e-Szignó Certification Authority

Non eIDAS covered Certificates Certification Practice Statement

ver. 2.11

Date of effect: 25/09/2019

OID	1.3.6.1.4.1.21528.2.1.1.168.2.11
Version	2.11
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	23/09/2019
Date of effect	25/09/2019

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

Version	Description	Effect date	Author(s)
2.0	New policies according to the RFC 3647.	01/07/2016	Csilla Endrődi, Szabóné Sándor Szőke, Dr. Kornél Réti
2.1	Changes according to the NMHH comments.	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.
2.2	Changes according to the auditor comments.	30/10/2016	Sándor Szőke, Dr.
2.3	Changes according to the NMHH comments.	30/04/2017	Sándor Szőke, Dr.
2.4	Yearly revision.	30/09/2017	Sándor Szőke, Dr.
2.6	Global revision. Introducing identity validation by state notaries. Smaller improvements.	24/03/2018	Sándor Szőke, Dr.
2.7	Yearly revision.	15/09/2018	Sándor Szőke, Dr.
2.8	Changes based on the suggestions of the auditor.	14/12/2018	Sándor Szőke, Dr.
2.11	Yearly revision.	25/09/2019	Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document is the *Certification Practice Statement* concerning the issuance of not eIDAS conform certificates service of e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or *Service Provider*).

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

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

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

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 *Service Provider* should know. This aims to foster that its *Client*s and future *Client*s:

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

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

The content and format of the present document complies with the requirements of the IETF RFC 3647 [22] framework. It consists of 9 sections that contain the security requirements, processes defined by the *Service Provider* and the practices to be followed during the provision of services. To strictly preserve the outline specified by IETF RFC 3647, section headings where the document does not impose a requirement have the statement "No stipulation".

Considering the end user activity related to the services used, besides the present *Certification Practice Statement* further requirements may be found in the *Time-Stamping Policy* [35], the General Terms and Conditions and the service agreement concluded with the provider, the *Certificate Policies* applied by the *Service Provider* (see section 1.2.1) and other regulation or document independent from the *Service Provider* as well.

1.2 Document Name and Identification

Issuer	e-Szignó Certification Authority
Document name	Non eIDAS covered Certificates Certification Practice Statement

Document version	2.11
Date of effect	25/09/2019

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

1.2.1 Certificate Policies

All *Certificate*s issued by the *Service Provider* refer to that *Certificate Policy* on the basis of 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 further numbers were allocated within Microsec's own scope of authority, the interpretation of it is as follows:

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

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

OID	DENOMINATION	SHORT NAME
1.3.6.1.4.1.21528.2.1.1.155.2.1	1, Not according to the eIDAS , certification class III., for natural persons issued on *Cryptographic Hardware Device*, Certificate Policy prohibiting the use of pseudonyms.	HETHN
1.3.6.1.4.1.21528.2.1.1.156.2.1	1Not according to the eIDAS , certification class III., for natural persons issued as a software token , Certificate Policy prohibiting the use of pseudonyms.	HETSN

1.3.6.1.4.1.21528.2.1.1.158.2.11	Not according to the eIDAS , certification class III., for legal persons issued as a software token , Certificate Policy prohibiting the use of pseudonyms.	HEJSN
1.3.6.1.4.1.21528.2.1.1.160.2.11	Not according to the eIDAS , certification class II., Certificate Policy prohibiting the use of pseudonyms.	KExxN
1.3.6.1.4.1.21528.2.1.1.190.2.11	Not according to the eIDAS , code signing, certification class III. controlling the issuance of Certificates, Certificate Policy prohibiting the use of pseudonyms.	HKxxN
1.3.6.1.4.1.21528.2.1.1.191.2.11	Not according to the eIDAS , code signing, certification class II. controlling the issuance of Certificates, Certificate Policy prohibiting the use of pseudonyms.	KKxxN

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

The *Service Provider* doesn't issue *Certificate*s with pseudonym.

The detailed requirements of the listed *Certificate Policy*(s) can be found in " e-Szignó Certification Authority – non eIDAS covered Certificates Certificate Policies ver.2.11." [34]

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

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

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

In case of a *Certificate Policy* ([xxxHx]) that requires the usage of *Cryptographic Hardware Device*, the *Service Provider*: guarantees that the private key belonging to the *Certificate* is stored only on such *Cryptographic Hardware Device* that has at least one of the following certifications:

- Certificate issued in any of the member states of the European Union certifying that the equipment is a *Qualified Electronic Signature Creation Device*;
- Common Criteria [29] certification according to CEN SSCD PP [31], at least at level EAL-4;
- FIPS 140-2, Level 2 (or higher) certification [28].

In case of the *Codesigning Certificate* the *Service Provider* conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at

`https://casecurity.org/resources/r`

url. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Among the present *Certificate Policies*:

- each *Certificate Policy* complies with the [LCP] *Certificate Policy* defined in the ETSI EN 319 411-1 [12] standard;
- except the a [KExxN], [KKxxN] *Certificate Policy* each *Certificate Policy* complies with the [NCP] *Certificate Policy*;
- the [HETHN] *Certificate Policy* complies with the [NCP+] *Certificate Policy*.

Compliance with the ETSI Certificate Policies

In cases when an ETSI Certificate Policy is based on another ETSI Certificate Policy and this way contains all the requirements of it, only the Identifier of the Higher Level Certificate Policy is referenced in the issued *Certificate*s.

	[LCP]	[NCP]	[NCP+]
HETHN	(x)	(x)	X
HETSN	(x)	X	
HEJSN	(x)	X	
KExxN	X		
HKxxN	(x)	X	
KKxxN	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 25/09/2019 date of effect, until withdrawal. The effect automatically terminates at the cessation of services or issuance of the newer version of the *Certification Practice Statement*.

Personal Scope

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

Geographical Scope

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

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

1.2.3 Security Levels

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

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

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

Based on the used container in descending order by security:

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

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

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

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

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

On an individual basis in special cases, the *Service Provider* can deviate from the strict application of the above list with regard to particular tasks (for example the personal identification for III. certificate class *Certificate*s in case of new qualified *Certificate* application or the modification of an existing one as a result of the same procedural identification rules it accepts the identification required for qualified *Certificate*).

1.3 PKI Participants

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 *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 *Service Provider*

Name:	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number:	01-10-047218 Company Registry Court of Budapest
Head office:	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C
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-Szignó Certification Authority

Customer service:

Hungary, H-1033 Budapest,
Ángel Sanz Briz str. 13.,
Graphisoft Park South Area, Building C

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

Introduction of the *Service Provider*

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

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [5] (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. [9] coming into force.

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

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

- qualified certificates for electronic seals

- qualified time stamping
- qualified archiving (preservation of digital signatures).

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

- qualified certificates for website authentication.

Quality and Information Security

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Service 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/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

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

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Service Provider*

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

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

`https://www.microsec.hu/hu/biztonsagi-garanciak`

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

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

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

Business Providing Certification Services

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

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

Services

The *Service Provider* provides the following services to the *Subscriber* within the framework of the present *Certification Practice Statement*:

- Issuance of Non-eIDAS Certificates

The Issuance of Non-eIDAS Certificates Service

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

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

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

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

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

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

Certificate Types

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

The e-Szignó 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 Profession* means a *Certificate* issued to a natural person which is not an *Organizational Certificate* and which contains the title or profession of the *Subject* in the "Title" field.
- *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 – verified by the *Service Provider* – 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.
- 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 *Service Provider* issues test certificates – firstly to test their system, on the other hand, to third parties in order to test the services. No legal effect belongs to the certificates, and the *Service Provider* does not take any responsibility for their issuance, usage and service availability.

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

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

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

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

Certification Units

In the following those *Certification Unit*s will be described, that appear in the system of the e-Szignó Certification Authority and stay under the effect of this *Certification Practice Statement*.

Further information can be found in the the certificate hierarchy of the *Service Provider* at the following address:

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

Active, SHA-256 based RSA hierarchy

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

  Issues SHA-256 based *Certificate*s for the *Certification Unit*s of the *Service Provider*. This *Certification Unit* has a self certified (SHA-256 based) certificate.

- "Advanced Class 3 e-Szigno CA 2009"

  This unit issues not *Codesigning Certificate*s to natural and legal persons exclusively according to the III. certification class. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- "Advanced CodeSigning Class3 e-Szigno CA 2016"

  This unit issues *Codesigning Certificate*s to natural and legal persons exclusively according to the III. certification class. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- "Advanced Class 2 e-Szigno CA 2009"

  This unit issued *Certificate*s to natural and legal persons exclusively according to the II. certification class till the 30th of June 2016. Certified by "Microsec e-Szigno Root CA 2009". This unit hasn't issued pseudonymous *Certificate*s.

- "Advanced eIDAS Class2 e-Szigno CA 2016"

  This unit issues other than *Codesigning Certificate*s to natural and legal persons exclusively according to the II. certification class from the 1st of July 2016. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- "Advanced CodeSigning Class2 e-Szigno CA 2016"

  This unit issues *Codesigning Certificate*s to natural and legal persons exclusively according to the II. certification class. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- "Advanced Pseudonymous e-Szigno CA 2009"

  This unit issues pseudonymous *Certificate*s to natural persons exclusively according to the II. and III. certification class. Certified by "Microsec e-Szigno Root CA 2009".

  Presently it is not used.

- "e-Szigno SSL CA 2014"

  This unit issues only *Website Authentication Certificate*s and *Certificate*s for networking authentication exclusively according to the III. certification class. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- "Class2 e-Szigno SSL CA 2016"

  This unit issues only *Website Authentication Certificate*s and *Certificate*s for networking authentication exclusively according to the II. certification class. Certified by "Microsec e-Szigno Root CA 2009". This unit does not issue pseudonymous *Certificate*s.

- OCSP responders;

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

The following *Certification Unit*s of the *Service Provider* issue *Certificate*s for the public administration:

- "Signature KET e-Szigno CA 2009"

  Productive not qualified *Certification Unit*, certified by KGYHSZ and issues not qualified *Certificate*s for public administration usage.

- "Class3 KET e-Szigno CA 2018"

  Productive not qualified *Certification Unit*, certified by KGYHSZ and issues not qualified *Certificate*s for public administration usage.

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

Latest, ECC based hierarchy

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

  that issues ECC based *Certificate*s for the *Certification Unit*s of the *Service Provider*. This *Certification Unit* has a self certified (ECC based) certificate.

- "e-Szigno Qualified TSA CA 2017"

  Productive qualified *Certification Unit*, issues *Certificate*s for Time Stamping Authorities, that are certified by the "e-Szigno Root CA 2017" .

- "e-Szigno Class3 CA 2017"

  This unit issues other than *Codesigning Certificate*s to natural and legal persons exclusively according to the III. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- "e-Szigno Class3 CodeSigning CA 2017"

  This unit issues *Codesigning Certificate*s to natural and legal persons exclusively according to the III. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- "e-Szigno Class2 CA 2017"

  This unit issues other than *Codesigning Certificate*s to natural and legal persons exclusively according to the II. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- "e-Szigno Class2 CodeSigning CA 2017"

  This unit issues *Codesigning Certificate*s to natural and legal persons exclusively according to the II. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- "e-Szigno Pseudonymous CA 2017"

  This unit issues pseudonymous *Certificate*s to natural persons exclusively according to the II. and III. certification class. Certified by "e-Szigno Root CA 2017".

  Presently it is not used.

- "e-Szigno Class3 SSL CA 2017"

  This unit issues only *Website Authentication Certificate*s and *Certificate*s for networking authentication exclusively according to the III. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- "e-Szigno Class2 SSL CA 2017"

  This unit issues only *Website Authentication Certificate*s and *Certificate*s for networking authentication exclusively according to the II. certification class. Certified by "e-Szigno Root CA 2017". This unit does not issue pseudonymous *Certificate*s.

- OCSP responders;

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

The aforementioned units have ECC based Certificates.

Every end-user RSA key is at least 2048 bit in the hierarchy above.

Retired, SHA-1 based RSA hierarchy

The *Service Provider* issued SHA-1 *Certificate*s based "Microsec e-Szigno Root CA" *Certification Unit* beforehand. The *Service Provider* does not issue *Certificate*s according to this hierarchy. The *Service Provider* keeps the SHA-1 based hierarchy for the verifiability of the previously issued *Certificate*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 *Service Provider*. This *Certification Unit* has a self-certified certificate.

- "Advanced e-Szigno CA3"

  This unit issued *Certificate*s to natural persons and automatisms exclusively according to the III. certification class. Certified by "Microsec e-Szigno Root CA". This unit did not issue pseudonymous *Certificate*s.

- "Advanced e-Szigno CA2"

  This unit issued *Certificate*s to natural persons and automatisms exclusively according to the II. certification class. This unit issued III. class pseudonymous *Certificate*s. Certified by "Microsec e-Szigno Root CA".

- "Signature e-Szigno CA6"

  This unit only issued non-qualified *Certificate*s compliant with public administrative Certificate Policies. The *Certificate*s were Certified by the Public Administrative Root Certification Authority (KGYHSZ).

- "Microsec e-Szigno Server CA"

  Certified by "Microsec e-Szigno Root CA" and KGYHSZ. This *Certification Unit* certified the time stamping units, and issued *Certificate*s compliant with public administrative certificate policies to automatisms.

- Time stamping units

  that were certified by "Microsec e-Szigno Server CA". The e-Szignó Certification Authority issued SHA-1 based, non-qualified time stamps with the private keys of these units. The *Certificate*s of the time stamping units contained "timeStamping" extended key usage.

- "e-Szigno OCSP CA" (self certified)

  OCSP responder certificate issuer *Certification Unit*.

- "Advanced e-Szigno OCSP Responder"

  OCSP responder – certified by the "e-Szigno OCSP CA".

Intermediate *Certification Unit*s in the SHA-1 based hierarchy issued "closing CRLs".

Publication of the *Root Certificate*s

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

- The SHA-1 fingerprint 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 fingerprint 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 fingerprint: `56 2c 85 5b 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68`,
  the SHA-1 fingerprint 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 fingerprint [1] :
  `89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e`,
  the SHA-256 fingerprint 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 "e-Szigno Root CA 2017" *Root Certificate* SHA-1 fingerprint:
  `89 d4 83 03 4f 9e 9a 48 80 5f 72 37 d4 a9 a6 ef cb 7c 1f d1`,
  The "e-Szigno Root CA 2017" *Root Certificate* SHA-256 fingerprint:
  `be b0 0b 30 83 9b 9b c3 2c 32 e4 44 79 05 95 06 41 f2 64 21 b1 5e d0 89 19 8b 51 8a e2 ea 1b 99`

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

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

The expired *Certificate* will be phased out from these trusted certificate stores.

