provider* becomes aware that the *Subscriber* failed to fulfil any of its financial obligations according to the service agreement;
- the *Certificate* was suspended, and was not reinstated during the ensured time period (see section: 4.9.16.);
- the termination of service agreement;
- the *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 *Provider* becomes aware that the *Certificate* was not issued according to the related *Qualified Signature Certificate Policy* and the *Certification Practice Statement*;
- the *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 *Provider* is no longer entitled to issue *Certificate*s, and maintenance is not provided for the existing CRL and OCSP services;
- the *Provider* has terminated its activities;
- the law makes revocation mandatory;

The *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 *Provider*;
- the *Provider* becomes aware that it is not in the exclusive possession of the private key;
- the *Provider* becomes aware that the *Certificate* is used illegally;
- the *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 Signature Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit does not comply with the relevant *Qualified Signature Certificate Policy* or *Certification Practice Statement*;
- the *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 *Provider* has ended its activities;
- the law makes the revocation mandatory.

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;
- if *Certification Authority* issued the *Certificate* based on a document from a third party, and that third party withraws the document in writing;
- 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 Signature Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit operator does not comply with the relevant *Qualified Signature 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.

4.9.2 Who Can Request Revocation

The revocation of the *Certificate* may be initiated by:

- the *Subscriber*;
- the *Subject*;
- in case of *Organizational Certificate*, the *Organization*'s authorized representative;
- the contact person specified in the service agreement;
- the *Provider*.

4.9.3 Procedure for Revocation Request

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

- on paper signed manually at the customer service of the *Provider* during office hours in person;
- in an electronic form with an electronic signature based on a non-pseudonymous *Certificate* 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 *Provider* verifies the authenticity of the request, and the submitter's eligibility during the evaluation of the request.

In case of submitting a personal request, the identification of the requester takes place according to section 3.2.3. In case of Certificate application signed with a valid qualified electronic signature,

there is no need for further verification of the identity of the applicant and the authenticity of the application.

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

The reason for revocation shall be stated. If the revocation was requested by the *Client*, and it does not state the reason for revocation, then the *Provider* considers that the reason for revocation is that the *Subject* does not want to use the *Certificate* anymore.

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

In case of a successful revocation the *Provider* notifies the *Subject* and the *Subscriber* about the fact by e-mail.

4.9.4 Revocation Request Grace Period

The *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 *Provider* shall process the revocation requests no later than the end of the working day following the arrival of the request.

In case of applications submitted in person, the time of arrival is when the *Client* provides all the necessary data for revocation. In case of applications sent by post or electronic mail, the time of arrival is when the mail arrives to the Customer Service office of the *Provider* at office hours, or when it arrives to the mailbox on the server of the *Provider*. Letters arriving out of office hours are considered as arrived at the beginning of the next office hours. The *Provider* only undertakes the requirements for requests sent for addresses stated in section 1.2., in case of statements sent to other addresses – specially directly sent to specific associate of the *Provider* – or via other channels, the *Provider* does not offer any availability.

If the *Client* wants to revoke its *Certificate* and the revocation is urgent, or the *Client* cannot appear in person at the office of the *Provider*, the *Provider* recommends to the *Client* to suspend the *Certificate* until the revocation, with the help of the available 24-hour telephone hotline (see section 4.9.13.). It is sufficient to take care of the revocation of the suspended certificates later, and the *Provider* automatically revokes the suspended *Certificate*s after the time for restoration elapses (see section: 4.9.16.).

4.9.6 Revocation Checking Requirement for Relying Parties

To maintain the level of security guaranteed by the *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 (If Applicable)

The *Provider* issues a new *Certificate* revocation list at least once a day, but in case of revocation immediately or suspension after the acceptance of the notification for its end user *Certificate*s.

The validity of these certificate revocation lists is to a maximum of 25 hours.

The *Provider* issues a new *Certificate* revocation list at least once a year or in case of a revocation within 24 hours for its intermediate certification units. The validity of these issued *Certificate* revocation lists is to a maximum of 12 months.

4.9.8 Maximum Latency for CRLs (If Applicable)

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

4.9.9 Online Revocation/Status Checking Availability

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

4.9.10 Online Revocation Checking Requirements

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

Certification Authority provides OCSP service through GET method.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements for Key Compromise

In case of any certification unit's private key is compromised, the *Provider* makes every reasonable effort in order to notify the *Relying Parties* about the incident. It publishes any status change on the provider *Certificate*s on its webpage. In case of compromised *Certificate*s issued by the *Provider*, the *Provider* is able to revoke the end-user *Certificate* belonging to the compromised private key. The revocation reason information (reasonCode) in this case is set to keyCompromise (1) value.

4.9.13 Circumstances for Suspension

The *Provider* ensures a possibility for *Client*s for the temporary suspension of the *Certificate* in case, that it can be assumed that any of the reasons establishing revocation exists.
The *Provider* is entitled for *Certificate* suspension for the following reasons:

- The *Subscriber* does not pay until the payment deadline.
- If the *Provider* presumes that the data indicated on the *Certificate* do not comply with reality. If the *Provider* becomes aware of those conditions, it initiates the suspension or revocation of the *Certificate*.
- If the *Provider* presumes that the private key belonging to the *Certificate* is not in the possession of the *Subject*, and it is confirmed by substantial evidence. If the *Provider* becomes aware of that the *Electronic Signature Creation Device* is possessed by an unauthorized person, the *Provider* suspends every *Certificate* it contains.

The *Provider* does not accept suspension requests related to *Certificate*s not valid, in addition to justify the reason for rejection.

4.9.14 Who Can Request Suspension

The suspension of a *Certificate* can be requested by the same persons, who are eligible to initiate the revocation of the *Certificate* (see section: 4.9.2.)

4.9.15 Procedure for Suspension Request

The *Provider* ensures opportunity for suspension initiation:

- via telephone hotline;
- via its webpage;
- the same way as submitting the revocation requests.

Suspension via Hotline

Suspension by telephone is available 7 days a week, 24 hours a day. The *Client*s of the *Provider* may use this transaction to indicate to the *Provider* if their *Electronic Signature Creation Device* or private key is possessed by unauthorized persons. The availability of the telephone suspension service is 99 , 9 %, while service outage may not exceed 3 hours in each case.

Requests arriving by telephone are processed by the *Provider* with out of turn and performed immediately.

Telephone requests are answered by the telephone hotline associate of the *Provider*. The *Provider* has the right to create a voice recording of conversations related to suspension and reinstation.

The following information is requested on every account by the *Provider*'s associates from the applicant :

- name of the applicant ,
- name of the *Subject* whose *Certificate* is to be suspended,
- date of birth of the *Subject* or the last three digits of the OID as indicated within the *Certificate* (e.g. 2.2.123),
- the data required for the validation of the suspension request:
  - the suspension password, or
  - instead of the a suspension password the *Subject* personal data,
    - name at birth and
    - date of birth and
    - place of birth and
    - mother's name.

Should the applicant fail to provide any of the data indicated in the list above, or to provide the appropriate password, the *Provider* rejects the suspension request.

As soon as the staff of the *Provider* has successfully determined the suspension authorization of the applicant during the telephone conversation, it indicates that the *Provider* has accepted the application and started its processing. Starting from this moment, the *Provider* assumes responsibility for the damages arising out of accepting the certificate until the new revocation state of the *Certificate* appears in the revocation records of the *Provider*.

If the applicant gives the password belonging to any of the *Client*'s *Qualified Electronic Signature Creation Device*, then the *Provider* suspenses every *Certificate* issued for that *Qualified Electronic Signature Creation Device*. If the applicant gives the password for any of the *Client*'s software

*Certificate*s, then the *Provider* revokes all of the software *Certificate*s. If the applicant gave the *Subject* personal data, then the *Provider* suspenses all of the *Subject*'s *Certificate*s.

The *Provider* processes the suspension application within the duration of phone call – typically within seconds – and the possibly changed revocation status appears within the *Provider*'s revocation status register after processing immediately. The inner processes of the *Provider* ensure that the process ends at most in 5 minutes, so the changed revocation status is published within the same time from receiving the revocation request.

As at suspension the verification of eligibility (namely the identification of the applicant) is performed with a password or personal data, the *Provider* accepts the suspension request from every person who can provide the necessary password or personal information.

In case of a successful suspension, the *Provider* notifies the *Subject* and the *Subscriber* about the fact by e-mail.

Suspension via Web

Suspension is also available via the website of the *Provider* at the following address:

`https://www.e-szigno.hu/felfuggesztes`

When suspending via the website of the *Provider* the *Client* needs to provide the same information as those provided when suspending via the hotline. Suspension requests submitted via the website of the *Provider* are processed without delay by the information system of the *Provider* and it immediately notifies the applicant about the result on its website.

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

The *Provider* logs every suspension request. In case of a successful suspension, the *Provider* notifies the *Subject* and the Subscriber about the fact of the suspension by e-mail.

The *Provider* undertakes maintenance for suspension requests by telephone only. If the webpage of the *Provider* is not available, the *Provider* recommends the *Client* to request suspension via telephone.

Suspension the Same Way as Revocation Request Submission

The *Provider* enables the submission of the suspension requests the same way, as the revocation requests, according to the requirements of section 4.9.3. From the suspension application, the *Provider* shall be able to determine that exactly which *Certificate* the applicant asks to the suspend and upon what grounds. The registration staff member sends a notification via e-mail to the *Subject* and the Subscriber.

At suspension, the reason of suspension shall be given. If the *Client* requests the suspension, and does not give the reason, the *Provider* assumes that the reason is private key compromise.

