NETLOCK
Trust Service Policy
for Qualified Certificate Services

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
[NETLOCK Informatics and Network Security Services Limited Liability Company]

Document name in Hungarian:	NETLOCK Bizalmi Szolgáltatási Rend Minősített Tanúsítványszolgáltatásokra
Document name in English:	NETLOCK Trust Service Policy for Qualified Certificate Services
Version:	20170721
Object identifier (OID):	1.3.6.1.4.1.3555.1.14.20170721
Date approved:	21/07/2017
Valid from:	21/08/2017
No. of pages:	96 pages, including cover
Prepared by:	**dr. Anett Barabás**, Quality Assurance Expert **Zoltán Szabó**, PKI Product Manager **Viktor Varga**, Chief Architect
Accepted by:	**dr Zsófia Fehér**, Chief Legal Officer

Table of contents

1 Introduction

(This document is a translation of the original same titled Hungarian language Service Policy that has also the same OID as the present document has (see Hungarian and English title and the OID on cover). The present English version is not the official Service Policy for qualified certificate services of NETLOCK. The official Service Policy registered by the Supervisory Body is the Hungarian version that is available same way on the TSP website as the present document. In case of any difference between the Hungarian and the English version, Hungarian version is considered the normative Service Policy.)

***

The purpose of the present Trust Service Policy is to summarize and systematize the minimum requirements (hereinafter: Service Policy) that pertain to NETLOCK Kft.'s (hereinafter: Service Provider) Certificate Issuance Trust Services.
This Service Policy covers the certificate issuance under the QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w and the EVCP certification policies, and also includes the requirements of the issuance, revocation processes, and also includes the requirements of the revocation services. The Service Provider issues only certificates following the mentioned certificate policies, as ruled by the Practice Statement covered by the qualified trust services written in Chapter 1.1.

See Chapter 1.2.1. for Detailed description of the Certificate Policies.
See Chapter 1.6 for the terms and abbreviations used in this document.

1.1 Overview

The present document contains the requirements pertaining to the Service Provider's following trust services:

- qualified certificate creation services,
    - creation of electronic signature certificates
    - creation of electronic seal certificates
    - creation of website authentication certificates
- qualified certification service for the employees – with powers to issue document and to act in the course of the administration – of the authorities where electronic administration service is available based on the Electronic Adiminstration Act (Eüt), and for the IT systems of these authorities (such certificates shall be hereinafter referred to as "governmental certificates");
- qualified certification service within the framework of the NETLOCK SIGN service;
- certificate status services related to qualified certificate services.

1.1.1 Standards and legislation

This document was prepared in accordance with the structure of the RFC 3647 standard. The document summarizes the requirements of eIDAS, the Electronic Administration Act (see 1.6.2 Acronyms), and other applicable Hungarian legislation, as well as standards ETSI EN 319401, ETSI EN 319411, ETSI EN 319412, and ETSI EN 319421. The various chapter titles serve only to order the contents according to the given logical order but are not governing in the interpretation of the provisions.
The document entitled NetLock Qualified Trust Service Practice Statement For Certification provides information on meeting the requirements. The Practice Statement and the Clauses shall define the details of the services and also shall include the needed tools for the use.

1.1.2 Service provider identification

Company Name:	**NETLOCK Informatics and Network Security Services Limited Liability Company**
Hungarian name:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Short name (EN/HU):	NETLOCK Ltd. / NETLOCK Kft.
Registered seat:	H-1101 Budapest, Expo tér 5-7.
Postal address:	H-1439 Budapest, Pf. 663
Company registration number:	01-09-563961
TAX ID:	12201521-2-42
Phone number:	+36 (1) 437-6655 Application for certificate status change: Press 3
Fax number:	(1) 700-2828
Website:	www.netlock.hu
Customer service e-mail:	info@netlock.hu
Orders, document copies, agreements are received at:	igenylesek@netlock.hu
NETLOCK Policy Acceptance Unit email:	szee@netlock.hu
Customer service / Business hours	At the place and within the time interval set out on the website of the Service Provider

The Trust Services Supervisory Authority registered the Service Provider as qualified certificate authority compliant with the provisions of the Electronic Signature Act[1] on March 19, 2003. Registration number: MH-1372-12/2003.