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

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

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

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

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 *Service Provider* by default.

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

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

Chained Certification Service

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

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

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

is bound to announce the cross-certification to the National Media and Infocommunications Authority, and ask for registration (except it is already registered at the National Media and Infocommunications Authority). These rules apply to other services related to electronic signatures as subordinate services (e.g. time stamp).

1.3.2 Registration Authorities

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

Tasks of the office:

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

The customer service operated by the *Service Provider* receives requests pertaining to various certificate actions, and initiates their processing.

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

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

1.3.3 Subscribers

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

- *Subscriber*
  - signs the service agreement with the *Service Provider*,
  - accepts the General Terms and Conditions,
  - defines the scope of the *Applicant*s,
  - may appoint *Organizational Administrator*s,
  - responsible for the payment of the fees arising from the usage of the service.
- *Subject*
  - the *Service Provider* issues the *Certificate* for the *Subject*.

1.3.4 Relying Parties

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

The *Service 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 its activity, the *Represented Organization* is the actual *Organization* also indicated within the *Certificate*. The *Service Provider* does not necessarily have a contractual relationship with the *Represented Organization*, but the *Service Provider* shall not issue an *Organizational Certificate* without the approval of that *Organization*. The *Service 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 *Service Provider* based on the present *Certification Practice Statement* can be only used for purposes defined in the *Certificate* attribute values set by the *Service Provider*, the *Certificate Policy* and the *Certification Practice Statement*. The purpose of usage typically can be encryption or authentication, but depending on the concrete usage scope, there can be differences within these in the set attribute values (see section 6.1.7.).

1.4.2 Prohibited Certificate Uses

*Certificate*s issued in accordance with the present *Certificate Policies*, and the private keys belonging to them using for other purposes than purposes defined in the *Certificate* attribute values set by the *Service Provider*, the *Certificate Policy* and the *Certification Practice Statement* is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

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

1.5.2 Contact Person

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

Contact person	Process management department leader
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

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

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

1.5.4 Practice Statement Approval Procedures

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

1.6 Definitions and Acronyms

1.6.1 Definitions

II. certification class	A group of non-qualified *Certificate Policies*, that make possible the *Certificate* issuance based on the *Applicant*'s remote registration.
III. certification class	A group of non-qualified *Certificate Policies*, that bound the *Certificate* issuance to the *Applicant*'s personal registration.
Data Centre	A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and security systems.
Subject	A natural person, *Organization*, or IT device, system, unit identified by the *Certificate*. The *Subject* can be the *Applicant* itself or the device under the control of the *Applicant*.

Subject Unique Identifier	The globally unique identifier of the *Subject*, given by the *Service Provider*. The identifier is in the "Subject DN Serial Number" field of the *Certificate*, according to the requirements of section 3.1.1.
Authentication	The public key certificate-based authentication is that process, when the *Relying Party* verifies the identity of the *Certificate Subject* (natural person, organization or application, website, service, server) by means of a method for this purpose, in which the private key of the *Subject* is used to be identified, and the identity is verifiable with the *Certificate*.
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. [9] 91.§ 1. paragraph)*
Trust Service	"Means an electronic service normally provided for remuneration which consists of: • the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or • the creation, verification and validation of *Website Authentication Certificate*; or • the preservation of electronic signatures, seals or certificates related to those services; " *(eIDAS [1] 3. article 16. point)*
Trust Service Policy	"A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common security requirements." *(Act CCXXII. of 2015. [9] 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 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 *Service Provider* in order to use some of its services.
Relying Party	In case of encryption, the party who encrypts the electronic document for the recipient. In case of authentication, the party who verifies the identity of the party seeking to be identified during a procedure for this purpose.
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. [9] 1. § point 21.)*
Suspension	A temporary pause of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate*. The *Certificate* suspension is not definitive; the suspended *Certificate*'s validity can be restored.
Root Certificate	Also known as top level certificate. Self-signed *Certificate*, which is issued by a specific *Certification Unit* for itself, which is signed with its own private key, so it can be verified with its own public key – indicated on the certificate.
HSM: Hardware Security Module	A hardware-based secure device that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions.

Certification Authority	A *Trust Service Provider*, who/which identifies the requester within the confines of the certification service, issues *Certificate*s, keeps a record, receives the *Certificate* related data changes, and publishes the regulations belonging to the *Certificate* , the public keys and the information on the current state (especially on possible revocation) of the *Certificate*.
Certification Unit	A unit of the *Service Provider*'s system that signs the *Certificate*s. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a *Certification Unit*. It is possible that a Certification Authority simultaneously operate several *Certification Unit*s.
Certificate Policy	"A *Trust Service Policy* which concerns the *Certificate* issued within the framework of the *Trust Service*." *(Act CCXXII. of 2015. [9] 1. § 24. point)*
Applicant	That natural person who acts during the application for the given *Certificate*.
Represented Organization	The *Organization*, which is represented by the *Organizational Administrator* during the actions related to the *Certificate*s issued to the given *Organization*.
Compromise	A cryptographic key is considered as compromised, when it can be assumed, that unauthorized person has access to it.
Public Administration Root CA	Organization unit defined in the E-Signature Government Decree [10] in section 3. § (2).
Intermediate Certification Unit	A *Certification Unit* whose *Certificate* was issued by another *Certification Unit*.
Cryptographic Key	A unique digital data string controlling a cryptographic transformation, the knowledge of which is required for encryption, decryption and the creation and verification of digital signatures.

Key Management	The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation and termination of keys which are closely linked to the used security method.
Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to the key-pair owner that the *Subject* shall keep strictly secret. In case of encryption, the recipient needs his private key for decrypt the document that was encrypted for him. In case of authentication, the party to be identified shall use his private key during the verification procedure. During the issuance of *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.
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to key-pair owner, which should be made public. The disclosure is typically in the form of a *Certificate*, which links the name of the actor with its public key. In case of encryption, the recipient public key is needed for creating an encrypted document for him. In case of authentication, the public key of the party to be identified is needed, to verify his identity. The authenticity of the *Certificate*s can be verified with the public key of the *Certification Unit*.
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices.
Registration Claim	The data and statement given beforehand for the preparation of the *Certificate Application* and the service agreement to the *Service Provider* by the *Client* in which the Client authorizes the *Service Provider* for data management.
Registration Authority	Organization that checks the authenticity of the *Certificate* holder's data and verifies that the *Certificate Application* is authentic, and it has been submitted by an authorized person.

Extraordinary Operational Situation	An extraordinary situation causing disturbance in the course of the operation of the *Service Provider*, when the continuation of the normal operation of the *Service Provider* is not possible either temporarily or permanently.
Server Authentication Certificate	*Certificate* which is used to authenticate a server or one of its services. The CN field of these *Certificate*s always contains a FQDN or an IP address. These type of *Certificate*'s are issued for example for the CISCO VPN server, domain controller, SCEP server, VPN server.
Organization	Legal person.
Organizational Certificate	A *Certificate*, the *Subject* of which is the *Organization*, or which presents that the natural person *Subject* belongs to an *Organization*. In this case the name of the *Organization* is indicated in the "O" field of the *Certificate*.
Organizational Administrator	The natural person who is acting in the name of the *Subscriber*, and is eligible to issue the *Certificate Application*, to grant the issuance of the *Certificate*, to act during the application, replacement, suspension, reinstatement and revocation of the *Certificate*s issued to the *Subscriber*.
Trust Service Practice Statement	"The statement of the *Trust Service Provider* of the detailed procedures or other operational requirements used in connection with the provision of particular *Trust Service*s." *(Act CCXXII. of 2015. [9] 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. [9] 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. [9] 1. § point 44.)*

Certificate Application	The data and statements given by the *Applicant* to the *Service Provider* for *Certificate* issuance, in which the *Applicant* reaffirms the authenticity of data to be indicated on the *Certificate*.
Certificate Repository	Data repository containing various *Certificate*s. A Certification Authority has a Certificate Repository in which the issued *Certificate*s are disclosed, but the system containing *Certificate*s available to the application on the computer of the *Subject* and the *Relying Party* is also called Certificate Repository.
Encryption	During the public-key cryptography, the process by which the sender using the recipient's public key encrypts the document, which then can be only decrypted by the addressed party private key.
Client	The collective term for the *Subscriber* and every related *Applicant* denomination.
Revocation	The termination of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate* too. The *Certificate* revocation is permanent, the revoked *Certificate* cannot be reinstated any more.
Revocation Status Records	The internal records of the suspended and revoked *Certificate*s which includes the fact of the suspension or revocation and the time of the suspension or revocation given in seconds maintained by the *Certification Authority*.

1.6.2 Acronyms

CA	Certification Authority	
CP	Certificate Policy	
CPS	Certification Practice Statement	
CRL	Certificate Revocation List	
eIDAS	electronic Identification, Authentication and Signature	
KGYHSZ	Public Administration Root CA	Kormányzati Gyökér Hitelesítés Szolgáltató
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 *Service Provider* 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 *Applicant* consented to.

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

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

2.2 Publication of Certification Information

The *Service Provider* discloses on its webpage

- its provider *Certificate*s;
- the end user *Certificate*s, provided that the *Applicant* consents to the disclosure;

Service Provider Certificates

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

- The denomination of the root certification units, and the hash of its root certificates in the *Certification Practice Statement*. (see section: 1.3.1.) The information related to their change of status are available at the website of the *Certification Authority*.
- The status change of *Certificate*s of intermediate (non-root) certification units is is disclosed on the *Certificate Revocation List*s, its website and within the confines of the online certificate status response services.
- For the signers of the online certificate status responses the *Service Provider* – compliant with 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.

  Each OCSP responder *Certificate* contains an indication that its revocation status doesn't need to be checked.

In case of key compromise, or any other problems there won't be any more new *Certificate* issued for the OCSP response signer old private key later. The *Service Provider* issues 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 *Service Provider* discloses status information related to the end-user *Certificate*s which it had issued:

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

The end-user *Certificate* revocation status information

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

2.2.1 Publication of the *Service Provider* Information

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

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

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

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

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

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

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

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

- the *Certificate*s of the root certification units operated by it are disclosed before commencing the service;
- the *Certificate*s of the intermediate certification units operated by it are disclosed within 5 workdays after issuance;
- the *Service Provider* discloses in case of the *Applicant*'s consent the end-user Certificates in its *Certificate Repository* after issuance without delay.

2.3.3 The Changed Revocation Status Publication Frequency

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

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

2.4 Access Controls on Repositories

Access is provided to anyone for reading purposes to public information of the *Certificate*s and status information disclosed by the *Service Provider* according to the particularities of publication.

The information disclosed by the *Service Provider* shall only be amended, deleted or modified by the *Service Provider*. The *Service Provider* shall prevent unauthorized changes to the information with various protection 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 [24] and IETF RFC 6818 [25] recommendations name-specific format requirements, in addition the *Service Provider* supports the Subject Alternative Names and Issuer Alternative Names fields located amongst the extensions.

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

3.1.1 Types of Names

Denomination of the *Subject*

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

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

  In case of natural persons, the name of the natural person *Subject* is in this field in the same form as verified by the *Service Provider* according to the section 3.2.3.

  In case of an *Organization* the organization's full or shortened name is in this field in the same form as verified by the *Service Provider* according to the section 3.2.2.

  If neither the full nor the shortened name of the Organization fits because of the size limit of the *Certificate*, then the unambiguous abbreviation of the Organization name is presented here.

  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*).

  In case of server authentication *Certificate* the requested domain name or IP address is in this field.

  It may contain only existing domain name or IP address which is used legally by the *Applicant*.

  In case of server authentication *Certificate* only this field and the "Subject Alternative Names" filed contains domain name or IP address.

  The server authentication *Certificate* shall not be pseudonym.

  Always filled out.

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

  In case of natural person *Subject*s the surname of the *Subject* is in this field, where the *Service Provider* generates the surname from the full name in the CN field.

  The *Service Provider* always fills it.

  If the *Subject* of the *Certificate* is an *Organization*, it is not filled.

  In case of server authentication *Certificate* the filling is optional. If it is filled then the surname of the *Applicant* is here.

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

  In case of natural person *Subject*s the given name of the *Subject* is in this field, where the *Service Provider* generates the given name from the full name in the CN field.

  The *Service Provider* always fills it.

  If the *Subject* of the *Certificate* is an *Organization*, it is not filled.

  In case of server authentication *Certificate* the filling is optional. If it is filled then the given name of the *Applicant* is here.

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

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

- 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 IETF RFC 4043 [23] recommendation:

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

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

  – The unique identifier issued by the *Service Provider* to the *Subject* is 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: is the unique identifier of the *Service Provider*),
    * "x" is the inner identifier used by the *Service Provider*,
    * "y" is the inner identifier used by the *Service Provider*,
    * "z" is an automatically issued, a unique identifier within a specific "x.y" value pair.

    So the "x.y.z" value set is the unique identifier of the *Subject* within the system of the *Service Provider*.

    Because the first part of the identifier identifies the *Service Provider* globally, and the rest of the identifier specifies the *Subject* within the system of the *Service 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 IETF RFC 4043 [23] recommendation if the *Certificate* "Subject Alternative Names" field contains the "assigner" but not the "identifierValue" according to IETF RFC 4043 recommendation.

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

    The *Service 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* may contain further Serial Number fields.

    The identifier may be given in a format
    * specified in the ETSI EN 319 412-1 section 5.1.3 (for example: "TINHU-8123456790"),
    * in (Name:Value) format (for example: "ID card number:AAAAAA"), or
    * in other format requested by the *Client*s.

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

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

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

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

  In case of *Codesigning Certificate* issued to a natural person the field is mandatory, the *Service Provider* writes here the name of the natural person.

  In case of other *Certificate* issued to a natural person the field is not filled out.

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

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

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

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

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

  Filling out this field is mandatory in case the *Subject* is a legal person.