If the *Client* asks for the suspension because of key compromise, then the *Provider* provides an opportunity for the *Client* during the suspension process to indicate that if the *Certificate* is not reinstated within a time frame (and so it becomes revoked), then a new certificate will be requested within the framework of *Re-key*. The rules of *Re-key* are in section 4.7.

4.9.16 Limits on Suspension Period

In case of a suspension requested by the *Subject*, a *Certificate* can only be suspended for 5 working days. If the *Certificate* is not reinstated after that time, the *Provider* revokes the *Certificate* without further notification.

The *Certificate* reinstatement means the process, in the course of which the suspended *Certificate* becomes valid again.

The *Certificate* reinstatement can be requested by the person who requested the certificate suspension. The reinstatement application can only be submitted to the *Provider*:

- personally in the customer service of the *Provider*;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a safety classification not lower than the suspended *Certificate* (see section 1.2.3.);

In case of a successful *Certificate* reinstatement, the *Provider* notifies the *Subject* and the *Subscriber* by e-mail of the fact.

4.10 Certificate Status Services

The *Provider* provides 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 are listed in the revocation lists.

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

The *Provider* publishes the revocation status of the end-user certificates after the expiration of the *Certificate*. The expired *Certificate*s are not deleted from CRL, and in case of the expired *Certificate*s, it gives OCSP service too.

The *Provider* indicates this fact in the revocation list with the use of the optional "expiredCertsOnCRL" extension.

The new status of the *Certificate* – see section: 4.9. – appeares instantly in the revocation records of *Provider* in case of suspension, reinstatement and revocation after the successful completion of the process. From that moment, the OCSP responses provided by the *Provider* shall contain the new revocation status of the certificate.

In case of suspension, reinstatement and revocation the *Provider* issues a new CRL without delay – see section: 4.9.

The *Provider* issues an extraordinary revocation list in case of *Certificate* revocation or suspension due to key compromise instantly after recording the event.

OCSP response issued by the *Provider* shall not contain "good" status information for *Certificate*s that were not issued by the given certification unit (positive OCSP).

4.10.1 Operational Characteristics

Each certification unit of the *Provider* issues revocation list with the frequency below:

- The productive (not root) SHA-256 based certification units operated within the system of the *Provider* issue CRL once in at the most of 24 hours.
- The "Microsec e-Szigno Root CA 2009" root certification unit issues a CRL once in at the most of 24 hours.
- The "Microsec e-Szigno Root CA" root certification unit issues a CRL at most per month.
- The "e-Szigno OCSP CA" root certification unit issues a CRL once at the most of 24 hours. [6].

The all-time current revocation lists for the specific *Certificate*s can be reached at the following address: `https://e-szigno.hu/en/pki-services/ca-certificates.html`

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

[6] The CRL issued by the "e-Szigno OCSP CA" does not apply to any *Certificate*, it is always empty, because the OCSP responder *Certificate*s issued by this unit includes an "ocspNoCheck" extension.

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

Online Certificate Status Protocol (OCSP)

The *Provider* publishes the revocation status of the *Certificate*s with the OCSP service too. Via this service, the same status is available as by the newest CRL.

In respect of the *Certificate* based on SHA-256, the *Provider* provides OCSP service according to the RFC 2560 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the *Certificate*s issued by the certification unit (section 1.3.1.).

The *Provider* provides OCSP services two different ways, below the characteristics of the two versions are shown.

OCSP Service Provided for Clients

- Only those *Client*s use of this version of the OCSP service, that have a valid service agreement for the maintenance of that *Certificate*. The *Provider* can identify the *Client* by the *Certificate* or by a username password pair at the query.
- This version of the OCSP service is available for all *Certificate*s, the responses always contain the current information listed in the registry of the *Provider*.
- The issued OCSP response is always made at the time of the query. The "thisUpdate" and "producedAt" time values in the OCSP response match with the time of the query.
- The "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.
- With the help of the OCSP service provided to *Client*s, an evidence always can be acquired that later verifies towards third parties the revocation status of the *Certificate* indicated in the registry of the *Provider* for the query date.

Public and Free OCSP Service

- This version of OCSP service is publicly and freely available, any *Relying Party* can avail itself of it same as the revocation lists. There is no need for authentication at query.
- This version of OCSP service can be reached through the URLs indicated on the *Certificate*s.

- Based on the RFC 6960 "Response Pre-production" process, the issued OCSP response can be created before the query and does not necessarily contain the nonce element. The *Provider* can give the same response for multiple queries. The "thisUpdate" and "producedAt" time values are identical, but these can precede the time of the query.
- The "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.
- The OCSP responses always contain the current information listed in the revocation registry of the *Provider*, but if the "thisUpdate" time of the OCSP response is earlier than the time for which the verification is carried out – which is either earlier or coincides with the time of the query –, then the OCSP response is not clear evidence for a third party regarding the revocation status of the *Certificate*.

Due to the indicated differences of the aforementioned two versions of the OCSP services, the public and free service can be considered equivalent to the service provided to the *Client*s in the following cases:

- If there is no need for OCSP response storage, rather it is used for prompt, immediate decision making. In this case, it is acceptable, that the OCSP response does not verify the validity of the *Certificate* clearly for third parties at a definite time subsequently.
- If the time span between the time of the OCSP query and the time, regarding when the verification is made, is bigger, than the difference of the "nextUpdate" and "thisUpdate" values of the stored OCSP response (which can be at most the validity period of the responser certificate used for signing the OCSP response). In this case, the OCSP responses provided by the public and free service can be accepted as a clear evidence for the third party, because the thisUpdate field in them is guaranteed to be later than the time, regarding when the verification is made.
- If the verifier party does not query the OCSP response itself (but for example uses an OCSP response attached to an archive signature), then it is not necessary to check, which sources the OCSP response came from originally. It is sufficient to verify only that the "thisUpdate" value in the OCSP response is later, than the time regarding which the verification is made.

The *Provider* ensures the aforementioned two versions of the OSCP services with the same availability.

4.10.2 Service Availability

The *Provider* ensures that the availability of the *Certificate Repository* and the terms and conditions pertaining to the *Certificate*s issued by the *Provider* is at least 99.9% per year, and the length of downtime shall not exceed at most 3 hours.

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

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

4.10.3 Optional Features

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

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

The *Provider* does not provide key escrow service for a private key belonging to a signatory *Certificate*.

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Symmetric Encryption Key Encapsulation and Recovery Policy and Practices

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

4.13 Ensuring the Electronical Verifiability of the Data Necessary for Personal Identification

The *Provider* ensures the electronical verifiability of the data necessary for personal identification in case of *Certificate*s issued based on the *Certificate Policies* referenced by this *Certification Practice Statement*, for every party who is entitled for that by legislation.

The ensurance of the electronical verifiability of the data necessary for personal identification is as follows:

1. The applicant downloads from the *Provider* the form designated for this purpose. Fills it out, inserts it into an e-dossier and signs it electronically.
2. The applicant sends the electronically signed dossier to the e-mail address of the *Provider* Customer Service.
3. The Customer Service staff member verifies the signature on the application, and the eligibility of the applicant.
4. If the application is feasible, the Customer Service staff member verifies the data indicated on the application, and gives YES or NO answer in the right part of the document. If the certificate in question can not be identified by the data given in the application, or the *Provider* did not issue a corresponding certificate, then this is stated in the document.
5. The document possibly containing the answer, and signed electronically is sent back to the e-mail address of the applicant given in the document.

The *Provider* archives both the application and the answer given to that.

5 Facility, Management, and Operational Controls

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

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

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

5.1 Physical Controls

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

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

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

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

In order to provide adequate security:

- The *Provider* implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.
- The Customer Service office of the *Provider* was designed, to be able to meet the requirements for registration services under realistic costs.
- The *Provider* constructed its mobile registration units, so that they comply with the requirements imposed on the registration service.
- The *Provider* requires its external offices and mobile units to have the same security level as the security of the *Provider* registration office and mobile units. The conditions and the expectations of the *Provider* are recorded in a contract with the external *Registration Authority*.
- The *Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

When leaving the computer room the administrator shall verify that:

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

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

5.1.3 Power and Air Conditioning

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

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems;

- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other;
- in case of lasting power outage has its own power generation equipment, which – by allowing refueling – is able to provide the necessary energy for any period of time.

The air of the outer environment shall not get into the *Data Centre* directly. The *Data Centre* air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity is reduced to the level required by the IT systems.

The *Provider* uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4 Water Exposures

The *Data Centre* of the *Provider* is adequately protected from water intrusion and flooding. The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it. The total area of water security zone is monitored by an intrusion detection system. In the protected computer room security is further increased by the use of a raised floor.

5.1.5 Fire Prevention and Protection

In the *Data Centre* of the *Provider*, a fire protection system approved by the competent fire headquarters operates. Smoke and fire detectors automatically alert the fire brigade. Water vapor based, automatic fire extinguishing system has been installed in the computer room, which is not hazardous to human life, and does not damage the IT equipment.

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

5.1.6 Media Storage

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

The *Provider* stores the primary media storages in the operational room of the certification organization, a code locked fireproof vault, the secondary copies in a vault in the customer service office.

5.1.7 Waste Disposal

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

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

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

5.1.8 Off-Site Backup

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

5.2 Procedural Controls

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

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

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

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

5.2.1 Trusted Roles

The *Provider* creates trusted roles (in the wording of the regulation, scope of activities) according to the requirements of decree 24/2016. [7] for the performance of its tasks. The rights and functions are be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

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

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

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

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

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

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

Registration officer: Individual responsible for the approval of production, issuance, revocation and suspension of end-user certificates.