The Trust Services Supervisory Authority registered the Service Provider as qualified archiving service provider compliant with the provisions of the Electronic Signature Act on September 15, 2010. Registration number: HL/18188-4/2010.

The registry of the services under the Electronic Signature Act maintained by the Trust Services Supervisory Authority is available at http://webpub-ext.nmhh.hu/esign/
The present Service Policy establishes the requirements of the provision of qualified trust certificate service compliant with the provisions of eIDAS. Service Provider is allowed to commence the provision of these services only upon the fulfillment of the statutory conditions set out in the Service Policy – e.g. compliance assessment, inclusion of the Service Provider and its service on the trust service list and registration with the supervisory authority.
The public registry of the qualified service providers and qualified services under the eIDAS maintained by the Trust Services Supervisory Authority is available at:

[1] Act XXXV of 2001 on Electronic Signature – repealed

http://webpub-ext.nmhh.hu/esign2016/szolgParams/init.do?tipus=mi

The EU Trust Services List (EUTSL) is available in the following formats at the following URLs:

- in machine readable format (xml): http://nmhh.hu/tl/pub/HU_TL.xml
- in human readable format (pdf): http://nmhh.hu/tl/pub/HU_TL.pdf

Service Provider is entitled to use the EU Trust Mark[2] as regards its qualified services.

1.2 Document name and identification

For the name of the document and its OID, see the cover sheet (first page with the logo of Service Provider) in the lines of "A dokumentum magyar neve" (Hungarian identification of the document) and "A dokumentum angol neve" (English identification of the document) and also in the "Azonosító szám (OID)" (identification number) lines.
On the other pages in the header the OID is displayed, and the Hungarian name in the footer.
The present document is one of the documents issued by the Service Provider that jointly regulate the conditions of the services it provides. Such documents are for example the General Terms and Conditions, the Service Agreement, the Practice Statements, and other contracts concluded with Clients and Partners.
The entity called in this document as Service Provider, the Netlock Ltd. detailed identification can be found in the Chapter 1.1.2.

1.2.1 Certificate Policies

In the field used to indicate the Certificate Policy (CP) in end-user certificates, the Service Provider is shall include a standard identifier or an identifier that itself created and registered, which aims to identify the standard or individual certification rules pertaining to the given certificate and to declare compliance with those. (Such standard identifiers can be e.g. the policy identifiers defined by ITU or CAB Forum). According to the recommendations of RFC 5280, one such identifier is recommended, for which reason only a single standard identifier should be indicated wherever possible.
The Service Provider should give test options for each certificate type. The test purpose of Test certficates needs to be displayed obviously.
The present document contains the provisions pertaining to the certificates and services applicable to the following Certificate Policies. If any of the provisions are only applicable to certain certificates issued with certain Certificate Policy, the given provision is clearly indicates the related Certificate Policies in brackets.

Identifier	**Certificate Policy name (or Service Practice)**	**OID**
EVCP	Policy for **Extended Validation** Website Authentication Certificate. The purpose of these certificates is to create website authenticating certificates based on the Guidelines For The Issuance And Management Of Extended Validation Certificates of CA/Browser Forum.	2.23.140.1.1
QCP-l	Policy for EU **qualified** certificate issued to a legal person	0.4.0.194112.1.1