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

  If the *Subject* is a legal person and the *Client* requests the inclusion of the *Subject*'s data regarding the Payment Services EU Directive (PSD2) [2] in the *Certificate*, then this field contains either an identifier consisting of the authorization number of the *Subject* issued by the national competent authority (NCA) supervising the payment services of the *Subject*, the abbreviation of the NCA and the two character ISO 3166 country code of the NCA, structured as defined in the ETSI TS 119 495 specification [18], or another registration identifier recognized by the NCA, structured as defined in the ETSI EN 319 412-1 [13] specification.

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

  In case of an *Organizational Certificate* the name of the organizational unit related to the organization named in the "O" field, or the trademark, or other information may be in this field.

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

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

  Optional field.

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

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

  In case of an *Organizational Certificate* the two-letter country code - according to ISO 3166-1 [19] - of the place of incorporation of the *Organization* indicated in the "O" field.

In case of a natural person *Subject* not related to an *Organization* the two-letter country code - according to ISO 3166-1 [19] - of the country which issued the document used for the identification of the *Subject*.

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 Certificate* it is filled out based on the official document presented by the Represented Organization indicated in the "O" field.

  In case of *Certificate for Profession* it is filled out based on the official document presented by an Organization independent of the *Subject*.

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

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

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

  Filling is optional.

  If filled, it is the same as the email 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 " ").

Extensions

- Subject Alternative Names - "Subject Alternative Names"

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

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

  The *Service 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 *Service Provider* to use that alternative name in the Subject Alternative Names field.

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

  The *Service Provider* also verifies the content to be in the "Subject Alternative Names" field, and decides on the names on an individual basis. A decision will be made on the basis whether it is proven that the *Organization* in question uses the name requested by the *Client* legally.

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

  – Furthermore the IETF RFC 4043 [23] "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 *Service Provider* is indicated. Then according to the IETF RFC 4043 recommendation, this "assigner" OID together with the first "Serial Number" value – containing the OID allocated by the *Service 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:

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

- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  The name of the *Service Provider* in English without accents.
- Organization Identifier (OrgId) – OID: 2.5.4.97
  Filling out is optional.
- Organizational Unit (OU) – OID: 2.5.4.11
  "e-Szigno CA"
  The name of the *Service Provider* organization unit's name without accents.
  It was filled in the SHA-1 based provider *Certificate*s, but it is not filled in the SHA-256 based provider *Certificate*s.
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  City of the seat of the *Service Provider* without accents.
- CountryName (C) – OID: 2.5.4.6
  "HU"
  Two letter code of the country of the seat of the *Service Provider*.
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  "info@e-szigno.hu"
  Filling out is optional.

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

The Alternate Names of the Certificate Issuer Certification Unit

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

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

3.1.2 Need for Names to be Meaningful

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

- the identifier shall be meaningful;
- the personal name in the *Certificate* shall be indicated the same way as verified by the *Service Provider* according to the section 3.2.3.
- the name of the *Organization* in the *Certificate* shall be indicated the same way as verified by the *Service Provider* according to the section 3.2.2.

3.1.3 Anonymity or Pseudonymity of Subscribers

The *Service Provider* doesn't issue *Certificate* with pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

In order to interpret the identifiers it is recommended for the *Relying Parties* to act as described in this document. If the *Relying Party* is in need for help related to the interpretation of the identifier or any other data indicated in the *Certificate*, it can contact directly the *Service Provider*. In such case, the *Service Provider* shall not give any further information on the *Client* than indicated in the *Certificate*, – provided that the law does not require it – only provides the information to help interpret the indicated data.

3.1.5 Uniqueness of Names

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

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

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

Procedures to Resolve Disputes Relating the Names

The *Service Provider* ensures that the *Client* is entitled to use the indicated names. The *Service Provider* is entitled to revoke the *Certificate* in question for the illegal use of the name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

In the fields of the end-user *Certificate* required by the *Subscriber* trade marks may occur. The *Service 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 trade mark indication, then the *Client* shall provide evidence of the legitimacy of its use. The *Service Provider* verifies the provided evidences before the issuance of the *Certificate* based on the following web page operated by the European Union Intellectual Property Office:

`https://www.tmdn.org/tmview/welcome`

The trade mark or brand name may be included in the *Certificate* only if:

- the trade mark or brand name is registered by the organization of the *Applicant*;
- the *Applicant* has the consent to use the trade mark or brand name issued by the registrant.

The trade mark or brand name may be included in the *Certificate* the following ways:

- in the field "O", in this case the trade mark or brand name is followed by the official - shortened as appropriate - name of the organization in parenthesis. In this case the *Applicant* may request the indication of the proper (C), (R) or (TM) mark in the *Certificate* after the trade mark or brand name;
- in the field "OU", in this case the trade mark or brand name is always followed by the proper (C), (R) or (TM) mark.

Any of the (C), (R) or (TM) marks may only be included in the *Certificate* in case of proper use of the trade mark or business name immediately following it.

The *Service 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 *Service Provider* can use any communication channel within the limits provided by law, for the verification of the identity of the person or organization requesting the *Certificate*, and for checking the authenticity of the data provided.

The *Service Provider* may refuse the issuance of the required *Certificate* at its sole discretion, without any apparent justification.

3.2.1 Method to Prove Possession of Private Key

Prior to the issuance of a *Certificate* the *Service 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 *Service Provider* generates within its organization the private key belonging to the *Certificate* of the *Subject* – typically on *Cryptographic Hardware Device* 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 *Service 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.

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.

Prior to the issuance of an *Organizational Certificate* the *Service Provider* verifies the organizational data authenticity to be included on the *Certificate* based on authentic public registers.
Furthermore it is verified in these cases, that:

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

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

- the official denomination, registered office and legal status of the *Organization*,
- official registration number of the *Organization* (e.g. company registration number, tax identification number), if applicable;
- the name of the organization unit within the *Organization*, if its indication in the *Certificate* is requested,
- 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.
- If the *Subject* is a legal person and the *Client* requests the inclusion of the *Subject*'s data regarding the Payment Services EU Directive (PSD2) [2] in the *Certificate*, then the *Client* shall give the authorization number of the *Subject* issued by the national competent authority (NCA) supervising the payment services of the *Subject* or another registration identifier of the *Subject* recognized by the NCA, the type of the payment service(s) and the name of the NCA.

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

- the statement with the application submitter's manual signature on that, justifying 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];

[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.

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

Identity validation of foreign Organizations

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

In respect of data verification, the *Service 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.

The *Service 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 *Service Provider* is the *Client*ś responsibility.

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

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

The *Service 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.

The *Service Provider* verifies the identity of the natural person applying one of the following methods.

[4] In case of Court of Registration registered firms the above documents can be acquired by the *Service Provider*.
[5] In case of Court of Registration registered firms the above documents can be acquired by the *Service Provider*.

1. During face to face identity validation.

   In case of *Certificate*s belonging to the III. certification policy:

   - the natural person shall appear in person at the officier of the *Registration Authority* or a state notary 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 identification can be based on the following official documents:

     – in case of natural persons within the scope of Act LXVI. of 1992. (henceforth: Nytv. [4]) official cards appropriate for verifying identity defined in Nytv. in accordance with Eüt. 82.§ (3) [9];
     – in case of natural persons outside the scope of Nytv. [4] on the basis of a travel document defined in the Act on the entry and residence of persons enjoying the right of free movement and residence or the law on entry and residence of third-country nationals [6] in accordance with Eüt. 82.§ (4) [9];
     – in case of abroad identification of natural persons who have none of the documents mentioned above the *Service Provider* applies personal identity verification in accordance with Eüt. 82.§ (5) [9] only in the case of identifying European citizens. In such case a personal identity card with a photo issued by the European country of natural person's nationality is accepted as a trusted document for identity verification.
   - the natural person shall declare the correctness of the personal identification data used for the identity validation with a written statement signed with a handwritten signature in the presence of the identification person; ;
   - the *Service Provider* verifies, whether any alteration or counterfeiting happened to the presented identity cards.

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

   - there's no need for personal meeting for the identification of the person, in such cases the *Service Provider* can identify the *Applicant* remotely;
   - the *Applicant* sends a copy of one of its official identity cards suitable for identity verification to the *Service Provider*.
   - 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 *Applicant* can prove its identity at its own discretion according to the III. certification class.

Further rules for the identity validation of foreign citizens

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

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

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

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

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

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

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

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

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

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

   - The *Applicant* submits the *Certificate Application* in electronic format with an electronic signature based on a non-pseudonymous *Certificate* with a security classification not lower than the requested *Certificate* (see section 1.2.3.).
   - The electronically signed *Certificate Application* shall contain the data needed for the definit identification of the natural person.
   - The authenticity and confidentiality of the *Certificate Application* shall be verified on the whole certification chain.
   - The *Service Provider* may accept only those electronic signatures, which are based on a *Certificate* issued by a Trust Service Provider according to a Trust Service which is listed on the Trusted List of one of the EU member states and was valid at the time of the signature creation.
   - The *Service Provider* may accept only those electronic signatures, which are based on such a *Certificate* which was issued in compliance with the paragraph (1) point (a) or (b) of Article 24 of the eIDAS regulation [1].

The *Service Provider* uses the data reconciled during a previous identification procedure, if the *Applicant* requests new *Certificate* instead of an expired or a revoked one, or if he requests a

new *Certificate* besides the existing one during the validity period of the service agreement. The authenticity of the *Certificate* application, the accuracy of the data to be in the *Certificate* and the identity of the person submitting the application shall also be checked.

The *Service 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 *Service Provider* which has been verified by the *Service Provider*.

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 *Organizational Administrator* appointed by an authorized person to represent the *Organization*.

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

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

3.2.6 Criteria for Interoperation

The *Service 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 *Service Provider* issues a *Certificate* to a *Subject* with a replaced public key. Re-key can only be requested during the validity period of the service agreement.

In case of a re-key request, the *Service Provider* verifies the existence and validity of the affected *Certificate*.

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

In case of the certificates belonging to the II. certification class, the *Service Provider* does not perform re-key. Issuing new key container *Certificate* only takes place within the framework of a new *Certificate* application process.

3.3.1 Identification and Authentication for valid Certificate

For the submission of the re-key applications, the *Service Provider* ensures the following options:

- on paper signed manually by the *Applicant* at the customer service of the *Service Provider* or to the mobile registration associate of the *Service Provider* on a date previously agreed,
- in electronic form with an electronic signature of the *Applicant* based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be renewed (see section 1.2.3.);
- 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.

In case of certificates belonging to the III. certification class if the renewal request is submitted on paper by post, the certificate is issued after the validation of the request. To validate the request the *Service Provider* uses a verified method of communication. The *Service Provider* for example may apply phone call in order to identify the applicant and verify the application.

In case re-key is necessary because the private key belonging to the *Certificate* became compromised, the *Service 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 invalid Certificate

The *Service Provider* accepts re-key requests – only during the validity period of the service agreement– in case of *Certificate*s suspended, revoked or expired. 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 3.3.1, 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 *Service Provider* issues a certificate with unchanged *Subject* identification information but for new validity period to a *Subject*. *Certificate* renewal can only be requested during the validity period of the service agreement and for valid *Certificate*s.

3.4.1 Identification and Authentication in Case of a Valid Certificate

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

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

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

In case of a *Certificate* application according to the aforementioned, signed with an electronic signature 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 in case of the renewal of certificates belonging to the III. certification class the handwritten signature on the request will be compared with the signature specimen available at the *Service Provider* and the *Service Provider* valiudates the request by using a Verified Method of Communication.

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 *Service Provider* issues a new *Certificate* to the *Subject* with an unchanged public key, but with different *Subject* identification data.

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

3.5.1 Identification and Authentication in Case of a Valid Certificate

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

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

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

In case of a *Certificate* application according to the aforementioned, signed with an electronic signature, 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 in case of the modification of certificates belonging to the III. certification class the handwritten signature on the request will be compared with the signature specimen available at the *Service Provider* and the *Service Provider* valiudates the request by using a Verified Method of Communication.

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 *Service 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 *Service 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. .

3.7 Verified Method of Communication

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

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

- verifies that the Verified Method of Communication belongs to the *Applicant* based on
  - records provided by the applicable phone company;
  - a Qualified Government Information Source;
  - a Verified Professional Letter issued by a notary;
  - the physical presence of the *Applicant*.
- confirms the Verified Method of Communication. The registration officier of the *Service Provider* contacts the *Applicant* by using the Verified Method of Communication. The reliability of the Verified Method of Communication is proved by physical presence of the *Applicant* or by using a communication channel password.

4 Certificate Life-Cycle Operational Requirements

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

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

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

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

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

4.1 Application for a Certificate

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

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

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

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

A new *Certificate* can be requested within the confines of a previously concluded service agreement. If the *Certificate* (*Certificate* replacement) is issued as a replacement of a *Certificate* indicated in

the service agreement, it is not necessary to modify the service agreement. If the *Client* requests a new *Certificate* in addition to the extant ones, the service agreement shall be modified.

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

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

The *Service 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, email 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, email 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 *Service Provider* ask for and check at least the following documents, certifications, procurations and declarations (in case of remote identification the copies of these):

- documents necessary to identify the *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 *Applicant* 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 *Applicant* 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. In case of *Organizational Certificate* representatives may only be natural persons according to section 3.2.5. *Certificate Application* submitted by any other person is refused automatically.

The precondition of *Certificate* issuance is a valid service agreement (signed by the *Subscriber* and the *Service 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 at the customer service of the *Service Provider* or to the mobile registration associate of the *Service Provider*, on a date previously agreed;
- on paper sent by post to the postal address of the *Service Provider* (then, in case of *Certificate*s belonging to the III. certification class 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 *Service Provider*'s email 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 *Service Provider* 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 *Service Provider* identifies the *Organization* (see section: 3.2.2.) and it ensures, that the *Applicant* is entitled to represent the *Organization* (see section: 3.2.5.) and to request a *Certificate* related to the *Organization* (see section: 3.2.2.).

The *Subscriber* determines which *Applicant* 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.

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

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

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

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

The *Service 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 *Service Provider* records and processes the data provided in the application;
- the decision about the disclosure of the *Certificate*;
- a statement that there's no brand name or trademark indicated in the requested *Certificate*, or it is indicated and the applicant is entitled to use that.

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

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

If the identity of the *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 in the *Certificate Application* is incorrect, then the *Service Provider* gives the *Client* the opportunity to correct the missing or incorrect data, and to provide the missing attestations within 3 months from the submission of the *Certificate Application* according to its inner regulations.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The *Service Provider* identifies the *Applicant* 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 *Service Provider* registers all the information used by the *Subject* or in case of an Organizational Certificate the *Organization* to certify its identity, including the registration number of the documentation used for the certification and the incidental limitations related to its validity.