Official active in the field of personalization: The individual, whose task is to manage the intelligent cards, personalization and the Certificate application compilation;

Official on duty: The individual with the task to provide 24 hour duty. Responsible for the provision of the 24 hour duty, and for the processing of received suspension and reinstatement applications without delay according to the security rules of the *Provider*.

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

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

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

5.2.2 Number of Persons Required per Task

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

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

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

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

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

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

5.2.4 Roles Requiring Separation of Duties

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

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

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

5.3 Personnel Controls

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

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

have the role to detect and gather the technical and business innovations and to organize, and share this knowledge with their colleagues.

Trusted roles can be held at the *Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *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 *Provider* only hires employees for trusted or leading roles, who

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

At the time of the appointment, shall the leading role holder *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 *Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process.

5.3.3 Training Requirements

The *Provider* trains the newly recruited employees, over the course of which they acquire

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

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

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

5.3.4 Retraining Frequency and Requirements

The *Provider* ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.

Further training is held if there's a change within the processes or the IT system of the *Provider*.

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

5.3.5 Job Rotation Frequency and Sequence

The *Provider* does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The *Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *Provider*, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability. Upon appointment every trusted role employee as part of the employment documents:

- gets written information about legal liabilities, rights, certification and management standards for the treatment of personal data,
- gets a job description that includes the concerning security tasks,
- signs a confidentiality agreement in which the related consequences non-compliant with safety measures, (criminal sanctions) can be found too.

All of these include the labor legislation or criminal consequences, that sanction the different discipline – job obligations – violation or breaking the law.

5.3.7 Independent Contractor Requirements

The *Provider* only assigns trusted roles to its employees.

The *Provider* chooses persons employed with engagement contract or subcontract to perform the other tasks, chosen if possible, from the list of previously qualified suppliers. The *Provider* concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons, and will not be exploited in any other way.The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the *Provider* does not hold any trainings for them.

5.3.8 Documentation Supplied to Personnel

The *Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents in writing:

- the organizational security regulations of the *Provider*,
- the signed confidentiality agreement,
- personal job description,
- educational materials on the occasion of the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational safety regulations.

5.4 Audit Logging Procedures

In order to maintain a secure IT environment the *Provider* implements and operates an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

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

- the time of the event;
- the type of the event;
- the 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 are available to the independent system auditors, who examine the compliance of the *Provider*'s operation.

The *Provider* logs The following events 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 *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 safety-critical data manually entered into the system;
  - safety-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 Signature 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 independent system auditors of the *Provider* evaluates the generated log files every working day.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the *Provider* uses automated evaluation tools too, that are used to monitor the resulting log entries according to preset criteria and, where necessary, alert the operational staff.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the on-line system, the logs are archived and their secure preservation is ensured by the *Provider* for the amount of time defined in Section 5.5.2.

For that time period, the *Provider* ensures the readability of archived data, and maintains the necessary software and hardware tools necessary for that.

5.4.4 Protection of Audit Log

The *Provider* protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

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

The *Provider* provides the log records with qualified *Time Stamp*s, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the *Provider* makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The *Provider* verifies the accesses in a secure way. The *Provider* preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

5.4.5 Audit Log Backup Procedures

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

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

The exact process of backups shall be defined in the backup regulations of the *Provider*.

5.4.6 Audit Collection System (Internal vs External)

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas are suspended by the *Provider* until the incident is resolved.

5.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary the *Provider* involves them in the investigation of the event. The Clients affected by triggering the event has the duty to cooperate with the *Provider* to explore the event.

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Provider* monthly review extraordinary events and perform analysis of vulnerability, based on which the *Provider* if necessary, takes measures to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat, but at least once a year the experts of the *Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access, and may affect the *Certificate* issuing process, or allow modification of the data stored in the *Certificate*. Based on the results of the analysis, the Certification Authority if necessary, will further develop its processes and systems in order to increase the overall security of the service.

5.5 Records Archival

5.5.1 Types of Records Archived

The *Provider* is prepared to the proper secure long-term archiving of electronic and paper documents.

The *Provider* archives the following types of information:

- every document related to the accreditation of the *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 *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 Signature Creation Device*;
- every electronic and paper based log entry.

5.5.2 Retention Period for Archive

The *Provider* preserves 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 signature generated with the certificate;

5.5.3 Protection of Archive

The *Provider* stores all archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper based copy of the document available.

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

During the preservation of the archived data, it is ensured that:

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

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

5.5.4 Archive Backup Procedures

The *Provider* stores the paper documents in a single original copy and makes an authentic electronic copy of the original in accordance with the relevant legislation. Electronic copies are stored according to the same rules as other protected electronic documents.

5.5.5 Requirements for Time-stamping of Records

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

The *Provider* ensures that in its service provider systems, the system clock is at maximum different from the reference time with 1 second.

The *Provider* provides the daily log files with a qualified *Time Stamp*.

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

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *Provider*'s protected computer system, and only the log files that are electronically signed and protected with qualified timestamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the *Provider* in an inner data storage operated by it.

5.5.7 Procedures to Obtain and Verify Archive Information

The *Provider* creates the log files manually or automatically. In case of an automatic logging system, the certified log files are generated daily.

The archived files are protected from unauthorized access.

Controlled access to the archived data is only available to the eligible persons:

- *Client*s are eligible to see the data stored about them;
- in legal litigation in order to provide evidence the necessary data shall be provided.

5.6 CA Key Changeover

The *Provider* ensures that the used *Certification Unit*s are continuously possessing a valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it generates a new key pair for the *Certification Unit*s and inform its Clients in time. The new provider key is generated and managed according to this regulation.

If the *Provider* changes any of its end-user *Certificate*s issuer provider Certificate keys, it complies with the following requirements:

- it discloses the affected Certificates and public keys in accordance with the requirements defined in section 2.2 ;
- after the provider re-key the end-user *Certificate*s to be issued will only be signed with the new provider keys;
- it preserves its old Certificates and public keys, and makes available the seal verification until all of the signing *Certificate* with the old provider key validity time expire.

5.7 Compromise and Disaster Recovery

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

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

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

5.7.1 Incident and Compromise Handling Procedures

The *Provider* has a business continuity plan.

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

The *Provider* annually tests the changeover to a backup system and reviews its business continuity plans.

The *Provider* has increased security tools and systems in order to minimize the software and hardware failures and data corruptions. The recoverability of services is guaranteed by the underpinning contracts and own backup tools of the *Provider*.

The *Provider* constructed its IT system providing the qualified services in such a way that in case of the dropout of any one device, it is able to continue the provision of its qualified services. If multiple units of the *Provider* fail, the *Provider* is able to launch its backup system within at most 3 hours, which is able to provide the services related to the continuously operating services – Certificate storage publication, suspension and revocation management, publication of revocation status – of the *Provider* for its *Client*s.

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

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

The *Provider* makes a full daily backup of its databases and the generated log events.

The *Provider* makes full system backups as frequently as necessary to be able to restore the full service in case of a disaster.

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

Once the problem resolved and the integrity restored, the *Provider* restarts 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

The emergency response plan of the *Provider* has an action plan in place in case the provider private keys compromise. The action plan reveals the circumstances of the compromise besides the revocation of the provider public key and the Certificate accompanying, arranges the notification of all concerned parties, takes the necessary steps against the recurrence of the compromise and, if necessary, provides new key to the service unit and the compromise affected end users. The *Provider* immediately ceases to use that particular key in case of authentication unit key compromise.

In case another certificate authority also issued certificate for the given authentication unit - by law, contract or agreement between CAs based - and over or cross certified this certification unit of the *Provider*, the *Provider* promptly informs that other Certification Authority for that given key compromise and initiates the certificate revocation belonging to the key in question.

The *Provider* publishes a notice about the provider public key revocation.

5.7.4 Business Continuity Capabilities After a Disaster

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

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

The secondary services site is placed so far away from the primary site that a probable disaster cannot reach both locations simultaneously.

The *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 *Provider* restores its devices damaged during the disaster and the original service security level as quickly as possible

5.8 CA or RA Termination

The *Provider* notifies the end users and the National Media and Infocommunications Authority at least 60 days before the shutdown in case of the planned discontinuance of any of its services.

The Certification Service and Certificate Status Service Shutdown

At the same time with the notification about the service shutdown, the *Provider* shuts down the following services:

- registration,
- Certificate creation,
- Certificate issuance,
- Certificate renewal,
- Certificate modification
- re-key.

The *Provider* at least 20 days before the planned termination shuts down the following services:

- managing the Certificate revocation /suspension,

At the same time of the termination, the *Provider* shuts down the following services:

- information provision,

- *Certificate* publishing,
- *Certificate* revocation status publishing,
- Online Certificate Status Protocol.

Before a planned discontinuation, the *Provider* engages in negotiations about the taking over of its services with other Certification Authorities whose rating is identical to its own. Under section 9.3 , it will hand over its records, including confidential user data, to such a Certification Authority or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.

The *Provider* takes measures concerning the revocation of provider *Certificate*s (and destroying private keys) during the 60 day period – depending on the outcome of the negotiations.

The *Provider* informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The *Provider* is to inform its *Client*s by electronic mail, and *Relying Parties* by means of a publication on its website.

Pursuant to section 2.2., the *Provider* will publish an announcement 5 days before its "Microsec e-Szigno Root CA", "Microsec e-Szigno Root CA 2009" and "e-Szigno OCSP CA" *Certificate* is revoked.