[2] https://ec.europa.eu/digital-single-market/en/eu-trust-mark

	The purpose of these certificates is to support advanced seals based on qualified certificates, in accordance with Articles 36-38 of eIDAS.	
QCP-l-qscd	Policy for EU **qualified** certificate issued to a legal person where the private key and the related certificate reside on a **QSCD.** The aim of these certificates is to support qualified seals in accordance with Article 3 (point 27) of eIDAS.	0.4.0.194112.1.3
QCP-n	Policy for EU **qualified** certificate issued to a natural person The purpose of these certificates is to support advanced signatures based on qualified certificates, in accordance with Articles 26-28 of eIDAS.	0.4.0.194112.1.0
QCP-n-qscd	Policy for EU **qualified** certificate issued to a natural person where the private key and the related certificate reside on a **QSCD.** The aim of these certificates is to support qualified signatures in accordance with Article 3 (point 12) of eIDAS.	0.4.0.194112.1.2
QCP-w	Policy for EU **qualified** website certificate issued to a natural or a legal person and linking the website to that person The aim of these certificates is to support website authentication with qualified certificates in accordance with Articles 45 and 3 (point 38) of eIDAS with the exception, that othese certificates are issued only for legal persons, to clearly meet the requirements pertaining to EV certificates.	0.4.0.194112.1.4

The QCP-l and QCP-n certificate policies can mean both Cryptographic device-based (non-QSCD) services and services that do not require a Cryptographic device (which is made clear by the certificate's secondary certificate policy field – see below). When a certificate issued following the QCP-w certificate policy, then also the EVCP certificate policy is applicable, and both the identifiers needs to be included into the certificate (see Chapter 7.1.6 Certificate Policy identifier)

In the issued certificate, the Service Provider can also indicate another, secondary certificate policy in addition to the standardised certificate policies described above. This certificate policy starts with the NetLock (1.3.6.1.4.1.3555.6) or MELASZ (1.3.6.1.4.1.48016.3) identifier.
The structure of the certificate policy:
Level.KeyStorage.Subject.KeyUse.Identification., where the individual attributes can have the following values:

Level:	0 - test 1 - non-qualified 2 - qualified
Key storage:	1 - software-based (not device-based) 2 - SCD (device-based)

	3 - QSCD (qualified device-based) 4 - managed SCD (device)-based
Subject:	1 - natural person 2 – legal person 3 - pseudonym 4 - domain name 6 - product name and trademark 9 - regulated professional and other special 12 - natural person connected to a legal person 41 - domain and natural person 42 - domain and legal person 71 - Employee of authorities providing electronic administration service, having powers to act in the course of the administration 72 - Employee of authorities providing electronic administration service, having powers to issue documents 73 - IT system of authorities providing electronic administration service 91 – Attorney
Key use:	1 - signature 2 - seal 5 - website authentication
Identification:	0 - Unchecked 1 - Without personal appearance 2 - Based on personal appearance 3 – Equivalent to a personal appearance

In the case of qualified trust services, the Service Provider applies the following primary certificate policies: QCP-l, QCP-l-qscd, QCP-n, QCP-n-qscd, and QCP-w.

1.2.2 Revisions of the Document

OID	Validity	Description of change	Prepared by
1.3.6.1.4.1.3555.1.14.20170721	from 21.08.2017 until it is withdrawn or until a new version comes into force	This document is a translation of the original same titled hungarian language Service Policy that has also the same OID as the present document has (see Hungarian and English title and the OID on cover). No translation of the earlier versions of the official Hungarian document was made.	Szabó Zoltán Varga Viktor

1.3 PKI participants

Within the framework of the present Certification Policy, PKI participants shall mean the Clients of the qualified certification service – the Applicants of the certificates and the Subscribers of the

Service, the End Users of the certificates, the Service Provider and its organizational units, as well as the Relying Parties.

See further the relevant definitions set out in Chapter 1.6.1 Definitions.

1.3.1 Certification Authorities

The Service Provider is generally liable for the services it provides. It can use the services of third parties to provide these services, but it shall ensure in the contract that the services they provide meet its Terms and Conditions, and it is liable for their activities towards clients.
The operation of the Certification Authority shall be in compliance with the requirements governing the Certification Authority set out in the applicable Service Policy (or Policies), Practice Statement(s) and other Terms. The employees of the Certification Authority shall comply with, and shall carry out their operations in accordance with, the requirements set out in its internal rules of operation.
The Service Provider shall, in all cases, be fully liable for the compliance with the requirements pertaining to the Certification Authority.
The Service Provider and its CA shall be mentioned (as issuer) in the certificates it issues, and the Service Provider's private key shall be used for certifying the certificate.