4.2.2 Approval or Rejection of Certificate Applications

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

The *Service 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 email address, the *Service Provider* verifies the email address to be indicated in the *Certificate*. It ascertains that the email address exists and verifies that it is the *Subject*'s email address indeed.

The *Service 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 *Service Provider*, then the *Service Provider* rejects the application.

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

4.2.3 Time to Process Certificate Applications

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

4.3 Certificate Issuance

The *Service Provider* only issues the *Certificate* to the *Subject* in case of certificates belonging to the III. certification class, 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 *Service 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 security 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 *Applicant* 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 *Applicant* matches the one on his/her ID card, and the Signature of the *Applicant* fits the one appears on the ID card.

Along with the takeover of the *Electronic Signature Creation Device*, the *Applicant* receives the activation codes necessary for activation, generated according to section 6.4.

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

4.3.1 CA Actions During Certificate Issuance

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

The *Service 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 *Applicant* and the *Subscriber* on the issuance of the *Certificate* and enables the *Applicant* to receive the *Certificate*.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

In case of *Certificate*s belonging to the III. certification class *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. The *Subject* or its representative verifies the reception of the *Certificate* by signing the statement.

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

If the *Service Provider* 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 *Applicant* shall sign manually a statement about takeover, in which – amongst others – he/she verifies that the data – which were the bases of the *Certificate* issuance – 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 receiving the confirmation of acceptance of the *Certificate* – if the *Applicant* consents – the *Service Provider* discloses the *Certificate* in its *Certificate Repository*.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The private key corresponding to the *Certificate* of the *Subject* can be only used according to according to section (6.1.7). the key usage of the *Certificate*, and any other usage is prohibited.

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

The *Subject* is bound to ensure the adequate protection of the private key and the activation data.

The limitations determined in Section 1.4. have to be followed during the usage.

4.5.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Service Provider*, in the course of performing tasks (e.g. identifying remote party, encrypt document for the recipient), 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*;
- public keys shall only be accepted in such applications that are in line with the content of the „Key Usage" and "Extended Key Usage" fields of the *Certificate*;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain;
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

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

4.6 Certificate Renewal

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

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

4.6.1 Circumstances for Certificate Renewal

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

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

If a previous *Certificate* of the *Subject* is revoked 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 *Applicant* is informed if the terms and conditions have changed since the previous *Certificate* issuance.

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

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

4.6.2 Who May Request Renewal

The Certificate renewal shall be initiated by a person 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 *Service Provider* is entitled to initiate the renewal of the *Certificate* if the service signatory key used for the issuance of the *Certificate* shall be replaced out of turn.

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

- on paper signed manually at the customer service of the *Service Provider* or to the mobile registration associate of the *Service Provider*, on a date previously agreed;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be 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 *Service Provider* verifies that:

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the submitter of the *Certificate* renewal application stated that the data of the *Subject* to be indicated in the *Certificate* are unchanged and accurate;
- the *Certificate* renewal application was submitted during the *Certificate*'s validity period;
- the *Certificate* to be renewed is not 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 *Service Provider* informs the *Applicant* 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 *Service 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 *Service Provider* discloses the renewed *Certificate* the same way as the original *Certificate*.

4.6.7 Notification of Other Entities about the Certificate Issuance

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

4.7 Certificate Re-Key

Re-key means the process when the *Service Provider* issues a new *Certificate* for the *Subject* in a way that the public key is to be changed.

Further data may be optionally changed in the new *Certificate* issued during the *Re-key* process, for example validity period, the CRL and OCSP links or the provider key used to sign the *Certificate*.

In case of keys belonging to the II. certification class, the Certification Authority does not perform *Re-key*. The issuance of a *Certificate* with a new key is exclusively performed within the framework of new Certificate application.

4.7.1 Circumstances for Certificate Re-Key

The validity of the previous *Certificate* is not required for *Re-key*, but the *Service Provider* shall only accept *Re-key* applications within the scope of the service agreement.

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

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

4.7.2 Who May Request Certification of a New Public Key

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

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

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

- on paper signed manually at the customer service of the *Service Provider* or to the mobile registration associate of the *Service Provider*, on a date previously agreed;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be 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 *Service Provider* verifies that:

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

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

4.7.4 Notification of the Client about the New Certificate Issuance

The *Service Provider* informs the *Applicant* 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 *Applicant* takes place in in a controlled environment while in accordance with the security regulations defined in section 6.1.2. The *Subject* (in case of non-natural person *Subject*, its representative) can take over the *Electronic Signature Creation 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 *Applicant* matches the one on his/her ID card, and the Signature of the *Applicant* fits the one appears on the ID card.

Along with the takeover of the *Electronic Signature Creation Device*, the *Applicant* 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 verify that the envelope hasn't been opened. The *Applicant* shall sign a statement manually about the takeover, in which – amongst others – it verifies that the data – which were the bases of the *Certificate* issuance – 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 it without any additional declaration.

4.7.6 Publication of the Re-Keyed Certificate

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

4.7.7 Notification of Other Entities about the Certificate Issuance

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

4.8 Certificate Modification

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

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

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

4.8.1 Circumstances for Certificate Modification

Certificate modification becomes necessary in the following cases:

- change of data indicated in the *Subject*'s *Certificate*;
- in the *Certificate* issuing system of the *Service Provider* any data of the *Certificate* issuer CA indicated in the "Subject DN" is changed, or its public key is changed and as a result of it, its provider *Certificate* is changed;
- the *Certificate* profile determined by the *Service Provider* is changed.

Requirements of *Certificate* modification:

- the *Certificate* modification application was submitted during the *Certificate*'s validity period;
- the *Certificate* to be modified is not suspended or revoked;
- the private key corresponding to the *Certificate* is not compromised.

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

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

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

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

4.8.2 Who May Request Certificate Modification

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

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

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

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

- on paper signed manually at the customer service of the *Service Provider* or to the mobile registration associate of the *Service Provider*, on a date previously agreed;
- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be 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 *Service Provider* verifies that:

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

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

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

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

4.8.4 Notification of the Client about the New Certificate Issuance

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

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

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

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.9 Certificate Revocation and Suspension

The process when the *Service Provider* terminates the validity of the *Certificate* before expiration is called *Certificate* revocation. The *Certificate* revocation is a permanent and irreversible status change, the revoked certificate will never be valid again.

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

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 suspension and revocation:

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

4.9.1 Circumstances for Revocation

Reasons for Revoking a Subscriber Certificate

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

- the *Applicant* or the *Subscriber* requests the revocation of the *Certificate* in writing;
- the *Applicant* or the *Subscriber* notifies *Certification Authority* that the *Certificate Application* is not approved and subsequently the approval is not given;
- the *Certification Authority* becomes aware that the private key corresponding to the public key in the *Certificate* has been compromised;
- the *Certification Authority* becomes aware that the public key in the Certificate does not comply with the requirements defined in Section 6.1.5. and 6.1.6.;
- the *Certification Authority* becomes aware that the certificate was misused;
- the *Service Provider* is made aware that a *Subscriber* has violated one or more of its material obligations under the service agreement or General Terms and Conditions;
- the *Certification Authority* is made aware of a material change in the information contained in the *Certificate*;
- the *Certificate* modification because of data change referring to the *Subject*;
- the *Certification Authority* becomes aware that the *Certificate* was not issued according to the related *Certificate Policy* or the *Certification Practice Statement*;
- the *Certification Authority* becomes aware that any of the data appearing in the *Certificate* is inaccurate;
- the *Certification Authority* is no longer entitled to issue *Certificate*s, and maintenance is not provided for the existing CRL and OCSP services;
- the revocation is required by the *Certification Authority*'s *Certificate Policy* or the *Certification Practice Statement*;
- the *Certification Authority* issued the *Certificate* based on a document from a third party, and it withdraws that document in writing;

- the format and technical content of the *Certificate* presents an unacceptable risk to the *Relying Parties* (for example, if the used cryptographic algorithm or key size is no longer secure);
- the *Certification Authority* becomes aware that the private key of the *Certificate* issuer certification unit might be compromised;
- the *Certification Authority* becomes aware that the *Subscriber* failed to fulfil any of its financial obligations according to the service agreement;
- the *Certificate* was suspended, and was not reinstated during the ensured time period (see section: 4.9.16.);
- the termination of service agreement;
- the *Certification Authority* has terminated its activities;
- the law makes revocation mandatory.

Reasons for Revoking a Subordinate CA Certificate

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

- the CA operating the intermediate certification unit requests the revocation of the *Certificate* in writing;
- the Subordinate CA notifies the *Service Provider* that the original *Certificate Application* was not authorized and does not retroactively grant authorization;
- the *Certification Authority* becomes aware that it is not in the exclusive possession of the private key;
- the *Certification Authority* becomes aware that the public key in the *Certificate* does not comply with the requirements defined in Section 6.1.5 and 6.1.6. ;
- the *Certification Authority* becomes aware that the *Certificate* was misused;
- the *Certificate* was not issued according to the relevant *Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit does not comply with the relevant *Certificate Policy* or *Certification Practice Statement*;
- the *Certification Authority* determines that any of the information appearing in the *Certificate* is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another *Certification Authority* to provide revocation support for the *Certificate*;
- *Certification Authority* is no longer entitled to issue *Certificate*s, and maintenance is not provided for the CRL and OCSP services related to the *Certificate*s ;

- the revocation is required by the Issuing CA's *Certificate Policy* or the *Certification Practice Statement*;
- *Certificate* modification because of data change relating to the certification unit or *Certification Authority*;
- the format and technical content of the *Certificate* presents an unacceptable risk to the *Relying Parties* (for example, if the used cryptographic algorithm or key size is no longer secure);
- the *Certification Authority* has terminated its activities;
- the law makes the revocation mandatory.

Reasons for Revoking a Subordinate CA Certificate operated by another CA

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

- the CA operating the intermediate certification unit requests the revocation of the *Certificate* in writing;
- the Subordinate CA notifies the *Service Provider* that the original *Certificate Application* was not authorized and does not retroactively grant authorization;
- the issuer *Certification Authority* becomes aware that the operator of the intermediate certification unit is not in the exclusive possession of the private key;
- the issuer *Certification Authority* becomes aware that the public key in the *Certificate* does not anymore comply with the requirements defined in Section 6.1.5 and 6.1.6. ;
- the *Certification Authority* becomes aware that the *Certificate* was misused;
- the issuer *Certification Authority* becomes aware that the *Certificate* is not issued according to the related *Certificate Policy* and the *Certification Practice Statement* or the operation of the intermediate certification unit operator does not comply with the relevant *Certificate Policy* or *Certification Practice Statement*;
- the *Certification Authority*
  determines that any of the information appearing in the *Certificate* is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another *Certification Authority* to provide revocation support for the *Certificate*;
- the *Certification Authority* is no longer entitled to issue *Certificate*s, and maintenance of the CRL and OCSP services for the existing *Certificate*s is not provided;
- the revocation is required by the Issuing CA's *Certificate Policy* or the *Certification Practice Statement*;

- *Certificate* modification because of data change relating to the certification unit or the other *Certification Authority*;
- if *Certification Authority* issued the *Certificate* based on a document from a third party, and that third party withdraws the document in writing;
- the format and technical content of the *Certificate* presents an unacceptable risk to the Relying parties (for example, if the used cryptographic algorithm and key size is no longer safe);
- the *Certification Authority* operating the certification unit or the issuer *Certification Authority* of its *Certificate* has terminated its activities;
- the law makes the revocation mandatory.

4.9.2 Who Can Request Revocation

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

- the *Subscriber*;
- the *Applicant*;
- in case of *Organizational Certificate*, the *Organization*'s authorized representative;
- the contact person specified in the service agreement; *Organizational Administrator* appointed by the *Subscriber*;
- the supervisory authority which issued the payment service licence for the *Subject*, if the *Certificate* contains the *Subject*'s data regarding the Payment Services EU Directive (PSD2) [2];
- the *Service Provider*.

4.9.3 Procedure for Revocation Request

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

- in an electronic form with an electronic signature based on the non-pseudonymous *Certificate* with a security classification not lower than the *Certificate* to be revoked (see section 1.2.3.);
- on paper signed manually at the customer service of the *Service Provider* during office hours in person, or sent by post.
- through the website of the *Service Provider* 24 hours a day.

  The IT system of the *Service Provider* processes the applications submitted through its website immediately, the site informs the application submitter about the results of the evaluation.

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

In case of Certificate application signed with a valid 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 *Service 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 *Service 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 *Service Provider* ensures a possibility during the revocation process, to request a new *Certificate* in the framework of *Re-key* to replace the *Certificate* to be revoked. The rules for *Re-key* are in section 4.7.

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

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

The requester shall provide particularly the following information:

- the exact denomination of the *Subject*;
- the *Certificate*'s unique identifier;
- the requested date of the revocation, if the revocation shall not happen immediately;
- identification data of the *Client*.

In case of invalid or incomplete application the *Service Provider* rejects the application. The *Service Provider* notifies the *Subject* and the *Subscriber* about the fact and reason of the rejection by email.

In case of complete and valid application the *Service Provider* makes a decision about the acceptence of the application. Depending on the content of the application the *Service Provider* revokes the *Certificate* immediately or sets up the date of revocation according to the request.

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

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

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/tanusitvany-felfuggesztese-es-visszavonasa.html`

High-Priority Certificate Problem Report

The *Service Provider* maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a *Certificate* that is the subject of such a complaint.

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

`HighPriorityCertificateProblemReport@e-szigno.hu`

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

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

4.9.4 Revocation Request Grace Period

The *Service Provider* does not apply grace period during the fulfilment of revocation requests.

4.9.5 Time Within Which CA Must Process the Revocation Request

The *Service Provider* processes the revocation requests within 24 hours following the arrival of the request.

In case of applications submitted in person, the time of arrival is when the customer service officier of the *Service Provider* receives the application.

In case of applications sent by post, the time of arrival is when the mail arrives to the *Service Provider* at office hours.

In case of applications sent by electronic mail, the time of arrival is when the email is received to the dedicated email address `revocation@e-szigno.hu` on the server of the *Service Provider*. Emails arriving out of office hours are considered as arrived at the beginning of the next business day.