Upon terminating a service, the *Provider* produces a full scope backup of its data contained in its IT system, affixing a qualified *Time Stamp* to it.

The *Provider* provides for authorised *Relying Parties* the possibility to interpret the data appearing in its revoked and suspended *Certificate*s records if necessary.

In order to make the handing over of its data to another service provider possible, the *Provider* places data on media and in a format which the new service provider can receive or provides the new service provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this.

6 Technical Security Controls

The *Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Provider* manages the cryptographic provider keys during their whole life-cycle within a *Hardware Security Module* that has appropriate Certification.

Both the *Provider* and the system supplier and execution contractors have significant experience with certification service deployment and they use internationally recognized technology.

The *Provider* continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

6.1 Key Pair Generation and Installation

The *Provider* makes sure that the generation and management of all the private keys generated by it – for itself, for some of its departments (for example *Certificate Repository*, *Registration Authority*) and for the *Subjects* – is secure and complies with the regulatory requirements in force and with industry standards.

6.1.1 Key Pair Generation

The *Provider* uses key generation algorithms for the key-pair generation, which comply with the requirements set out in the following normatives:

- ETSI TS 119 312 [20];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [6] 92. § (1) b) .

The *Provider* in case of the generation of a key pair of its own ensures:

- 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 [22] , or
  - meets the requirements of FIPS 140-2 [30] level 3 or higher, or
  - meets the requirements of CEN 14167-2 [32] workshop agreement,
  - is a reliable system that is evaluated in accordance with MSZ/ISO/IEC 15408 [21] 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 *Provider*, it ensures that:

- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.
- In case of *Certificate Policies* requiring the use of a *Qualified Electronic Signature Creation Device* or a *Hardware Security Module* the *Provider* generates the signing private key on the user's *Subject Qualified Electronic Signature Creation Device* or on its *Hardware Security Module* (or in case of Server-Based Signature Service on the *Hardware Security Module* of the provider) which makes the disclosure of the signing private key impossible.
- If the private key is handed over to the *Subject*: The signer keys generated outside a *Qualified Electronic Signature Creation Device* or a *Hardware Security Module* are stored in an adequately secure environment by the *Provider* to prevent the disclosure. After the documented handover of the signer private key to the *Subject* the *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 *Provider* ensures that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6 , and the private key is not one of a known weak key pair.

In case of an *Subject* generated key pair:

- the production of keys shall be done in a properly secure environment that is under the supervision of the *Subject*;
- the *Subject* shall ensure the proper protection of the generated private key;
- the *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 *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 *Provider* responsible for key management and as a witness a trusted person independent from the operation of the *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 *Provider* generated the *Subject*'s private key, then the following requirements are met:

If the Private Key is Handed Over to the *Subject*:

- Until the key handover, the *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 *Provider* shall ensure that the private keys and their activation data can only be taken over by the *Subject*.
- The *Provider* shall gain sufficient evidence of the handover of the private key to the *Subject*, and the exact time of the handover.
- After the handover of the signer private key to *Subject*, the *Provider* shall not reserve any copy of the signer private key.

If the *Subject* uses the Server-Based Signature Service:

- During the whole service, the *Provider* shall store 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 people.
- The *Provider* shall use an identification procedure that ensures that the private keys can only be used by the *Subject*.
- The *Provider* shall store sufficient evidence of the fact that, the handover of the disposal over the private key to the *Subject* happened at a specific authentic time.
- The *Provider* shall ensure that following the handover of the disposal over the private key only the *Subject* is able to run the identification process necessary for the usage of the private key.

In case of *Certificate Policies* requiring the use of a *Hardware Security Module* (in particular *Qualified Electronic Signature Creation Device*) the private key of the *Subject* together with the *Hardware Security Module* providing the secure storage and usage of the private key, is handed over to the *Subject* in person at the registration point with the closed envelope containing the activation code.

Following the key generation the *Qualified Electronic Signature Creation Device* containing the private key is in transport mode, which ensures that the private key can not be used for electronic signature creation before the activation of the *Qualified Electronic Signature Creation Device*.

In case of *Certificate Policies* not requiring the use of a *Hardware Security Module*, in all cases the *Client* generates the private key, so it does not have to be delivered to the *Client*.

6.1.3 Public Key Delivery to Certificate Issuer

If the key pair is generated by the *Subject*, the following provisions shall be complied with:

- the public key shall be sent to the *Provider* in a manner that it can be unambiguously assigned to the *Subject*;
- the *Certificate Application* process shall prove that the *Subject* really owns the private key corresponding to the public key.

In case of end user keys generated by the *Subject*, the *Subject* sends the *Provider* a PKCS#10 formatted request which he or she signs with the private key belonging to the public key to be indicated on the Certificate. The PKCS#10 formatted request contains the public key generated by the *Subject* and the *Subject* data to be indicated on the *Certificate*, so both requirements are met.

6.1.4 CA Public Key Delivery to Relying Parties

The *Provider* discloses the status information related to the provider Certificates for the Relying Parties by the following methods:

- The *Provider* publishes the full provider certificate hierarchy containing every root and intermediate provider certificate from which every current provider Certificate is downloadable (see at the Provider certificates point at the `https://e-szigno.hu/en/pki-services/ca-certificates.html` url).
- The denomination of the root and intermediate certification units and the root *Certificate*s' hash is in the 1.3.1 section of the *Certification Practice Statement*.
- The Certificates of the intermediate certification units are published on the certified Hungarian provider list [35] maintained and published by the National Media and Infocommunications Authority within the framework of the European common regulations [34]. The list contains every provider certificate (even the expired and revoked ones).
- For the online certificate status response signer responders the *Provider* – according to the best international practice – issues *Certificate*s with very short validity periods, thus eliminating the necessity of checking the revocation status of the *Certificate*s. The current status of the *Certificate*s is continuously available at the webpage of the *Provider* at the `https://e-szigno.hu/en/pki-services/ca-certificates.html` address.

The *Provider* discloses for the *Relying Parties* the status information related to the *Certificate* of the certification units operated by it, and of the units that take part in the online certificate status service by the following methods:

- The status information related to the *Certificate*of the root certification units is available on the webpage of the *Provider*.
- The status change information of the intermediate (not root) certification units' certificates is 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 *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 *Provider* guarantees that in case of key compromise or other problem no new *Certificate* will be issued for the old private key signing the OCSP responses . The *Provider* issues the OCSP response *Certificate*s for new, secure private keys.

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

6.1.5 Key Sizes

The *Provider* uses algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [20];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [6] 92. § (1) b) .

The *Provider* uses at least 2048 bit RSA keys in every currently active root and intermediate provider *Certificate* and even in the *Certificate*s of the *Time-Stamping Unit*s and the OCSP responders.

6.1.6 Public Key Parameters Generation and Quality Checking

The *Provider* generates the keys according to the description of the section 6.1.1.

Hardware/Software Key Generation

The generation of the *Provider* keys used for *Certificate* issuance is done with a *Hardware Security Module*, which has FIPS 140-2 Level 3 certifications. The denomination of each device is in the 8. section.

The other keys – necessary for the internal operation of the certification Authority – keys are generated by the *Provider* on a *Hardware Security Module* or on a computer operating in a secure environment.

The signature key pair generation of *Certificate*s issued according to *Certificate Policies* requiring the use of a *Qualified Electronic Signature Creation Device* or a *Hardware Security Module* is done on a *Qualified Electronic Signature Creation Device* (cryptographic hardware device) with on-board hardware key generation.

The key generation of *Certificate*s issued according to Certificate Policies not requiring the use of a *Qualified Electronic Signature Creation Device* or a *Hardware Security Module* is always done by the *Subject*.

Verification of Compliance of Parameters

The compliance of the key generation parameters is verified by the system from two points of view:

- checking the conformity of the random number generation used for the parameters (whether the generation is sufficiently statistically random),
- checking the fulfilment of the requirements for parameters.

Every *Hardware Security Module* used in the system is able to statistically test the uniformity and independence of the bit sequence it generated. The modules enable the invocation of the tests through a standard interface.

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

The *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 *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 *Provider* includes the Key Usage extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [29] 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 signer private key may only be used for electronic signature creation by the *Signatory*, any other uses of the key are specifically prohibited.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

The *Provider* private keys used for the certification organization *Certificate* and issuance are stored at a physically secure location, in a secure *Hardware Security Module*.

The *Provider* the *Qualified Electronic Signature Creation Device*s used to create *Certificate*s issued according to *Certificate Policies* requiring the use of a *Qualified Electronic Signature Creation Device* stores at a physically secure location, with special attention in order to prevent the illegal use of private keys after the on-board key generation until handing over to the *Subject*.

In case of *Certificate*s issued according to *Certificate Policies* not requiring the use of a *Qualified Electronic Signature Creation Device* the *Provider* does not issue private keys to the *Subject* beforehand, eliminating the need to ensure the preservation of the end-user private keys.

The *Provider* deletes the signing private keys stored on the *Hardware Security Module*s which are out of order in as defined in the device's manual so that it is virtually impossible to restore the keys.

6.2.1 Cryptographic Module Standards and Controls

The systems of the *Provider* issuing *Certificate*, signing OCSP responses and CRL lists store the private keys used for the electronic signature creation in such secure hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [22], or

- the requirements of FIPS 140-2 [30] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [32] 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 [21] 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 denomination of the used *Hardware Security Module* is described in section 8.