1.3.2 Registration Authorities

The Registration Authority may operate as part of the Service Provider, but it can also be a separate, independent body (External Registration Authority).
The operation of the Registration Authority has to meet the requirements set out in the applicable Certificate Policy (or Policies), Practice Statement(s), and in other Clauses, as well as the requirements pertaining to the Registration Authority. The employees of the Registration Authority shall comply with, and shall carry out their operations in accordance with, the requirements set out in its internal rules of operation.
The Service Provider is always fully liable for adhering to the requirements applicable to the Registration Authority.
The Service Provider shall obligate any External Registration Authorities to ensure their operations meet the applicable requirements.

1.3.3 Subscribers, End-Users, and Applicants

The Subscriber and the Applicant are the Service Provider's clients, with whom the Service Provider enters into a contractual relationship.
The person of the End User shall be determined by the Subscriber.

See further the relevant definitions set out in Chapter 1.6 Definitions and Abbreviations.

The Service Provider, and any employee, organizational unit or partner service provider thereof may be the Client of service only if it is expressly enabled in the practice statement of Service Provider.

1.3.4 Relying Parties

The Relying Parties are typically not in contractual relationship with the Service Provider, but the practice statement prepared on the basis of the present Service Policy may provide them with

recomendations in relation to the services they use, which are typically free of charge, mostly certificate status reports.
The Service Provider primarily communicated with Relying Parties by way of the certificate repository.

See Chapter 1.6.1 for the term Relying Party.

1.3.5 Other participants

Signatory partners

By entering into unique agreements, Service Provider may involve so called Signatory Partners in the provision of the NL Sign service.
The Signatory Partners may participate in the preparation of the registration of the End Users. The Signatory Partners have no access to the certificate, the keys and the activation data.
The Signatory Partners shall not come into contact with, and shall not be aware of, the private key and activation data of the End Users, and therefore the Signatory Partners shall not be able to create signature or stamp on behalf of the End Users.

The Root Certification Service Provider for the Hungarian Public Administration (Public Root Provider; Hungarian: Közigazgatási Gyökér Hitelesítés-szolgáltató – KGyHSz)

The Root Certification Service Provider for the Hungarian Public Administration (hereinafter: Public Root Provider) is the organization that certifies the certificates to be used in the Hungarian public administration by the public organizations where electronic administration is available.
The Service Provider shall warrant that service provider certificate that is used for certifying such end user certificates are certified by the Public Root Provider.
The Service Provider shall maintain an issuing body, the certificate of which is certified the Public Root Provider, and shall warrant that Service Provider uses this issuing body to issue the certificates for Hungarian public organizations where electronic administration is available.

1.4 Certificate usage

The certificates issued according to the QCP-I and QCP-n certificate policies are qualified certificates, the private keys of which can only be used for creating non-qualified signatures / seals.
The certificates issued according to QCP-I-qscd and QCP-n are qualified certificates, the private keys of which can be used for creating qualified signatures / seals.
The certificates issued according to the EVCP, and QCP-w certificate policies can be used to identify web servers accessed via SSL and TLS protocols.
See the Key Use field and the Key Usage of the secondary certificate policy, as well as the other restrictions included in the certificate (which can even be text-based) for the applicability of the certificates.

1.4.1. Proper use of certificates

The private keys belonging to the end user certificates issued under the present Service Policy shall be used only for creating electronic signatures and electronic stamps. With the certificates and the public keys stored therein the Relying Parties may vertify the given electronic signature or