The *Service 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 *Service Provider* – or via other channels, the *Service 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 *Service Provider*, the *Service Provider* recommends to the *Client* to suspend the *Certificate* until the revocation by using the SMS based suspension service (see section 4.9.13). It is sufficient to take care of the revocation of the suspended certificates later, and the *Service 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 *Service Provider*, prior to the adoption and use of the information indicated in the *Certificate*, it is necessary for *Relying Parties* to act with proper carefulness. It is particularly recommended for them to verify all of the *Certificate*s located in the *Certificate* chain according to the relevant technical standards. The verification should cover the verification of the *Certificate*s' validity, the policy requirements and key usage, and the checking of the referenced CRL or OCSP based revocation information.

4.9.7 CRL Issuance Frequency

The *Service Provider* issues a new *Certificate Revocation List* for its end user *Certificate*s at least once a day.

The validity of these *Certificate Revocation List*s

is 25 hours.

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online Revocation/Status Checking Availability

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

4.9.10 Online Revocation Checking Requirements

The online *Certificate* status service complies with the requirements of Section 4.10 .
Certification Authority provides OCSP service through GET method.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.13 Circumstances for Suspension

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 *Service Provider* ensures opportunity for suspension initiation:

- via its webpage;
- by sending a fixed-format SMS text message;
- the same way as submitting the revocation requests.

Suspension via Web

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

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

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

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

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

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

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

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

Suspension by sending a fixed-format SMS text message

The *Client*s of the *Service Provider* may indicate in an SMS text message sent to the *Service Provider*'s suspension phone number if a Qualified Electronic Signature Creation Device or a private key is possessed by an unauthorized person.

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

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

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

Examples of formally correct suspension request:

- "1976-11-04 a1b2c3d4"
- "2.1.134 pacsirta"

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

Suspension the Same Way as Revocation Request Submission

The *Service 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 *Service 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 email 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 *Service Provider* assumes that the reason is private key compromise.

If the *Client* asks for the suspension because of key compromise, then the *Service 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

If the suspension of the *Certificate* was requested by the *Client*, the *Client* may request the reinstatement of the *Certificate* within 5 working day after the suspension. If the reinstatement of the *Certificate* is not requsted within this interval the *Service Provider* revokes the *Certificate*.

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

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

In case of a successful *Certificate* reinstatement, the *Service Provider* notifies the *Subject* and the *Subscriber* by email of the fact.

4.10 Certificate Status Services

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

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

In case of *Codesigning Certificate*s the *Service Provider* guaranties the availability of the OCSP based revocation information beyond the *Codesigning Certificate*'s expiration date for at least 10 years.

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

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

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

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

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

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

4.10.1 Operational Characteristics

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

- The productive (not root) SHA-256 based certification units operated within the system of the *Service Provider* issue CRL within 60 minutes after the revocation status change of any *Certificate* issued by the given certification unit, but at least once in every 24 hours.
- The "Microsec e-Szigno Root CA 2009" root certification unit issues a CRL once in at the most of 24 hours.
- The "e-Szigno Root CA 2017" root certification unit issues a CRL once in at the most of 24 hours.
- The productive (not root) ECC based certification units operated within the system of the *Service Provider* issue CRL within 60 minutes after the revocation status change of any *Certificate* issued by the given certification unit, but at least once in every 24 hours.

The validity period of the *Certificate Revocation List* is 25 hours. The all-time current *Certificate Revocation List*s for the specific *Certificate*s can be reached at the following address:

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

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

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

Online Certificate Status Protocol (OCSP)

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

In respect of the *Certificate* based on SHA-256, the *Service Provider* provides OCSP service according to the IETF RFC 6960 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the *Certificate*s issued by the certification unit (section 1.3.1.).

The *Service 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 *Service 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 *Service 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 *Service Provider* for the query date.

Public and Free OCSP Service

- This version of the OCSP service is publicly and freely available, any *Relying Party* can avail itself of it same as the *Certificate Revocation List*s. There is no need for authentication at query.
- This version of the OCSP service can be reached through the URLs indicated on the *Certificate*s.
- Based on the IETF RFC 6960 "Response Pre-production" process, the issued OCSP response can be created before the query and does not necessarily contain the nonce element. The *Service Provider* can give the same response for multiple queries. The "thisUpdate" and "producedAt" time values are identical, but these can precede the time of the query.
- The "nextUpdate" indicated in the response is either not filled, or contains a time value not later than the responder certification expiration time.
- The "thisUpdate" value indicated in the issued OCSP response is never older than 24 hours, because the *Service Provider* creates a new OCSP response at least in every 24 hours.

- The time difference between the "nextUpdate" and "thisUpdate" values in the issued OCSP response is never greater than 10 days.
- The OCSP responses always contain the current information listed in the revocation registry of the *Service 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 *Service Provider* ensures the aforementioned two versions of the OSCP services with the same availability.

4.10.2 Service Availability

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

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

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

4.10.3 Optional Features

The *Service Provider* provides various (CRL and two types of OCSP) services according to the descriptions in this section, in the framework of *Client*s and *Relying Parties* can verify the

revocation status of the *Certificate*s issued by the *Service Provider*. Besides these, the *Service 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 *Service Provider* revokes the end-user *Certificate*s in case of the termination of the contract concluded with the *Subscriber*.

4.12 Key Escrow and Recovery

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

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Symmetric Encryption Key Encapsulation and Recovery Policy and Practices

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

5 Facility, Management, and Operational Controls

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

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

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

5.1 Physical Controls

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

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

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

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

In order to provide adequate security:

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

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

Service Provider ensures that:

- each entry to the *Data Centre* is registered;
- only authorized staff members with trusted roles with the right permissions can entry to the computer room individually;
- persons without independent authorization can only stay in the *Data Centre* in justified cases, for the time required and accompanied by personnel with appropriate rights;
- the entry logs shall be archived continuously and evaluated weekly.

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

In the presence of unauthorized persons:

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

When leaving the computer room the administrator shall verify that:

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

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

5.1.3 Power and Air Conditioning

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

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

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

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

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

5.1.6 Media Storage

The *Service Provider* protects its media storages from unauthorized access and accidental damage. All audit and archive data is created in duplicate. The two copies are stored 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 *Service 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 *Service Provider* ensures the environmental standards compliant disposal of the superfluous assets, and media.

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

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

5.1.8 Off-Site Backup

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

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

5.2 Procedural Controls

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

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

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

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

5.2.1 Trusted Roles

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

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

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

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

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

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

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

Official active in the field of personalization: The individual, whose task is the Certificate application compilation;

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

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

Up to date records are kept by the *Service Provider* of the trusted roles.

5.2.2 Number of Persons Required per Task

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

- the generation of the *Service Provider*'s own service key pair;
- the backup of the provider's private key;
- the activation of the provider's private key;
- the destruction of the provider's private key.

At least one of the persons performing the procedures listed above shall be a system administrator, and the other person shall not be the independent system auditor.

During the implementation of the operations listed, unauthorized person shall not be present in the room.

5.2.3 Identification and Authentication for Each Role

The users managing the IT system of the *Service Provider* have unique identification data, enabling secure identification and authentication of the users.

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

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

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

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

5.2.4 Roles Requiring Separation of Duties

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

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

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

5.3 Personnel Controls

The *Service Provider* takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the *Service Provider*'s operation. The objective of precautions applicable to personnel is to reduce the risk of human errors, theft, fraud and cases of misuse.

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

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

Trusted roles can be held at the *Service Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Service Provider*. All personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the the *Service Provider*'s operations.

The manager with overall responsibility for the IT system can only be a person who has:

- specialized degree (mathematics, physics college or university degree or a college/university degree acquired at an engineering department belonging to the technical field of science);
- at least three years of expertise in professional working experience related to information security.

5.3.2 Background Check Procedures

The *Service Provider* only hires employees for trusted or leading roles, who

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

At the time of the appointment, shall the leading role holder *Service Provider* employee with a statement, a trusted role holder employee with a certificate of good conduct less than 3 months old justify the clean criminal record.

The *Service Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process, like previous employment, professional references, most relevant educational qualifications.

5.3.3 Training Requirements

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

- basic PKI knowledge;
- the specifics and the way of handling the *Service Provider*'s IT system;
- the necessary special knowledge for fulfilling their scope of activities;
- processes and procedures defined in the public and inner regulations of the *Service Provider*;
- the legal consequences of the individual activities;
- the applicable IT security regulations to the extent necessary to the specific scope of activities;
- the data protection rules.

The *Service Provider* trains the employees concerned with registration about the dangers and risks related to the verification of the data to be indicated on the Certificate.

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

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

5.3.4 Retraining Frequency and Requirements

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

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

The training material is updated at least in every 12 months and contains the new threats and actual security practices.

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

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

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

5.3.7 Independent Contractor Requirements

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

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

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

5.3.8 Documentation Supplied to Personnel

The *Service Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.
Each employee in trusted role receives the following documents in writing:

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

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

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

- the time of the event;
- the type of the event;
- the 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 *Service Provider*'s operation.
The *Service Provider* logs The following events at minimum:

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- LOGGING:

  - the shutdown, restart of the logging system or some of its components;
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
  - the modification or deletion of the stored logging data;
  - the activities performed because of the logging system's failure.

- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles;
  - in case of password based authentication:
    * the change of the number of permitted unsuccessful attempts;
    * reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
    * readmission of the user blocked because of the unsuccessful login attempts;
  - changing the authentication technique (for example from password based to PKI based).

- KEY MANAGEMENT:
  - all events for the entire life cycle of service keys (key generation, 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 *Service Provider*.

- CERTIFICATE MANAGEMENT:
  - every event related to the issuance and the status change of the provider *Certificate*s.
  - every request including *Certificate* issuance, re-key, key renewal , suspension and revocation;
  - events related to the request processing;
  - every verification activity performed related to the *Certificate* issuance.
  - refusal of the certificate applications;
  - *Certificate* issuance or status change.

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

- CA CONFIGURATION:
  - re-parameterization , any change of the settings of any component, of the CA;
  - user admission, deletion;
  - changing the user roles, rights;
  - changing the Certificate profile;

  - changing the CRL profile;
  - generation of a new CRL list;
  - generation of an OCSP response;
  - *Time Stamp* generation;
  - exceeding the required time accuracy threshold.

- HSM:
  - installing an HSM;
  - removing an HSM;
  - disposing, destructing an HSM;
  - delivering HSM;
  - clearing (resetting) an HSM;
  - uploading keys, certificates to the HSM.

- CONFIGURATION CHANGE:
  - hardware;
  - software;
  - operating system;
  - patch;

- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the CA components;
  - access to a CA system component;
  - a known or suspected breach of physical security;
  - firewall or router traffic.

- OPERATIONAL ANOMALIES:
  - system crash, hardware failure;
  - software failures;
  - software integrity validation error;
  - incorrect or wrongly addressed messages;
  - network attacks, attack attempts;
  - equipment failure;
  - electric power malfunctions;
  - uninterruptible power supply error;
  - an essential network service access error;
  - violation of the *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 *Service Provider* evaluates the generated log files every working day.

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

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

The 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 *Service Provider* for the amount of time defined in Section 5.5.2.

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

5.4.4 Protection of Audit Log

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

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

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

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

5.4.5 Audit Log Backup Procedures

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

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

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

5.4.6 Audit Collection System (Internal vs External)

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

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

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Service Provider* monitor the publicly available information about possible vulnerabilities and the new software patches. They analise the information, classify the vulnerability and if necessary inform the management about the result and propose an action plan to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat within a period of 48 hours after its discovery, but at least once a year the experts of the *Service Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access, and may affect the *Certificate* issuing process, or allow modification of the data stored in the *Certificate*.

Based on the results of the analysis the *Service Provider*

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis for the decision that the residual risk is accepted and the vulnerability does not require remediation.

At first the new software versions and software patches are installed on the test system of the *Service Provider* and only after the successfully finished test are installed on the live system which is used to provide the services.

The new software patches are not installed on the live system if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reasons for not applying any security patches are documented.

5.5 Records Archival

5.5.1 Types of Records Archived

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

The *Service Provider* archives the following types of information:

- every document related to the accreditation of the *Service Provider*;
- all issued versions of the *Certificate Policies* and *Certification Practice Statement*s;
- all issued versions of the Terms and Conditions;
- contracts related to the operation of the *Service Provider*;
- all information related to the registration, including:
  - every document handed in with the Certificate application;
  - the identification data of the document(s) presented during the personal identification;
  - service agreement(s);
  - other subscriber disclaimers;
  - the ID of the administrator assessing the registration application;
  - conditions and the results of the examination of the application;
- all information related to the Certificate for the whole life-cycle;
- every electronic and paper based log entry.

5.5.2 Retention Period for Archive

The *Service 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;

5.5.3 Protection of Archive

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

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

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

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

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

5.5.4 Archive Backup Procedures

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

After archiving the authentic electronic copies the *Service Provider* may destroy the original paper documents.

5.5.5 Requirements for Time-stamping of Records

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

The time value is given by the internal clock of the *Service Provider* which is synchronized to two separate Stratum-1 UTC time sources:

- one accurate time source uses the satellite-based GPS signal;
- the other accurate time source is based on the longwave time signal service (DCF77).

In order to provide accuracy the *Service Provider* synchronizes its own internal time with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization at least 4 times a day.

This way the *Service Provider* guarantees that the deviation of the time indicated in the time marks from the UTC time base is at most 1 second.

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

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

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *Service 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 *Service Provider* in an inner data storage operated by it.

5.5.7 Procedures to Obtain and Verify Archive Information

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

The archived files are protected from unauthorized access.

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

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

5.6 CA Key Changeover

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

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

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

5.7 Compromise and Disaster Recovery

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

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

Once the problem resolved, the event is reported – depending on the severity – within 24 hours to every organization, towards which such a requirement exists.

5.7.1 Incident and Compromise Handling Procedures

The *Service Provider* has a business continuity plan.

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

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

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

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

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

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

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

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

Once the problem resolved and the integrity restored, the *Service Provider* restarts its services as soon as possible.

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

5.7.3 Entity Private Key Compromise Procedures

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

In case another certificate authority also issued *Certificate* for the given certification unit - by law, contract or agreement between CAs based - and over or cross certified this certification unit of the *Service Provider*, the *Service Provider* promptly informs that other Certification Authority for that given key compromise and initiates the certificate revocation belonging to the key in question. In case of the key compromise of the intermediate CA issuing *Certificate*s for the public administration this means the notification of the KGYHSZ.