The *Provider* provider keys are only stored in coded forms outside of the *Hardware Security Module*. For coding only those algorithms and key parameters are used by the current order of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [6] 92. § (1) b) that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The *Provider* provider private keys are stored in a physically secure site even in an encrypted form, in the safe of the *Data Centre* , where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the *Provider* destroys the coded keys or recodes them again using algorithm and key parameters that ensure higher protection.

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

The *Provider* implements the "n out of m" at the activation of the private key related key management functions. The parameters are determined so that the simultaneous presence of at least two; trusted role holder employees is needed for the critical operations carried out with its provider private keys.

6.2.3 Private Key Escrow

The *Provider* does not escrow its own provider private key.

The *Provider* does not provide for the end-user signer private keys any escrow service, under no circumstance does it store their copy, multiple usage, except for a private key generated on a *Qualified Electronic Signature Creation Device*, stored on a *Qualified Electronic Signature Creation Device* until its hand over to the *Subject*.

6.2.4 Private Key Backup

The *Provider* makes security copies of its provider private keys, before putting the private key into service as described in section 6.2.1. in a protected environment, in the simultaneous presence of

at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 6.2.2..

The *Provider* stores the backup copy in duplicate, and at least one copy of those is stored at a different place from the service provider location.

The same strict safety standards are applied to the management and preservation of backups as for the operation of the production system.

The *Provider* does not make any copy of the end-user signer private keys.

6.2.5 Private Key Archival

The *Provider* does not archive its private keys and the end-user signer private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Provider* is created in a *Hardware Security Module* that meets the requirements.

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

The *Provider* only exports the private key from the *Hardware Security Module* for the purpose of making a secure copy.

The export and loading of the provider private keys is performed according to section 6.2.2.

6.2.7 Private Key Storage on Cryptographic Module

The *Provider* keeps its private keys used for service provision in *Hardware Security Module*s according to section 6.2.1.

Private keys are stored and used in the *Hardware Security Module* as specified in the certification of the device with full compliance with the related operating instructions.

6.2.8 Method of Activating Private Key

The *Provider* keeps its provider private keys in a secure *Hardware Security Module* and complies with its user guide and the requirements outlined in the certification documents. The *Hardware Security Module* can only be activated by the corresponding operator cards and the private keys within the *Hardware Security Module* can not be used before activating the module. The *Provider* keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the *Provider*.

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

In case of the end-user private keys generated by the *Provider* it ensures that the private keys and the private key activation data are generated and managed in a properly secure way that excludes the possibility of the unauthorized usage of the private key.

The *Qualified Electronic Signature Creation Device*s prepared for the *Signatory* and configured and handed over by the *Provider* to the *Subject* so that:

- it can be clearly established that the device has not been used for electronic signature creation before the handover;
- before the electronic signature creation the *Subject* shall identify itself towards the *Electronic Signature Creation Device*.

In case of Server-Based Signature Service provision the *Provider* ensures that:

- the private key generated for the *Subject* has not been used for signature creation before its delivery to the *Subject*;
- before creating the electronic signature the *Subject* identifies itself towards the *Electronic Signature Creation Device*.

In case of *Subject* generated private key the protection of the private key is the *Subject*'s full responsibility.

6.2.9 Method of Deactivating Private Key

Provider Private Keys

The private key used by the *Provider*, and managed by the cryptographic devices becomes deactivated if (in a regular or irregular way) the device is removed from active status. This can happen in the following cases:

- the user deactivates the key,
- the power supply of the device is interrupted (switched off or power supply problem),
- the device enters an error state.

The private key deactivated like this can not be used until the module is in active state again.

End-User Private Keys

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* ensures that the private keys become deactivated in the following cases:

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

The deactivated key and the *Qualified Electronic Signature Creation Device* may only be used for electronic signature creation after the re-identification of the *Subject*.

In case of the Server-Based Signature Service the technical solution applied by the *Provider* ensures that the signer keys become deactivated in the following cases:

- the power supply of the device ceases for some reason;
- the connection with the application of the *Subject* disconnects for some reason;
- the *Subject* gives a deactivation (exit) instruction.

The deactivated key may only be used for electronic signature creation after the re-identification of the *Subject*.

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 *Subject*.

6.2.10 Method of Destroying Private Key

Provider Private Keys

The discarded, expired or compromised *Provider*'s private keys are destroyed in a way that makes further use of the private keys impossible.

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

The *Provider* destroys each backup copy of the private key in a documented way in such a way that its restoration and usage becomes impossible.

End-User Private Keys

The destruction of the discarded signer private keys issued on a *Qualified Electronic Signature Creation Device* is possible by the physical destruction of the *Qualified Electronic Signature Creation Device*, which is the responsibility of the *Subject*.

For the request of the *Client* in its presence the *Provider* destroys the *Qualified Electronic Signature Creation Device* presented by the *Client* personally free of charge.

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

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 *Subject*.

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 *Subject*.

The discarded signer 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 *Provider* is stored in a cryptographic module that

- has a certification according to ISO/IEC 19790 [22], or
- has a certification according to FIPS 140-2 Level 3 [30], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [32] 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 *Provider* archives every *Certificate* its certification organization issued for ten years after the end of the validity period or until until the completion of the incurred dispute related to the *Certificate* (or to the electronic signature based on the *Certificate*).

For the same time period, the *Provider* preserves devices, with which the content of the *Certificate* can be established.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Keys and Certificates of the Root Certification Units

The validity period of the *Provider* root certification unit certificates and the private keys belonging to them shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority.
The validity period of the *Provider* root certification unit certificates and the private keys:

- the key of the "Microsec e-Szigno Root CA" root certification unit is valid until 2017.04.06;
- the key of the "e-Szigno OCSP CA" root certification unit is valid until 2017.04.26;
- the key of the "Microsec e-Szigno Root CA 2009" root certification unit is valid until 2029.12.30.

The Keys and Certificates of the Intermediate Certification Units

The validity period of the *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*.

The intermediate (not root) certification unit keys of the *Provider* are valid until the expiration date of the *Certificate*s belonging to them.

End-User Certificates

The validity period of the end user *Certificate*s issued by the *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 *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 *Provider* revokes the related *Certificate*s.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

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

In case of *Qualified Electronic Signature Creation Device*s and *Hardware Security Module*s provided by the *Provider* for the *Subject*, the *Provider* provides:

- the activation data is created and installed to the *Qualified Electronic Signature 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 *Subject* using a safe method.

In case of the provision of the Server-Based Signature Service for the *Signatory*:

- The *Provider* uses an identification procedure that ensures that the private key can be only activated by the *Subject* authorized to do so.

In case of private keys created for and handed over to the *Subject* via software by the *Provider* the *Provider* creates the activation data and assigns them to the private key in a physically secure environment, with an adequate quality random number generator;

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

6.4.2 Activation Data Protection

The employees of the *Provider* manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

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

- the *Provider* only records the activation data for the purpose of delivering them to the *Subject*;
- the *Provider* distributes the activation data to the *Subject*s using a secure method.

The protection of the activation data of the private keys created by the *Subject*, is the duty and responsibility of the *Subject*.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the *Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *Provider* are sufficiently protected from unauthorized access;
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

6.5.2 Computer Security Rating

Microsec lays much emphasis on customer complacency. In order to keep up the high quality services, the *Provider* operates a quality management system according to the ISO 9001 standard since 23. January 2002. Compliance with this standard is certified by Lloyd's Register Quality Assurance.

Microsec pays close attention to the security of the systems it operates, therefore, in the main areas of its activity it operates a ISO/IEC 27001 compliant information security management system (previously BS 7799) since 19. may 2003. Compliance with this standard is certified by Lloyd's Register Quality Assurance.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The *Provider* only uses applications and devices in its production IT system that:

- are commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by a reliable party for the *Provider* during which design structured development methods and controlled development environment were used, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

Procurement of IT tools is performed in a way that excludes changes to the hardware and software components using reliable, regularly qualified suppliers.

The hardware and software components applied for the provision of services are not used for other purposes by the *Provider*.

The *Provider* prevents the malicious software from entering into the devices used for certification services with appropriate security measures.

The hardware and software components are checked regularly for malicious software prior the first usage, and subsequently.

The *Provider* acts with the same carefulness in case of program update purchases as at the acquisition of the first version.

The *Provider* employs reliable, adequately trained staff over the course of installing software and hardware.

The *Provider* only installs softwares to its service provider IT equipment necessary for the purpose of service provision.

The *Provider* has a version control system where every change of the IT system is documented.

The *Provider* operates automatic monitoring system to record all unauthorized changes, which records all changes in every file and in case of changes in the monitored files it generates a log entry or sends an alert to the system operators.

6.6.2 Security Management Controls

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

Each *Hardware Security Module* applied by the *Provider* has been verified, tested and evaluated. The *Provider* verifies the integrity of the modules:

- following the acquisition of the devices during the takeover,
- immediately before the first usage,
- regularly during operation.

The *Provider* deletes the provider keys from the *Hardware Security Module*s permanently or temporarily withdrawn from use.

The *Provider* stores the unused *Hardware Security Module*s at a physically protected location.

6.6.3 Life Cycle Security Controls

The *Provider* ensures the protection of the used *Hardware Security Module*s during their whole life cycle.

During the operation of the IT services, devices and operating systems used for the provision of the services the *Provider* taking into account the safety aspects of the equipment life cycle.

- it uses in its system a *Hardware Security Module* which has the right certification;
- at the reception of the *Hardware Security Module*, during the qualitative takeover it verifies that the protection of the *Hardware Security Module*s against tampering was ensured during transportation;
- it stores the *Hardware Security Module* at a secure location, and the protection of the *Hardware Security Module* against tampering is ensured during storage;

- during the operation it continuously complies with the requirements of the *Hardware Security Module* appropriation of security, user guide and the certification report;
- it deletes the private keys stored in the discarded *Hardware Security Module*s in a way that it is virtually impossible to restore the keys.

6.7 Network Security Controls

The *Provider* keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too. The *Provider* implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The *Provider* checks the authenticity and integrity of every software component at their first loading.

The *Provider* applies proper network security measures for example:

- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .

The *Provider* undergoes or performs a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least once per quarter.

6.8 Time-stamping

For the protection of the integrity of the log files and other electronic files to be archived the *Provider* uses qualified electronic *Time Stamp*s issued by the e-Szignó Certification Authority.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The end-user *Certificate*s issued by the *Provider* and the provider certification unit (root and intermediate) *Certificate*s used during the service comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [29]

- RFC 5280 [26]
- RFC 6818 [27]
- ETSI EN 319 412-1 [15]
- ETSI EN 319 412-2 [16]
- ETSI EN 319 412-5 [19]

7.1.1 Version Number(s)

The provider certification unit (root and intermediate) *Certificate*s used by the *Provider* and the end-user *Certificate*s issued by the *Provider* are "v3" *Certificate*s according to the X.509 specification [29].

The provider certification unit (root and intermediate) *Certificate*s used by the *Provider* and the end-user *Certificate*s issued by the *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. [26]
- Serial Number
  The unique identifier generated by the *Certificate* issuer certification unit.

  In case of the end-user *Certificate*s the "Serial Number" field contains a random number with at least 8 byte entropy.
- Algorithm Identifier
  The identifier (OID) of the algorithm set used for the creation of the electronic seal certifying the *Certificate*.

  The *Provider* uses the following algorithm:

  – "sha256WithRSAEncryption" (1.2.840.113549.1.1.11),
- Signature
  Electronic seal made by the *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 *Provider* supports the RSA algorithm in the end-user *Certificate*s. The length of the public key is at least 1024 bit.

  The value to be included in this field:

  – "rsaEncryption" (1.2.840.113549.1.1.1)
- *Subject* Public Key Value
  The public key of the *Subject*.
- Issuer Unique Identifier
  Not filled out.
- *Subject* Unique Identifier
  Not filled out.

7.1.2 Certificate Extensions

the *Provider* only uses the following certificate extensions according to the X.509 specification [29]:

Certificate of the Root Certification Unit

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

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

  In case of the self-signed root certification unit certificate the value is identical with the value of the *Subject* key identifier field.

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

- Subject Alternative Names – not critical
  OID: 2.5.29.17

  It is filled in according to section 3.1.1.

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

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

  The "pathLenConstraint" field 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. It is not present.

The above fields are always filled out. There is not 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 *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 seal certifying the *Certificate*.

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

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

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  It is filled in according to section 3.1.1.

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

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

  The "pathLenConstraint" field 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. It is not 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 *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 *Provider* provides online certificate status service. The availability of this service is indicated here.
- To facilitate the certificate chain building the *Provider* gives the access path through http or ldap protocol of the *Certificate* of the *Certificate* issuer certification unit.

The above fields are always filled out. There is not any more *Certificate* extensions.

End-User Certificate

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

  In case of end-user certificates, the *Provider* fills 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 [7] from which it can be established that:
    * the *Certificate* is qualified;
    * the private key related to the *Certificate* is protected by a *Qualified Electronic Signature Creation Device* (exclusively in case of policies requiring the usage of *Qualified Electronic Signature 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 [14] , which the *Certificate* complies with too. The certification policies specified by the ETSI EN 319 411-2 are the following:
    * QCP-n: Policy for EU qualified *Certificate* issued to a natural person;
    * QCP-n-qscd: Policy for EU qualified *Certificate* issued to a natural person where the private key and the related *Certificate* reside on a qualified signature creation device.

  In all cases of end-user certificates at least one *Certificate Policy* is indicated according to what the *Provider* issued the *Certificate* and according to what it later acts on. At least

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

one such *Certificate Policy* identifier (OID) and the related *Certification Practice Statement* availability (URL) is indicated on the *Certificate*s issued by the *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 seal certifying the *Certificate*.

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

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

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

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

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

  The "pathLenConstraint" field is not present in the end-user *Certificate*s.

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

  In end-user *Certificate*s the value is exclusively set to the following: "nonRepudiation";

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

  Not 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. The CRL availability related to the *Certificate* is present here (url).

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

  In case of end-user certificate certificates the field contains the following data:

  – For the purpose of the fast and reliable verification of the current *Certificate* revocation status, the *Provider* provides online certificate status service. The availability of this service is indicated here.

  – To facilitate the certificate chain building the *Provider* gives 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 are present in every end-user qualified *Certificate*:

  – the *Certificate* is an EU qualified *Certificate* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);

  – the transactional limit related to the *Certificate* – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2);

  – that statement that the *Provider* retains the registration data related to the *Certificate* for 10 years after the expiration of the *Certificate* – 'id-etsi-qcs 3' (0.4.0.1862.1.3);

  – that statement that the private key related to the *Certificate* resides inside a *Qualified Electronic Signature Creation Device* – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – only in the case of certification policies requiring the use of a *Qualified Electronic Signature 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 signing purposes (the value of the field is 'id-etsi-qct-esign') – 'id-etsi-qcs 6' (0.4.0.1862.1.6);

The above fields are always filled out according to the given rules. There is no more filled out *Certificate* extensions.

7.1.3 Algorithm Object Identifiers

The denomination of the algorithm that has been used to certify the *Certificate*. The following algorithms are used by the *Certification Authority* for sealing the end-user *Certificate*s:

- "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)

7.1.4 Name Forms

The *Provider* uses a distinguished name – composed of attributes defined in the standards RFC 5280 [26], ETSI EN 319 412-2 [16], ETSI EN 319 412-3 [17] and ETSI EN 319 412-4 [18] – for the Subject identification in the *Certificate*s issued based on this *Certification Practice Statement*.

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

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

7.1.5 Name Constraints

The *Provider* does not use name constraints with the use of the "nameConstraints" field.

7.1.6 Certificate Policy Object Identifier

The *Provider* includes the not critical (*Certificate Policy*) extension in the *Certificate*s according to the requirements of the Section 7.1.2..

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The *Provider* can put short information related to the *Certificate* usage into the *Certificate Policy* extension Policy Qualifier field. The field contains 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* issues version "v2" certificate revocation lists according to the RFC 5280 [26] 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 algorithm set used for creating the electronic seal certifying the revocation list . The name and ID of the algorithm sets used by the *Provider*:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Signature
  The electronic seal of *Certification Authority* certifying the revocation list. The given certification unit certifies 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
  The date of the entry into force of the revocation list. Value according to UTC with encoding according to RFC 5280 [26]. In case of the revocation lists issued by the *Certification Authority* this is the same as the issuance time.
- Next Update
  The issuance time of the next revocation list (see Section 4.10.). Value according to UTC with encoding according to RFC 5280 [26].
- 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 are in this field.

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

- expiredCertsOnCRL – not critical
  The *Certification Authority* indicates 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 is 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.

  The *Certification Authority* need not fill this field.
- Hold Instruction – not critical
  The management of the suspended certificate can be in this field.

  The *Certification Authority* need not fill this field.

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

7.3 OCSP Profile

The *Provider* operates an online certificate status service according to the RFC 2560 [23] and RFC 6960 [28] standard.

7.3.1 Version Number(s)

The *Provider* supports the online certificate status requests and responses conforming to the “v1” version according to the standards RFC 2560 [23] and RFC 6960 [28].

7.3.2 OCSP Extensions

The *Provider* may optionally include the above OCSP extension:

- expiredCertsOnCRL – not critical
  The *Certification Authority* indicates 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 *Provider* may include the above OCSP registration extension:

- Reason Code – not critical
  The reason of the revocation is 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 *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 *Provider* location. Before the site inspection, the *Provider* has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the *Provider* meets the requirements of the eIDAS Regulation [1] and the related Hungarian legislation and the requirements of the applied *Qualified Signature Certificate Policy*(s) and the corresponding *Certification Practice Statement*(s).

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

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [12]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11]
- 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 [13]
- 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; [14]

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

The conformity certificate issued in accordance with the conformity assessment report is published on the webpage of the *Provider*.

The *Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Provider* uses the following cryptographic modules for the certification of the *Certificate*s, and for the provider private key storage:

- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.18.15-3;
- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.22.6-3;
- nCipher nShield F3 PCI nC4033P-500, firmware verzió: 2.33.60-3;
- nCipher nShield F3 PCI nC4033P-500, firmware verzió: 2.38.7-3;
- nCipher nShield F3 PCIe nC4433E-500, firmware verzió: 2.61.2-3.

The above devices have FIPS 140-2 [30] Level 3 certification.

The *Provider* provides the following *Qualified Electronic Signature Creation Device*s for the *Subject*s:

- Smartcard which consist of ST19WR66I microchip and Touch & Sign2048 V1.00 signature creation application.
  (Supplier: ST Incard)
- MultiApp ID Citizen 72k smartcard which consist of S3CC91C microchip, MultiApp v1.1 Java Card platform and IAS Classic v.3.0 electronic signature application.
  (Supplier: Gemalto)
- IDOneClassIC smartcard which consist of P5CT072VOP microchip, ID-One Cosmo 64 RSA v5.4 platform and IDOneClassIC v1.0 electronic signature application.
  (Supplier: Oberthur)
- IDClassic 340 smartcard which consist of P5CC081V1A microchip, MultiApp ID v2.1 Java Card platform and IAS Classic v.3 electronic signature application (version: MPH117 V2.2 filter).
  (Supplier: Gemalto)
- ARX CoSign v7.1 Secure Signature Creation Device (version: v7.1).
  (Supplier: DocuSign (ARX))

The *Provider* has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The *Provider* keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

In addition to the external audit, the *Provider* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Provider* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation. (see section: 1.3.1.)