The *Service Provider* publishes a notice about the provider public key revocationaccording to the section 1.3.1

5.7.4 Business Continuity Capabilities After a Disaster

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

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

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

The *Service Provider* is obliged to notify the affected users as quickly as possible in the event of the disaster.

After the restoration of the services, the *Service Provider* restores its devices damaged during the disaster and the original service security level as quickly as possible

5.8 CA or RA Termination

The *Service 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 *Service Provider* shuts down the following services:

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

The *Service Provider* at least 20 days before the planned termination but at least 14 days after the notification of the *Client*s :

- revokes all valid enduser *Certificate*s;
- stop processing the revocation and suspension requests;
- terminates the regular issuance of the *Certificate Revocation List*s;
- issues a closing *Certificate Revocation List*.

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

- information provision,
- *Certificate* publishing,
- *Certificate* revocation status publishing,
- OCSP service.

Before a planned discontinuation, the *Service 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 *Service Provider* takes measures concerning the revocation of provider *Certificate*s (and destroying private keys) during the 60 day period – depending on the outcome of the negotiations.

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

Pursuant to section 2.2.1., the *Service Provider* will publish an announcement 5 days before its "Microsec e-Szigno Root CA 2009" and "e-Szigno Root CA 2017" *Certificate* is revoked.

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

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

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

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

6.1 Key Pair Generation and Installation

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

6.1.1 Key Pair Generation

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

- ETSI TS 119 312 [17];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [9] 92. § (1) b) .

The *Service 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 at least 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 [21] , or
  - meets the requirements of FIPS 140-2 [28] level 3 or higher, or
  - meets the requirements of CEN 14167-2 [30] workshop agreement,
  - is a reliable system that is evaluated in accordance with MSZ/ISO/IEC 15408 [20] 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. The independent auditor certifies that the key generation occurred according to the script.

In case of the generation of the key pair generated for the *Subject*s) by the *Service 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 *Cryptographic Hardware Device* the *Service Provider* generates the private key on the user's *Cryptographic Hardware Device* which makes the disclosure of the private key impossible.

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

In case of an *Applicant* generated key pair:

- the production of keys shall be done in a properly secure environment that is under the supervision of the *Applicant*;
- the *Applicant* shall ensure the proper protection of the generated private key;
- the *Service Provider* shall ensure that the generated key pair is compliant with the requirements defined in Sections 6.1.5 and 6.1.6, and the public key is not one of a known weak key pair.

In case of provider root and intermediate *Certificate* creation the *Service Provider* shall make a key generation record demonstrating that the process has been conducted in accordance with the predetermined workflow that ensures the confidentiality and integrity of the generated keys. The record shall be signed by:

- in case of the generation of the provider root certification unit private key the trusted officer of the *Service Provider* responsible for key management and as a witness a trusted person independent from the operation of the *Service Provider* (eg. notary, auditor) who verifies 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 *Service Provider* generated the *Subject*'s private key, then the following requirements are met:

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

In case of *Certificate Policies* requiring the use of a *Cryptographic Hardware Device* the private key of the *Subject* together with the *Cryptographic Hardware Device* providing the secure storage and usage of the private key, is handed over to the *Applicant* in person with the closed envelope containing the activation code.

In case of *Certificate Policies* not requiring the use of a *Cryptographic Hardware Device*, 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

When the key pair is generated by the *Applicant*, the following provisions shall be complied with:

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

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

The *Service Provider* issues the provider *Certificate*s needed for his trust services himself and generates the provider key pairs himself also, so there is not necessary to deliver the public keys. In case of the provider *Certificate* issued by another service provider – for example KGYHSZ –, the *Service Provider* sends to the issuer a PKCS#10 formatted *Certificate Application*, which is certified with the private key belonging to the public key to be indicated on the *Certificate*.

6.1.4 CA Public Key Delivery to Relying Parties

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

- The *Service Provider* publishes the full provider certificate hierarchy containing every root and intermediate provider certificate from which every current provider Certificate is downloadable (see at the Provider certificates point at the

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

  url).
- The denomination of the root and intermediate certification units and the *Root Certificate*s' hash is in the 1.3.1 section of the *Certification Practice Statement*.
- The Certificates of the intermediate certification units are published on the certified Hungarian provider list [33] maintained and published by the National Media and Infocommunications Authority within the framework of the European common regulations [32]. The list contains every provider certificate (even the expired and revoked ones).

- For the online certificate status response signer responders the *Service Provider* – according to the best international practice – issues *Certificate*s with very short validity periods, thus eliminating the necessity of checking the revocation status of the *Certificate*s. The current status of the *Certificate*s is continuously available at the webpage of the *Service Provider* at the

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

  address.

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

- The status information related to the *Certificate* of the root certification units is available on the webpage of the *Service Provider*.
- The status change information of the intermediate (not root) certification units' certificates is disclosed on the *Certificate Revocation List*s, on its webpage and within the confines of the online certificate status response service.
- For the responders signing the online certificate status responses the *Service Provider* – according to the best international practices – issues a *Certificate* with very short validity period to eliminate the necessity of checking the *Certificate* revocation status. The *Service Provider* guarantees that in case of key compromise or other problem no new *Certificate* will be issued for the old private key signing the OCSP responses . The *Service Provider* issues the OCSP response *Certificate*s for new, secure private keys.

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

6.1.5 Key Sizes

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

- ETSI TS 119 312 [17];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [9] 92. § (1) b) .

The *Service Provider* uses at least 2048 bit RSA keys or at least 256 bit ECC keys in every currently active root and intermediate provider *Certificate* and even in the *Certificate*s of the *Time-Stamping Unit*s and the OCSP responders.

6.1.6 Public Key Parameters Generation and Quality Checking

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

Hardware/Software Key Generation

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

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

The key pair generation of *Certificate*s issued according to *Certificate Policies* requiring the use of a *Cryptographic Hardware Device* is typically done on a *Cryptographic Hardware Device* with on-board hardware key generation. In case of the encryption *Certificate*s the *Service Provider* generates the key pairs on a *Hardware Security Module* or on a computer operating in a secure environment. The generated keys are imported to the *Cryptographic Hardware Device* in a secure environment.

The key generation of *Certificate*s issued according to Certificate Policies not requiring the use of a *Cryptographic Hardware Device* 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 *Service Provider* root certification unit private key may only be used for the following purposes:

- issuance of the self-signed *Certificate* of the root certification unit itself ,
- to sign the intermediate certification units' *Certificate*s,
- to sign the OCSP responder *Certificate*,
- to sign CRLs.

The private key of the *Service Provider*'s intermediate certification units – as well as the private key issued to the intermediate certification unit of other organizations – can only be used for the following purposes:

- to sign the intermediate certification units' *Certificate*s,
- to sign the end user *Certificate*,

- to sign the *Time-Stamping Unit Certificate*,
- to sign the OCSP responder Certificate,
- to sign CRLs.

The *Service Provider* includes the Key Usage extensions in the end-user certificates that define the scope of the Certificate usage and in the X.509v3 [27] compatible applications technically restrict the usage of the Certificates. The requirements set out for the value of the field are in Section 7.1.2.

The private key of the *Subject* belonging to its *Certificate* may only be used according to the key usage in the *Certificate*, any other usage is not permitted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

The *Service Provider* stores and uses the Root CA private keys physically isolated from normal operations such that only designated trusted personnel have access to the keys for use.

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

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

The *Service 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 *Service Provider* does not issue private keys to the *Subject* beforehand, eliminating the need to ensure the preservation of the end-user private keys.

6.2.1 Cryptographic Module Standards and Controls

The systems of the *Service 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 [21], or
- the requirements of FIPS 140-2 [28] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [30] 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 [20] 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 *Service Provider* provider keys are only stored in encrypted 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 [9] 92. § (1) b) that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

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

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

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

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

6.2.3 Private Key Escrow

The *Service Provider* copied its root CA keys in encrypted form into a CD. The CD is stored in a bank tresor in a closed envelop.

The *Service Provider* does not escrow its own provider private keys other than the root keys.

The *Service Provider* does not provide for the end-user authentication 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 *Applicant*.

6.2.4 Private Key Backup

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

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

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Service 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 *Service Provider* only exports the private key from the *Hardware Security Module* for the purpose of making a secure copy.

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

6.2.7 Private Key Storage on Cryptographic Module

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

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

6.2.8 Method of Activating Private Key

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

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

In case of the end-user private keys generated by the *Service 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.

In case of the private keys handled over by the *Service Provider* to the *Applicant* on a *Cryptographic Hardware Device* (like intelligent card or token): and configured and handed over by the *Service Provider* to the *Applicant* so that:

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

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

6.2.9 Method of Deactivating Private Key

Provider Private Keys

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

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

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

End-User Private Keys

In case of *Certificate Policies* requiring the use of *Cryptographic Hardware Device* the private keys shall be used in accordance with the requirements defined in the used cryptographic module's user guide and in the certification documents.

The *Cryptographic Hardware Device* handed over to the *Subject* ensures that the private keys become deactivated in the following cases:

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

The deactivated key and the *Cryptographic Hardware Device* may only be used after the re-identification of the *Applicant*.

In case of *Certificate Policies* not requiring the use of a *Cryptographic Hardware Device* the proper usage of the private keys is the responsibility of the *Applicant*.

6.2.10 Method of Destroying Private Key

Provider Private Keys

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

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

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

End-User Private Keys

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

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

Discarded authentication private keys of the end users are recommended to be disposed however, the encryption private keys are recommended to be preserved so that the previously encrypted documents can be decrypted later.

6.2.11 Cryptographic Module Rating

According to the requirements of Section 6.2.1 every provider private key of the *Service Provider* is stored in a cryptographic module that

- has a certification according to ISO/IEC 19790 [21], or
- has a certification according to FIPS 140-2 Level 3 [28], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [30] 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 *Service 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*.

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Keys and Certificates of the Root Certification Units

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

The validity period of the *Service Provider* root certification unit certificates and the private keys:

- the key of the "Microsec e-Szigno Root CA" root certification unit was valid until 2017-04-06;
- the key of the "e-Szigno OCSP CA" root certification unit was valid until 2017-04-26;
- the key of the "Microsec e-Szigno Root CA 2009" root certification unit is valid until 2029-12-30.
- the key of the "e-Szigno Root CA 2017" root certification unit is valid until 2042-08-22;

The Keys and Certificates of the Intermediate Certification Units

The validity period of the *Service Provider* intermediate certification unit certificates and the private keys belonging to them:

- shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority;
- shall not exceed the validity period of the issuer root or intermediate provider *Certificate* that issued the intermediate provider *Certificate*.

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

End-User Certificates

The validity period of the end user *Certificate*s issued by the *Service Provider*

- is maximum
  - in case of *Codesigning Certificate*s 39 months,
  - in case of other *Certificate*s 10 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 *Service Provider* may issue the new *Certificate* for the same end-user private key.

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.
If this happens, the *Service Provider* revokes the related *Certificate*s.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

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

In case of *Cryptographic Hardware Device*s provided by the *Service Provider* for the *Applicant*, the *Service Provider* provides:

- the activation data is created and installed to the *Cryptographic Hardware Device* is generated in a physically secure environment, with an adequate quality random number generator;
- the activation data to be handed over to the *Applicant* using a safe method.

The *Service Provider* never generates software based private keys for the end user *Certificate*s.

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

6.4.2 Activation Data Protection

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

In case of *Cryptographic Hardware Device*s issued for *Applicant*s by the *Service Provider*:

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

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;

- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *Service Provider* are sufficiently protected from unauthorized access;
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

6.5.2 Computer Security Rating

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Service 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/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

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

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Service Provider*

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

- commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by the *Service Provider* itself during which design structured development methods and controlled development environment were used, or;
- custom hardware and software solutions developed by a reliable party for the *Service Provider* during which design structured development methods and controlled development environment were used, or;

- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

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

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

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

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

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

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

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

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

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

6.6.2 Security Management Controls

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

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

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

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

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

6.6.3 Life Cycle Security Controls

The *Service 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 *Service Provider* taking into account the security aspects of the equipment life cycle.

- it uses in its systems 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 practically impossible to restore the keys.

6.7 Network Security Controls

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

The *Service Provider* applies proper network security measures for example:

- divides its IT system into well separated security zones;
- separates dedicated network for administration of IT systems and the *Service Provider*'s operational network;
- separates the production systems for the TSP services from systems used in development and testing;
- establishes communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- operates the IT systems used for the live operational network in secure network zones;
- restricts access and communications between zones to those necessary for the operation of the service;

- disables the not used protocols and user accounts;
- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .
- reviewes the established rule set on a regular basis.

The *Service Provider* undergoes or performs a vulnerability scan on public and private IP addresses:

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

The *Service Provider* checks the compliance of the local network components (e.g. routers) configuration with the requirements specified by the *Service Provider* at least every three months.

The *Service Provider* orders a penetration test from an external independent expert who has the necessary skills, tools, proficiency and code of ethics to provide a reliable report yearly and in case of a significant change in the IT network.

6.8 Time-stamping

For the protection of the integrity of the log files and other electronic files to be archived the *Service 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 *Service Provider* and all the provider's root and intermediate *Certificate*s which are in the *Certificate* Chain used to issue the *Certificate*s comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [27]
- IETF RFC 5280 [24]
- IETF RFC 6818 [25]
- ETSI EN 319 412-1 [13]
- ETSI EN 319 412-2 [14] in case of *Certificate*s issued to natural persons
- ETSI EN 319 412-3 [15] in case of *Certificate*s issued to legal persons

7.1.1 Version Number(s)

The provider certification unit (root and intermediate) *Certificate*s used by the *Service Provider* and the end-user *Certificate*s issued by the *Service Provider* are "v3" *Certificate*s according to the X.509 specification [27].
The *Certificate*s have the following basic fields:

- Version
  The *Certificate* complies with "v3" *Certificate*s according to the X.509 specification, so the value "2" is in this field. [24]
- 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 cryptographic algorithm set used for the creation of the electronic seal certifying the *Certificate*.

  The *Certification Authority* uses the following cryptographic algorithm:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Signature
  Electronic seal made by the *Certification Authority* certifying the *Certificate*, that has been created with an Algorithm set defined in the "Algorithm Identifier" field.
- Issuer
  The unique name of the *Certificate* issuer *Certification Unit* according to the 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 IETF 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 *Service Provider* supports the RSA end the ECC algorithms in the end-user *Certificate*s.