8.1 Frequency or Circumstances of Assessment

The *Provider* has the conformance assessment carried out annually on its IT system performing the provision of the services .

If the *Provider* cooperates with an external *Registration Authority*, then its processes are audited annually.

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

8.2 Identity/Qualifications of Assessor

The *Provider* performs 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 is performed by a person who:

- is independent from the owners, management and operations of the examined *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 *Provider*.
- remuneration is not dependent on the findings of the activities carried out during the audit.

8.4 Topics Covered by Assessment

The review covers the following areas:

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

If the *Provider* cooperates with an external *Registration Authority*, and it issued a provider *Certificate* for the certification unit of another organization then the listed areas are examined at these external organizations as well.

8.5 Actions Taken as a Result of Deficiency

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

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

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

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 *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 *Provider* publishes the summary report on the assessment. It does not publish the discrepancies revealed during the independent system assessment, they are treated as confidential information.

9 Other Business and Legal Matters

9.1 Fees

The *Provider* publishes fees and prices on its webpage, and makes them available for reading at its customer service.

The *Provider* may unilaterally change the price list. The *Provider* publishes any modification to the price list 15 days before it becomes effective. Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service contract and its annexes – the general terms of contract in particular.

9.1.1 Certificate Issuance or Renewal Fees

See section: 9.1.

9.1.2 Certificate Access Fees

The *Provider* grants free of charge on-line access to its *Certificate Repository* for the *Relying Parties*.

9.1.3 Revocation or Status Information Access Fees

The *Provider* provides free of charge on-line CRL and OCSP service for the *Relying Parties* on the status of all end-user and intermediate *Certificate*s it issued.

9.1.4 Fees for Other Services

See section: 9.1.

9.1.5 Refund Policy

See section: 9.1.

9.2 Financial Responsibility

In order to facilitate trust the *Provider* complies with the financial and liability requirements below.

9.2.1 Insurance Coverage

The *Provider* has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

- The *Provider* has liability insurance to ensure reliability.
- The liability insurance policy shall cover the following damages caused by the *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 *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 *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 *Provider* manages clients' data according to legal regulations. The *Provider* has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

By applying for a *Certificate*, and signing the service agreement, *Client*s consent to the *Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the *Provider*'s services go offline; moreover to forwarding such information to the *Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

*Subject*s shall make a declaration as to their consent to the disclosure of a *Certificate* on the certificate application form that is linked to the service agreement.

The *Provider* uses clients' data solely in connection with the provision of its services. The *Provider* discloses *Subject*s' and *Represented Organization*s' data appearing in a *Certificate* together with the *Certificate* in case a *Subject* consents to this. The *Provider* stores their data that are not entered in a *Certificate* in a secured manner, for the purpose of providing evidence about the *Subject*s' identity, *Represented Organization*s' organisational identity, and that of its miscellaneous data provision related obligations. The *Provider* retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the *Provider* sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The *Provider* provides for the confidentiality and intactness of information that is not public during the forwarding of *Client*s' data.

9.3.1 Scope of Confidential Information

The *Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 9.3.2;
- besides the *Client* data:
  - private keys and activation codes,
  - certificate applications and Service Contracts,
  - transaction related data and log data,
  - non-public regulations,
  - all data whose public disclosure would have an adverse effect on the security of the service.

9.3.2 Information Not Within the Scope of Confidential Information

The *Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

In case the *Subject* grants consent, the *Provider* treats all of the data it indicates in a *Certificate* as non-confidential information. Such data appear in the *Certificate* application form linked to the service agreement in a clearly marked way.

The *Provider* manages the revocation and suspension status of the end-user and intermediate provider *Certificate*s as public information and makes it available without restriction to the *Relying Parties* by publishing a revocation list (CRL) and by providing on-line Certificate Status Protocol (OCSP) service. The disclosed information contains the serial number of the Certificate, the time of the revocation and the reason for revocation. For more information, see section 7.2. and 7.3.

9.3.3 Responsibility to Protect Confidential Information

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

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

The *Provider* processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following cases:

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the *Provider* – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the *Provider* according to the section (1) of the Eüt. [6] 90. § to investigating authorities and national security services free of charge.

  The *Provider* records the fact of data transfers, but does not inform involved clients about it.

- **Provision of information in the scope of litigation**

  In the course of litigation and non-litigious actions under common law, the *Provider* may hand over – in case their being affected is certified – *Subject* identity information and the information verified by the *Provider*, to an adverse party or its representative, as well as it may disclose them to the inquiring court.

  The *Provider* records the fact of data transfers and informs impacted clients about it.

- **Disclosure upon owner's request**

  Upon a *Client*'s personal request to do so or on the basis of its authorisation granted officially, in writing, the *Provider* reveals confidential user information pertaining to the *Client* to third parties.

- **Miscellaneous circumstances resulting in the disclosure of information**

  Upon termination of its activity the *Provider* is bound to hand over its records subject to the access obligations together with confidential user data to the trusted service provider that takes it over according to section (6) of 88. § Eüt. [6].

9.4 Privacy of Personal Information

The *Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [4].

The *Provider*:

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

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

The *Provider* stores identification data, data about the *Subject* appearing in the *Certificate*, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.

The *Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

In case of pseudonymous *Certificate*s, the *Provider* hands over the data related to the real identity of the *Subject* to third parties solely in cases where this is stipulated by a legal regulation or if the *Subject* or in case of an *Organizational Certificate*, the *Represented Organization* has granted its consent to that in writing.

9.4.1 Privacy Plan

The *Provider* has a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing is published on the webpage of

the e-Szignó Certification Authority on the following URL: `https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

The *Provider* may disclose the data of the *Subject*s indicated in the *Certificate* based on the written consent of the *Subject*.

The *Provider* may indicate the unique provider identifier assigned to the *Subject* in the *Certificate*.

9.4.4 Responsibility to Protect Private Information

The *Provider* stores securely and protects the personal data related to the *Certificate* issuance and not indicated in the *Certificate*. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

9.4.5 Notice and Consent to Use Private Information

The *Provider* only discloses personal data indicated in the *Certificate*s with the written consent of the *Client*.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the 90. § of the Electronic Administration Act [6] the *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 *Provider* shall not harm any intellectual property rights of a third person.

The owner of the private and public key issued by the *Provider* to clients is the *Subscriber* and the full user is the *Subject* regardless of the physical media that contains and protects the keys.

The owner of the *Certificate* issued by the *Provider* to its clients is the *Provider* and its full user is the *Subject*.

The *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 *Provider* which is disclosed as defined in sections 7.2. and 7.3.

The unique provider identifier issued to the *Client*s by the *Provider* is the property of the *Provider* which

is disclosed as a part of the *Certificate* by the *Provider* in the *Certificate Repository*.

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

The present *Certification Practice Statement* is the exclusive property of the *Provider*. The *Client*s, *Subject*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Certification Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

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

The rules of the application of the software provided for the use of the service by the *Provider* is accessible in the description of the software and it is included in the user's guide referenced in the description.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the *Provider* is in the *Certification Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- The *Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;

- The *Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [5] in relation to the *Client*s which are in a contractual relationship with it.
- The *Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [5] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8.).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Provider* is not responsible:

- for the *Subject* activities related to the private key;
- for the *Subject* activities related to the *Electronic Signature Creation Device*;
- for the certificate verification and usage activities of the *Relying Parties*;
- for the regulations issued by the *Relying Parties* or others.

Certification Authority Obligations

The *Provider* shall fulfil the requirements defined in section (2) of article 24. of the eIDAS regulation [1].
The *Provider*'s basic obligations is that it shall provide the services in line with the *Qualified Signature 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 *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 Signature Creation Device* activation code and the keys uploaded to the device;
- in general for the compliance with its obligations.

9.6.2 RA Representations and Warranties

The customer service has the task of representing the *Provider* at end-users in connection with the services. It performs the following tasks in the scope thereof:

- participates in selling the services;
- performs the registration of *Subject*s;
- receives requests pertaining to various certificate operations (suspension, revocation, reinstation, certificate replacement);
- receives and handles data modification related filings;
- participates in revocation status publication;
- offers information provision activity to *Client*s and *Relying Parties* in connection with its activities associated with the services provided by the *Provider*;

The *Registration Authority* is responsible:

- for establishing the personal identity of *Subject*s;
- for establishing the organisational identity of *Represented Organization*s, and in this latter case for establishing the right of representation of an individual acting in the name of a *Represented Organization*;
- for the genuineness of recorded registration data;
- for providing information to those using the services as to the contents and availability of the *Qualified Signature Certificate Policy* and the *Certification Practice Statement*, as well as the terms and conditions of using the service prior to concluding the service agreement;
- in general to fully comply with its obligations.

9.6.3 Subscriber Representations and Warranties

Subscriber Responsibility

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

Subscriber Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *Provider* while using the service including requesting and applying the *Certificate*s and private keys.

The obligations of the *Subscriber* are determined by this *Certification Practice Statement*, the service agreement and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Qualified Signature Certificate Policy*s.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *Certification Practice Statement*.
- *Subscriber*s are entitled to specify which *Subject*s should be allowed to receive certificates, in writing, and *Subscriber*s have the right to request the suspension and revocation of such certificates.
- *Subscriber*s have the right to request the suspension and revocation of certificates.
- *Subscriber*s are entitled to appoint an organisational administrator.

Subject Responsibility

The *Subject* 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 Signature Creation Device*, private key and *Certificate* according the regulations;
- the secure management of its private key and activation code;
- the secure management of the *Electronic Signature Creation Device*
- the correct and secure usage of the service in case of Server-Based Signature Service ;
- for the immediate notification and for full information of the *Provider* in cases of dispute;
- to generally comply with its obligations.

***Subject* obligations**

The *Subject* shall:

- read carefully this *Certification Practice Statement* before using the service;
- completely provide the data required by the *Provider* necessary for using the service, and to provide truthful data;
- if the *Subject* 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 *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 *Provider* in writing and without delay in case a legal dispute starts in connection with

  any of the electronic signature or the *Certificate*s associated with the service;
- cooperate with the *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;
- in case a *Subject*'s private key, *Electronic Signature Creation Device* or the secret codes necessary for activating the device end up in unauthorized hands or are destroyed, the *Subject* is obliged to report this fact to the *Provider* promptly and in writing, and will also be obliged to initiate the suspension and/or revoking of the *Certificate*s and terminating the usage of the *Certificate*;
- the *Subject* shall answer to the requests of the *Provider* within the period of time determined by the *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 *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 *Provider* only displays data that are corresponding to reality in issued *Certificate*s. Accordingly, the *Provider* validates data to be entered in *Certificate*s according to the *Certification Practice Statement*;
- acknowledge that the *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 *Subject* and in this case, the *Subject* is bound to terminate the usage of the *Certificate*;
- acknowledge that the *Provider* has the right to suspend, and revoke *Certificate*s if the *Subscriber* fails to pay the fees of the services by the deadline;
- in case of requesting an *Organizational Certificate*, acknowledge that the *Provider* will issue the *Certificate* solely in the case of the consent of the *Represented Organization*;
- in case of requesting an *Organizational Certificate*, acknowledge that the *Represented Organization* has the right to request the revocation of the *Certificate*;
- acknowledge that the *Provider* has the right to suspend, and revoke *Certificate* if the *Subscriber* violates the service agreement or the *Provider* becomes aware that the *Certificate* was used for an illegal activity.

***Subject* Rights**

- *Subject*s have the right to apply for *Certificate*s in accordance with the *Certification Practice Statement*.
- In case this is allowed by the applicable *Certificate Policy*, *Subject*s are entitled to request the suspension or the revocation of their *Certificate*s, according to this *Certification Practice Statement*.

9.6.4 Relying Party Representations and Warranties

The *Relying Parties* decide based on their discretion and/or their policies about the way of accepting and using the *Certificate* . During the verification of the validity for keeping the security level guaranteed by the *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 Signature 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 Signature Certificate Policy* and the *Certification Practice Statement*.

9.6.5 Representations and Warranties of Other Participants

Represented Organisation responsibility

The *Represented Organization* is solely responsible for the documents it issues. In particular for document in which it attests that a *Subject* is a staff member of the *Provider*, moreover is entitled to appear in the *Represented Organization*'s *Certificate*. In case the information appearing in any certification made out by the *Represented Organization* is changed, reporting this to the *Provider* without delay is the *Represented Organization*'s responsibility.

Represented Organisation rights

- The *Provider* only issues *Certificate*s in which the *Represented Organization*'s name is indicated in possession of the *Represented Organization*'s consent.
- The *Represented Organization* is entitled to suspend and revoke *Certificate*s in which the *Represented Organization*'s name was also indicated.

9.7 Disclaimers of Warranties

The *Provider* excludes its liability if:

- *Subject*s do not follow the requirements related to the management of the *Electronic Signature Creation Device* and of the private key;
- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it;
- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by the National Media and Infocommunications Authority algorithmic decree.

9.8 Limitations of Liability

- The *Provider* is not responsible for damages that arise from the *Relying Party* failing to proceed as recommended according to effective legal regulations and the *Provider*'s

regulations in the course of validating and using certificates, moreover its failing to proceed as may be expected in the situation.

- The *Provider* shall only be liable for contractual and non-contractual damages connected to its services in relation to third parties with respect to provable damages that occur solely on account of the chargeable violation of its obligations.
- The *Provider* is not liable for damages that result from its inability to tend to its information provision and other communication related obligations due to the operational malfunction of the Internet or one of its components because of some kind of external incident beyond its control.
- The *Provider* engages in data comparison with an authentic database, before issuing a *Subject*'s *Certificate*. The *Provider* will not assume any liability for damages arising out of the inaccuracy of information provided by such authentic databases.
- The *Provider* assumes liability solely for providing the services in accordance with the provisions of this *Certification Practice Statement*, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

Administrative Processes

The *Provider* logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

Financial Liability

The *Provider* has appropriate deposit according to the relevant legal requirements for its financial liability and to guarantee costs related to its termination and for reliability.

The *Provider* has liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

The *Provider* specifies the highest level of the obligation undertaken at the same time. If the *Certificate* is used for signing transaction exceeding this limit, then the *Provider* is not liable for any damage it may have caused. In case of qualified *Certificate*s the highest level of the obligation

undertaken at the same time is the value indicated in the *Certificate*. If there is no indicated transaction limit then it is 200 000 000 HUF.

In connection with the services provided as a qualified provider, the *Provider* defines tariff plans, which differ from each other in the highest level of the obligation undertaken at the same time and the financial liability of the *Provider* as stated below.

Plans	Maximum transaction value [M HUF]	Limitation of the provider liability [M HUF]
bronze	1	0, 1
silver	20	5
gold	80	20
platinum	200	50

If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

9.9 Indemnities

9.9.1 Indemnification by the *Provider*

The detailed rules of the indemnities of the *Provider* are specified in this regulation (see section: 9.8.), the service agreement and the contracts concluded with the *Client*s.

9.9.2 Indemnification by Subscribers

The *Subscriber* and the Subject are liable for damages to the *Provider* for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3 Indemnification by Relying Parties

See section: 9.8.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific *Certification Practice Statement* is specified on the cover of the document.

9.10.2 Termination

The *Certification Practice Statement* is valid without a time limit until withdrawal.

Section 9. of the *Certification Practice Statement* shall remain effective even after the termination of the *Certification Practice Statement*'s effect (regardless of the manner in which effectiveness is terminated) in connection with any and all *Certificate*s which the *Provider* will have issued while the *Certification Practice Statement* was effective.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Certification Practice Statement* the *Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

The *Provider* guarantees that in case of a the *Certification Practice Statement* withdrawal, requirements for the protection of the confidential data remain in effect.

9.11 Individual Notices and Communications with Participants

The *Provider* maintains a customer service in order to contact with its *Client*s.

The *Client*s may make their legal declarations to the *Provider* solely in writing, and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

Issued *Certificate*s may also be suspended by telephone. Notifications of other nature may also be given in writing, in the form of electronic mail or fax.

The e-Szignó Certification Authority informs its *Client*s by means of publication on its webpage or in electronic mail.

9.12 Amendments

The *Provider* reserves the right to change the *Certification Practice Statement* in a controlled way in case of the change of normative rules, safety requirements, market conditions or other circumstances.

In exceptional cases (for example the need for taking critical security measures) the changes can be put into force with immediate effect.

9.12.1 Procedure for Amendment

The *Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Provider* has a number of internal

security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 8.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Provider*'s certification organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certification Authority.

The team produces internal, non-public working copies of the regulations as it collects changes, and these undergo internal review before being published. The *Provider* strives to only issue new regulations at the least frequent intervals possible.

The *Provider* reviews the *Certification Practice Statement* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change 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 *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 *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 *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 *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 *Provider* issues a new version number in case of even the smallest change to the *Certification Practice Statement*, 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 *Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Provider* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The *Client* in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the *Provider* or the use of issued *Certificate*s shall be addressed to the customer care centre office in written form. The *Provider* notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Provider* may request the provision of information required for giving a response from the submitter. The *Provider* investigates complaints within 30 days, and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the *Provider* involved, the submitter may initiate consultation with the *Provider* and the *Relying Parties*. All participants of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof; and the submission, the *Provider*'s response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The *Relying Parties* shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

9.14 Governing Law

The *Provider* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Provider* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

9.15 Compliance with Applicable Law

The applicable regulations:

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [6];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [7];
- (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 [8];
- (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 [9];
- (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 [10];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [4];
- (Hungarian) Act V of 2013. on the Civil Code. [5].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The *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 *Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Certification Practice Statement*, it would waive the enforcement of claims for damages.

9.16.5 Force Majeure

The *Provider* is not responsible for the defective or delayed performance of the requirements set out in the *Qualified Signature Certificate Policy* and the *Certification Practice Statement* if the reason for failure or delay was a condition that is outside the control of the *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] (Hungarian) Act III of 1952 on Civil Procedure .

[3] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

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

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

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

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

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

[9] (Hungarian) 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 .

[10] (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 .

[11] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[12] 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;.

[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 .

[14] 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; (Replaces ETSI TS 101 456).

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

[16] 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; (Replaces ETSI TS 102 280).

[17] 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 (Replaces ETSI TS 101 861).

[18] 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.

[19] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[20] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

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

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

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

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

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

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

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

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

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

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

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

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

[33] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.

[34] EU Trusted Lists of Certification Service Providers, (`https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers`.

[35] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

[36] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített aláíró tanúsítvány hitelesítési rendek.

[37] e-Szignó Certification Authority - Qualified Signing Certificate Policies .