  The value to be included in this field:
  - "rsaEncryption" (1.2.840.113549.1.1.1)
  - "ecPublicKey" (1.2.840.10045.2.1)
- *Subject* Public Key Value
  The public key of the *Subject*.

- Issuer Unique Identifier
  Not filled out.
- *Subject* Unique Identifier
  Not filled out.

7.1.2 Certificate Extensions

the *Service Provider* only uses the following certificate extensions according to the X.509 specification [27]:

Certificate of the Root Certification Unit

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

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

  In case of the self-signed root certification unit certificate the value is identical with the value of the *Subject* key identifier field.
- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Subject* public key. The field value: the SHA-1 hash of the public key.

  Always filled in.
- Subject Alternative Names – not critical
  OID: 2.5.29.17

  It is filled in according to section 3.1.1.
- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

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

  The "pathLenConstraint" field is not present in the root *Certificate*.
- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  The used values are:

  - "keyCertSign",
  - "cRLSign".

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

The above fields are always filled out. There is no any more *Certificate* extension.

Certificate of the Intermediate Certification Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field may limit the *Certificate Policy*s which can be used in the Enduser *Certificate*.

  The intermediate CAs below this CA may issue only that type of Enduser *Certificate*s which fit to at least one of the *Certificate Policy*s listed here.

  It is always filled.

  In case of *Certificate*s issued to the intermediate certification units of the *Service Provider*, the "anyPolicy" Identifier may be present in this field.

  The reference to the related *Certification Practice Statement* can be given in this field. In case of certification unit *Certificate*s issued to other *Certification Authority*, only that identifier can be in this field, which relates to a *Certificate Policy* which complies to the *Certificate Policy* implemented by the issuer *Certification Authority*, and there can be no "anyPolicy" Identifier.

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

  It is always filled.

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

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

  It is always filled.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  It is filled in according to section 3.1.1.

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

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

  The "pathLenConstraint" is not present in the *Certificate*.

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

  The field contains the following values:

  – "keyCertSign",
  – "cRLSign".

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

  The Intermediate Certification Unit *Certificate*s issued after 2019-01-01 for issuing *Codesigning Certificate*s contains the following EKU value:

  – Code Signing EKU=1.3.6.1.5.5.7.3.3
  – OCSP Signing EKU=1.3.6.1.5.5.7.3.9

  The Intermediate Certification Unit *Certificate*s issued for other purposes does not contain any "Extended Key Usage" extension.

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL accessibility through http and/or ldap protocol.
  It is always filled.

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

  Mandatory, and the field contains the following data:

  – For the purpose of the fast and reliable verification of the current *Certificate* revocation status, the *Service Provider* provides online certificate status service. The availability of this service is indicated here.
  – To facilitate the certificate chain building the *Service 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 *Service Provider* fills in this field in all cases by providing the following data:

  - the identifier of the *Certificate Policy* (OID according to section 1.2.1);
  - the availability of the *Certification Practice Statement*;
  - the textual warning in English and Hungarian from which it can be established that it is a II. or III. certification class certificate, namely personal appearance did or did not happen at the registration, the Subject of the *Certificate* is a natural person, and the private key belonging to the *Certificate* is protected by a cryptographic hardware device.
  - The identifier specified by ETSI EN 319 411-1 [12] the policy which the *Certificate* complies with. as follows:
    * in case of DVCP *Certificate* OID 0.4.0.2042.1.6,
    * in case of OVCP *Certificate* OID 0.4.0.2042.1.7,
    * in case of IVCP *Certificate* OID 0.4.0.2042.1.8.

  The end-user *Certificate*s that do not contain the "Certificate Policies" field shall be considered test certificates. The test *Certificate* can only be used for testing purposes, and they shall be declined in case of real transactions.

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

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

  It is always filled in.

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

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

  It is always filled in.

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

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

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

  The "pathLenConstraint" field is not present in the end-user *Certificate*s.

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

In case of the different usage purpose *Certificate*s the following key usage bits are set (other value is not present):

Certificate type	keyUsage (kritikus)	ExtKeyUsage
Authentication	digitalSignature, keyAgreement (ECC)	clientAuth (1.3.6.1.5.5.7.3.2)
Cisco VPN client	digitalSignature, keyAgreement, keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
Cisco VPN Server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
Code Signing	digitalSignature	codeSigning (1.3.6.1.5.5.7.3.3), softwarePublishing (1.3.6.1.4.1.311.2.1.22)
DomainController	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)
Encryption	keyAgreement (ECC), keyEncipherment (RSA)	emailProtection (1.3.6.1.5.5.7.3.4)
RDP Gateway	keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1)
SCEP server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	
Smartcardlogon	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), smartcardLogon (1.3.6.1.4.1.311.20.2.2)
VPN Server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1)

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

  In case of the different usage purpose end-user *Certificate*s the key usage bits of the above table are set (other value is not present).

- 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 *Service 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 *Service Provider* provides online certificate status service. The availability of this service is indicated here.
  - To facilitate the certificate chain building the *Service Provider* gives the access path through http protocol of the *Certificate* of the *Certificate* issuer certification unit.

  The *Service Provider* may give in this field the data of more than one service and *Certificate* of the *Certificate* issuer certification unit.

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

  Based on the request of the *Client* the enduser *Certificate* may contain the optional statement describing the *Subject*'s data regarding the Payment Services EU Directive (PSD2) [2] (OID: 0.4.0.19495.2). If this data is present, its value is a data structure containing the service type of the *Subject*'s PSD2 service and the name and the abbreviation of the supervisory authority supervising the *Subject*'s financial service.

  In any other case the field is not present.

The above fields are always filled out according to the given rules.
Other certificate extensions will not be filled out.

7.1.3 Algorithm Object Identifiers

The denomination of the cryptographic algorithm that has been used to certify the *Certificate*. The following cryptographic algorithms are used by the *Certification Authority* for sealing the end-user *Certificate*s:

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

7.1.4 Name Forms

The *Service Provider* uses a distinguished name – composed of attributes defined in the standards IETF RFC 5280 [24], ETSI EN 319 412-2 [14], ETSI EN 319 412-3 [15] and ETSI EN 319 412-4 [16] – 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 *Service Provider* does not use name constraints with the use of the "nameConstraints" field.

7.1.6 Certificate Policy Object Identifier

The *Service Provider* includes the not critical (*Certificate Policy*) extension in the *Certificate*s according to the requirements of the Section 7.1.2..

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The *Service 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 *Certificate Revocation List*s according to the IETF RFC 5280 [24] specification.

7.2.2 CRL and CRL Entry Extensions

The *Certificate Revocation List*s issued by the *Certification Authority* shall compulsorily include the following fields:

- Version
  The value of the field is compulsorily "1".
- Signature Algorithm Identifier
  The identifier (OID) of the cryptographic algorithm set used for creating the electronic seal certifying the *Certificate Revocation List*. The name and ID of the cryptographic algorithm sets used by the *Service Provider*:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Signature
  The electronic seal of *Certification Authority* certifying the *Certificate Revocation List*. The given certification unit certifies the *Certificate Revocation List* with its key used for signing the *Certificate*s.

- Issuer
  The unique identifier of the *Certificate Revocation List* issuer certification unit.
- This Update (thisUpdate)
  The date of the entry into force of the *Certificate Revocation List*. Value according to UTC with encoding according to IETF RFC 5280 [24]. In case of the *Certificate Revocation List*s issued by the *Certification Authority* this is the same as the issuance time.
- Next Update (nextUpdate)
  The issuance time of the next *Certificate Revocation List* (see Section 4.10.). Value according to UTC with encoding according to IETF RFC 5280 [24].
- 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 *Certificate Revocation List* extensions to be filled in by *Certification Authority* as mandatory:

- CRL number – not critical
  OID: 2.5.29.20
  The consecutive serial numbers of the *Certificate Revocation List*s are in this field.

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

- expiredCertsOnCRL – not critical
  OID: 2.5.29.60
  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
  OID: 2.5.29.21
  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 *Service Provider* operates an online certificate status service according to the IETF RFC 6960 [26] standard.
The OCSP responses issued by *Certification Authority* contain the following fields:

- Algorythm identifier (signatureAlgorithm)
  The identifier of the cryptographic algorithm used for signing the OCSP response (OID). The *Service Provider* supports the following cryptographic algorithms:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- (Signature)
  The digital signature of the *Service Provider*.
- Identifier of the Responder (responderID)
  The unique identifier of the OCSP Responder which issues the OCSP Response.
- This Update (thisUpdate)
  The date of the entry into force of the OCSP Response. Value according to UTC with encoding according to IETF RFC 5280 [24].
- Next Update (nextUpdate)
  The latest issuance time of the next OCSP Response. Value according to UTC with encoding according to IETF RFC 5280 [24]. Optional.
- *Certificate* Status Response (SingleResponse)
  The field contains the ID of the *Certificate* (CertID) and the revocation status of the *Certificate* (CertStatus).

  The *Service Provider* issues positive OCSP response according to the requirements of the CABF BR. The Response contains the "good" value only if the *Certificate* is included in the *Certificate Repository* of the *Service Provider* and its revocation status is not suspended or revoked.

7.3.1 Version Number(s)

The *Service Provider* supports the online certificate status requests and responses conforming to the “v1” version according to the standard IETF RFC 6960 [26]. The default value of the (Version) field is "v1", so this field is not included in the OCSP response.

7.3.2 OCSP Extensions

The *Service Provider* may optionally include the following OCSP extension:

- ArchiveCutoff – not critical
  The *Certification Authority* may indicate with a standard notation according to the IETF RFC 6960 [26] specification that it retain revocation information beyond the *Certificate*'s expiration. (See Section 4.10.)

The *Service Provider* may include the following 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 *Service Provider* has its operation periodically examined by independent external auditor. During the audit it is examined that the operation of the *Service Provider* complies with the following normative documents:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [12]

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 *Service Provider*.

The *Service Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Service Provider* has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The *Service Provider* keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

In addition to the external audit, the *Service Provider* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Service Provider* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation. (see section: 1.3.1.)

8.1 Frequency or Circumstances of Assessment

The *Service Provider* has the conformance assessment carried out annually on its IT system performing the provision of the services .

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 *Service Provider* performs the internal audits with the help of its employees who hold the independent system auditor role.

The eIDAS and ETSI conformity assessment is performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

8.3 Assessor's Relationship to Assessed Entity

External audit is performed by a person who:

- is independent from the owners, management and operations of the examined *Service Provider*;
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the *Service Provider*.
- remuneration is not dependent on the findings of the activities carried out during the audit.

8.4 Topics Covered by Assessment

The review covers the following areas:

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

If the *Service Provider* issued a subordinate *Certificate* for the certification unit of another organization then the listed areas are examined at these external organizations as well.

8.5 Actions Taken as a Result of Deficiency

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

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

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

8.6 Communication of Results

The *Service Provider* publishes the summary report of the assessment on its web page on the following url:

`https://e-szigno.hu/en/eidas/`

The *Service Provider* doesn't publish the detailes of the findings, they are treated as confidential information.

9 Other Business and Legal Matters

9.1 Fees

The *Service Provider* publishes fees and prices on its webpage, and makes them available for reading in printed form at its customer service.

The *Service Provider* may unilaterally change the price list. The *Service Provider* publishes any modification to the price list 30 days before it comes into force. The changes favorable for the *Client* may come into force with shorter deadline than 30 days. Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service agreement and its annexes – the General Terms and Conditions in particular.

9.1.1 Certificate Issuance or Renewal Fees

See section: 9.1.

9.1.2 Certificate Access Fees

The *Service 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 *Service 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 *Service Provider* takes financial responsibility to fulfil all its obligations defined in the present *Certification Practice Statement*, the related *Certificate Policy* and the service agreement concluded with the *Client*.

9.2.1 Insurance Coverage

The *Service Provider* has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

The *Service Provider* does not have liability insurance. The *Service Provider* indemnification is described in section 9.6.1.

9.3 Confidentiality of Business Information

The *Service Provider* manages clients' data according to legal regulations. The *Service Provider* has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

By applying for a *Certificate*, and signing the service agreement, *Client*s consent to the *Service Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the *Service Provider*'s services go offline; moreover to forwarding such information to the *Service Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

*Applicant*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 *Service Provider* uses clients' data solely in connection with the provision of its services. The *Service Provider* discloses *Subject*s' and *Represented Organization*s' data appearing in a *Certificate* together with the *Certificate* in case a *Applicant* consents to this. The *Service Provider* stores their data that are not entered in a *Certificate* in a secured manner, for the purpose of providing evidence about the *Subject*s' identity, *Represented Organization*s' organisational identity,

and that of its miscellaneous data provision related obligations. The *Service Provider* retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the *Service Provider* sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The *Service Provider* provides for the confidentiality and intactness of information that is not public during the forwarding of *Client*s' data.

9.3.1 Scope of Confidential Information

The *Service Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 9.3.2;
- besides the *Client* data:
  - private keys and activation codes,
  - certificate 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 *Service Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

In case the *Applicant* grants consent, the *Service Provider* treats all of the data it indicates in a *Certificate* as non-confidential information. Such data appear in the *Certificate* application form linked to the service agreement in a clearly marked way.

The *Service 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 *Certificate 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 optionally the reason for revocation. For more information, see section 7.2. and 7.3.

9.3.3 Responsibility to Protect Confidential Information

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

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

The *Service Provider* processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following cases:

- **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 *Service Provider* reveals confidential user information pertaining to the *Client* to third parties.

9.4 Privacy of Personal Information

The *Service Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Service Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [7] and the 2016/679 EU General Data Protection Regulation [3].
The *Service Provider*:

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

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

The *Service Provider* stores identification data, data about the *Subject* appearing in the *Certificate*, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.

The *Service Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

9.4.1 Privacy Plan

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

9.4.3 Information Not Deemed Private

The *Service Provider* may disclose the data of the *Subject*s indicated in the *Certificate* based on the written consent of the *Applicant*.

The *Service Provider* may indicate the unique provider identifier assigned to the *Subject* in the *Certificate*.

9.4.4 Responsibility to Protect Private Information

The *Service Provider* stores securely and protects the personal data related to the *Certificate* issuance and not indicated in the *Certificate*. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

9.4.5 Notice and Consent to Use Private Information

The *Service Provider* only discloses personal data indicated in the *Certificate*s with the written consent of the *Client*.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the relevant legislation the *Service Provider* may disclose the stored personal data about the *Client* without notifying the *Client*.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

During its business operation, the *Service Provider* shall not harm any intellectual property rights of a third person.

The owner of the private and public key issued by the *Service Provider* to clients is the *Subscriber* and the full user is the *Applicant* regardless of the physical media that contains and protects the keys.

The owner of the *Certificate* issued by the *Service Provider* to its clients is the *Service Provider* and its full user is the *Applicant*.

The *Service Provider* may publish, reproduce, revoke and manage the issued end-user *Certificate*s, with the public key contained in them in the manner described in the terms and conditions.

The certificate revocation status information is the property of the *Service Provider* which is disclosed as defined in sections 7.2. and 7.3.

The unique provider identifier issued to the *Client*s by the *Service Provider* is the property of the *Service Provider* which

is disclosed as a part of the *Certificate* by the *Service 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 *Service Provider*. The *Client*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Certification Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

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

The rules of the application of the software provided for the use of the service by the *Service Provider* is accessible in the description of the software and it is included in the user's guide referenced in the description.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the *Service Provider* is in the *Certification Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- The *Service Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Service Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;
- The *Service Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [8] in relation to the *Client*s which are in a contractual relationship with it.
- The *Service Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [8] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Service Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8.).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Service 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 *Service Provider*'s basic obligations is that it shall provide the services in line with the *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 *Service Provider*'s internal, operative regulations specify how a certification organization shall be operated. Certification Authority's certificates issued by certification units are managed (for registration staff members, on-call duty staff, etc.) in accordance with the stipulations of operative regulations. This statement only includes stipulations in connection with the public provider and end-user certificates.

Tasks to be performed in the scope of managing regulations:

- the specification, approval, and maintenance of certificate types that are used;
- preparing the public regulations of the services and internal (not public) stipulations, their reconciliation with legal regulations and internal (not public) regulations, furthermore carrying out any updates;
- the recording of observations associated with regulations applicable to the services, and to evaluate recommendations.

The e-Szignó Certification Authority is responsible:

- for the authenticity and accuracy of the *Certificate*s it issued;

- for the regulations it has issued, and for their the conformity and compliance with statutory regulations;
- for the compliance of the key pairs it generated, and for the relationship between the private-public key and the *Certificate*;
- for the relationship of the *Electronic 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 *Service Provider* at end-users in connection with the services. It performs the following tasks in the scope thereof:

- participates in selling the services;
- performs the registration of *Subject*s;
- receives requests pertaining to various certificate operations (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 *Service Provider*;

The *Registration Authority* is responsible:

- for establishing the personal identity of *Applicant*s;
- for establishing the organisational identity of *Represented Organization*s, and in this latter case for establishing the right of representation of an individual acting in the name of a *Represented Organization*;
- for the genuineness of recorded registration data;
- for providing information to those using the services as to the contents and availability of the *Certificate Policy* and the *Certification Practice Statement*, as well as the terms and conditions of using the service prior to concluding the service agreement;
- in general to fully comply with its obligations.

9.6.3 Subscriber Representations and Warranties

Subscriber Responsibility

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

Subscriber Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *Service Provider* while using the service including requesting and applying the *Certificate*s and private keys.

The obligations of the *Subscriber* are determined by this *Certification Practice Statement*, the service agreement and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Certificate Policy*s.

When the *Subscriber* is informed about any actual or suspected misuse or compromise of the private key associated with the public key included in a *Certificate* belonging to the *Subscriber*, the *Subscriber* is obliged to

- promptly report this fact to the *Service Provider*,
- promptly request the revocation or suspension of the *Certificate*,
- promptly cease using the *Certificate* and its associated private key.

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 *Organizational Administrator*s.

Applicant Responsibility

The *Applicant* is responsible for:

- the authentication, accuracy and validity of the data provided during registration;
- the verification of the data indicated in the *Certificate*;
- to provide immediate information on the changes of its data;
- using its private key and *Certificate* according the regulations;
- the secure management of its private key and activation code;
- for the immediate notification and for full information of the *Service Provider* in cases of dispute;
- to generally comply with its obligations.

Applicant obligations

The *Applicant* shall:

- read carefully this *Certification Practice Statement* before using the service;
- completely provide the data required by the *Service Provider* necessary for using the service, and to provide truthful data;
- if the *Applicant* becomes aware of the fact that the necessary data supplied for using the service – especially data indicated in the certificate – have changed, it is obliged to immediately:
  - notify the *Service Provider* in writing,
  - request the suspension or revocation of the *Certificate* and
  - terminate the usage of the *Certificate*;
- use the service solely for the purposes allowed or not proscribed by legal regulations, according to the cited regulations and documents;
- ensure that no unauthorized individuals have access to data and tools (passwords, secret codes, signature-creation devices) necessary for using the service;
- notify the *Service Provider* in writing and without delay in case a legal dispute starts in connection with the *Certificate*s associated with the service;
- cooperate with the *Service Provider* in order to validate the data necessary for issuing certificates, and to do everything they can to allow the soonest possible completion of such verification;
- the *Applicant* shall answer to the requests of the *Service Provider* within the period of time determined by the *Service Provider* in case of key compromise or the suspicion of illegal use arises;
- acknowledge that the *Subscriber*s entitled to request the revocation and/or suspension of the *Certificate*;
- acknowledge that the *Service Provider* issues *Certificate*s in the manner specified in the *Certification Practice Statement*, upon the completion of the validation steps described therein;
- acknowledge that the *Service Provider* only displays data that are corresponding to reality in issued *Certificate*s. Accordingly, the *Service Provider* validates data to be entered in *Certificate*s according to the *Certification Practice Statement*;
- acknowledge that the *Service Provider* revokes the issued *Certificate* in case it becomes aware that the data indicated in the *Certificate* do not correspond to the reality or the private key is not in the sole possession or usage of the *Applicant* and in this case, the *Applicant* is bound to terminate the usage of the *Certificate*;

- acknowledge that the *Service Provider* has the right to suspend and revoke *Certificate*s if the *Subscriber* fails to pay the fees of the services by the deadline;
- in case of requesting an *Organizational Certificate*, acknowledge that the *Service 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 *Service Provider* has the right to suspend and revoke *Certificate* if the *Subscriber* violates the service agreement or the *Service Provider* becomes aware that the *Certificate* was used for an illegal activity (for example phishing, fraud, malware spreading).

***Applicant* Rights**

- *Applicant*s have the right to apply for *Certificate*s in accordance with the *Certification Practice Statement*.
- In case this is allowed by the applicable *Certificate Policy*, *Applicant*s are entitled to request the suspension and 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 *Service Provider* it is necessary for the *Relying Party* to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the present *Certificate Policy* and the corresponding *Certification Practice Statement*;
- use reliable IT environment and applications;
- verify the 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 *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 *Applicant* is a staff member of the *Service Provider*, moreover is entitled to appear in the *Represented Organization*'s *Certificate*. In case the information appearing in any certification made out by the *Represented Organization* is changed, reporting this to the *Service Provider* without delay is the *Represented Organization*'s responsibility.

Represented Organisation rights

- The *Service Provider* only issues *Certificate*s in which the *Represented Organization*'s name is indicated in possession of the *Represented Organization*'s consent.
- The *Represented Organization* is entitled to suspend and revoke *Certificate*s in which the *Represented Organization*'s name was also indicated.

9.7 Disclaimers of Warranties

The *Service Provider* excludes its liability if:

- *Applicant*s do not follow the requirements related to the management of the private key;
- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it;
- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by international standard recommendations.

9.8 Limitations of Liability

Conditions of liability of the *Service Provider*:

- The *Service Provider* is not responsible for damages that arise from the *Relying Party* failing to proceed as recommended according to effective legal regulations and the *Service Provider*'s regulations in the course of validating and using certificates, moreover its failing to proceed as may be expected in the situation.
- The *Service Provider* shall only be liable for contractual and non-contractual damages connected to its services in relation to third parties with respect to provable damages that occur solely on account of the chargeable violation of its obligations.
- The *Service Provider* is not liable for damages that result from its inability to tend to its information provision and other communication related obligations due to the operational malfunction of the Internet or one of its components because of some kind of external incident beyond its control.
- If The *Service Provider* engages data comparison with an authentic database before the issuance of the *Subject*'s *Certificate*, it relays on the data received from the authentic database. The *Service Provider* will not assume any liability for damages arising out of the inaccuracy of information provided by such authentic databases.
- The *Service Provider* assumes liability solely for providing the services in accordance with the provisions of this *Certification Practice Statement*, as well as the documents to which reference is cited herein (Certification Policies, standards, recommendations), moreover with its proprietary internal regulations.

Administrative Processes

The *Service Provider* logs its activities, protects the intactness and authenticity of log entries, moreover retains (archives) log data over the long term in the interest of allowing for the establishing, documenting, and evidencing of financial accountability, its proprietary liability related to damage it causes, as well as that of damage compensation due to it for damage it suffers.

Financial Liability

The *Service Provider* has liability insurance according to the legal regulations required in order to ensure reliability.

Limitation of Financial Liability

The *Service Provider* limits the obligation for compensation related to services, the extent of this limitation is 100.000,-HUF per damage event.

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 *Service Provider*

The detailed rules of the indemnities of the *Service Provider* are specified in this regulation (see section: 9.8.), the service agreement and the contracts concluded with the *Client*s.

9.9.2 Indemnification by Subscribers

The *Subscriber* and the Subject are liable for damages to the *Service Provider* for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3 Indemnification by Relying Parties

See section: 9.8.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific *Certification Practice Statement* is specified on the cover of the document.

9.10.2 Termination

The *Certification Practice Statement* is valid without a time limit until withdrawal or the issuance of the newer version of the *Certification Practice Statement*.

Section 9. of the *Certification Practice Statement* shall remain effective even after the termination of the *Certification Practice Statement*'s effect (regardless of the manner in which effectiveness is terminated) in connection with any and all *Certificate*s which the *Service Provider* will have issued while the *Certification Practice Statement* was effective.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Certification Practice Statement* the *Service Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

The *Service Provider* guarantees that in case of a the *Certification Practice Statement* withdrawal, requirements for the protection of the confidential data remain in effect.

9.11 Individual Notices and Communications with Participants

The *Service Provider* maintains a customer service in order to contact with its *Client*s.

The *Client*s may make their legal declarations to the *Service Provider* solely in writing, and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

Issued *Certificate*s may also be suspended by sending an SMS. Notifications of other nature may also be given in writing, in the form of electronic mail or fax.

The e-Szignó Certification Authority informs its *Client*s by means of publication on its webpage or in electronic mail.

9.12 Amendments

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

9.12.1 Procedure for Amendment

The *Service Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Service Provider* has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 8.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Service 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 *Service Provider* strives to only issue new regulations at the least frequent intervals possible.

The *Service Provider* reviews the *Certification Practice Statement* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change 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 *Service Provider* .

9.12.2 Notification Mechanism and Period

The *Service Provider* notifies the *Relying Parties* of new document version issuances as described in Section 9.12.1..

9.12.3 Circumstances Under Which OID Must Be Changed

The *Service 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 *Service Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Service Provider* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The *Client* in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the *Service Provider* or the use of issued *Certificate*s shall be addressed to the customer care centre office in written form. The *Service Provider* notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Service Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Service Provider* may request the provision of information required for giving a response from the submitter. The *Service Provider* investigates complaints within 30 days, and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the *Service Provider* involved, the submitter may initiate consultation with the *Service Provider* and the *Relying Parties*. All participants of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof;

and the submission, the *Service Provider*'s response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The *Relying Parties* shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

9.14 Governing Law

The *Service Provider* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Service Provider* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

9.15 Compliance with Applicable Law

The applicable regulations:

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

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 *Service Provider*.

9.16.3 Severability

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The *Service Provider* is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the *Service Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Certification Practice Statement*, it would waive the enforcement of claims for damages.

9.16.5 Force Majeure

The *Service Provider* is not responsible for the defective or delayed performance of the requirements set out in the *Certificate Policy* and the *Certification Practice Statement* if the reason for failure or delay was a condition that is outside the control of the *Service Provider*.

9.17 Other Provisions

No stipulation.

A Interpretation of the short policy names

For the simplier handling of the *Certificate Policies* the *Service Provider* defines a five characters long short name (identifier) for each *Certificate Policy*, where each character is meaningful and defines some basic feautures of the given policy according to the following rules:

- First character [?....]
  - M: qualified *Certificate Certificate Policy*
  - H: non-qualified, III. certificate class *Certificate Certificate Policy*
  - K: non-qualified, II. certificate class *Certificate Certificate Policy*
  - A: non-qualified, automatic issuance *Certificate Certificate Policy*
- Second character [.?...]
  - A: Signing purpose *Certificate Certificate Policy*
  - B: Seal creation purpose *Certificate Certificate Policy*
  - W: *Website Authentication Certificate Certificate Policy*
  - K: *Codesigning Certificate Certificate Policy*
  - E: Other purpose *Certificate Certificate Policy*
- Third character [..?..]
  - T: *Certificate* issued to a natural person *Certificate Policy*
  - J: *Certificate* issued to a legal person *Certificate Policy*
  - x: no stipulation, can be issued to any type of *Subject*
- Fourth character [...?.]
  - B: *Certificate* issued on *Qualified Electronic Signature Creation Device Certificate Policy*
  - H: *Certificate* issued on *Cryptographic Hardware Device Certificate Policy*
  - S: *Certificate* issued by software *Certificate Policy*
  - x: no stipulation, it can be issued on any platforms
- Fifth character [....?]
  - A: pseudonymous *Certificate Certificate Policy*
  - N: pseudonym excluding *Certificate Certificate Policy*

B REFERENCES

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC .

[2] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC .

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

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

[5] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

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

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

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

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

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

[11] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[12] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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

[14] 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;.

[15] 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.

[16] 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.

[17] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[18] ETSI TS 119 495 V1.3.2 (2019-06); Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.

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

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

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

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

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

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

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

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

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

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

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

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

[31] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.

[32] EU Trusted Lists of Certification Service Providers, (`https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers`.

[33] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

[34] e-Szignó Certification Authority - Non eIDAS covered Certificate Certificate Policies.

[35] e-Szignó Certification Authority - Qualified Signing Certificate Policies .