electronic stamp, and they can verify the entity specified as the subject is identical to the person who created the signature/stamp. The creators of the signature/stamp may certify the authenticity of the electronic documents or other data sigend/stamped by them.
The private key that belongs to the qualified signature/stamp certificates issued in accordance with the QCP-l-qscd and QCP-n-qscd certification policies are protected by a qualified signature creation device (QSCD). The eIDAS-compliant qualified certificates issued this way are capable of creating qualified eIDAS-compliant electronic signatures.
The private key that belongs to the qualified signature/stamp certificates issued under the QCP-l and QCP-n certification policies may be stored on an electronic signature creating device (SCD) and by software key storage, as well. The eIDAS-compliant qualified certificates issued this way are capable of creating increased security eIDAS-compliant electronic signatures/stamps that are based on eIDAS-compliant qualified certificates.
The qualified electronic signature or stamp and the increased security electronic signature or stamp based on qualified certificate are capable of creating – by electronic means – public or private document with full probative value pursuant to Articles 195 and 196 of Act III of 1952 on the Code of Civil Procedure.
There is no similar requirement as to the storage of keys in the case of the qualified website certification certificates issued under the QCP-w certification policy. The qualified website certification certificates are capable of certifying websites and are issued by the Service Provider in accordance with the rules of EVCP.

1.4.2. Prohibited use of certificates

a. End user certificates

The signing and sealing certificates issued under the present Service Policy (QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd) and the related keys are prohibited to be used for purposes other than the creation or verification of electronic signature or stamp.
Website authentication certificates issued under the present Service Policy (QCP-w, EVCP) and the related keys are prohibited to be used for purposes other than website authentication.

b. Service provider certificates

The intermediate certificates, and their keys, that certify the service provider root and end user certificates shall not be used for certification of certificates prior to the publication of the service provider certificate and its public key.

1.5 Policy administration

The Service Provider’s policy unit issues and maintains this Service Provider’s Trust Service Policy. The Service Provider operates its policy unit as part of its own unit; the separate regulations contain its exact structure, tasks, scope, and responsibilities.

1.5.1 The organization that carries out the administration of the document

The name of the organizational unit of the Service Provider that is responsible for the policies (terms) is NETLOCK Policy Adopting Authority (Hungarian: NETLOCK Szabályzatelfogadó Egység). The permanent members of the Policy Adopting Authority are those employees of the Service Provider, who are appointed in writing by the Management of the Service Provider. The

operation of the Authority is regulated in the internal, non-public rules of operation of the Policy Adopting Authority.

See Chapter 9.12 for the amendment to the policies of the Service Provider.

1.5.2 Contact person of the document

The responsible contact person of the Policy Adopting Authority shall be the approver of the present document (see the cover page of the document).

Customers, End Users and the Relying Parties may submit their questions and comments related to the present document to the NETLOCK Policy Adopting Authority in e-mail to szee@netlock.hu.

The employees of Service Provider may also submit their comments to the Policy Adopting Authority in other channels, as well, but their comments shall be made in writing in all cases.

The contact person shall be responsible for replying to queries sent in e-mail to the Policy Adopting Authority and for implementing other measures, if necessary, on the basis of the comment.

In the case of any question or comment related to the present document and submitted to the Policy Adopting Authority, the contact person shall designate the member of the Authority who shall process the query. In the case of a complicated query, the contact person shall convene the meeting of the Policy Adopting Authority in accordance with the rules of operation of the Authority.

In the course of processing the query the Authority or the member shall identify the section(s) of the document affected by the comment or question, then shall respond to the sender in e-mail upon consulting with the other members of the Authority, and with other employees, if necessary.

In the event the amendment of the present Service Policy or any other document becomes necessary on the basis of the query, the Service Provider shall act in accordance with Chapter 9.12 in relation to the amendment.

1.5.3 The organization responsible for the compliance of the practice statement with the service policy

The compliance of the Practice Statement – which contains the detailed practical requirements of the provisioning and use of the qualified certification service under the present Service Policy – with the Service Policy shall be monitored by the NETLOCK Policy Adopting Authority. The practice statement prepared on the basis of the present Service Policy may be approved by the Policy Adopting Authority if practice statement is in complete compliance with the the present Service Policy.

The Certificate Policy or its public draft may be published only upon approval.

1.5.4 Approval of the Practice Statement

The rules of procedure of approving the Practice Statement shall be set out by the Service Provider in the Service Policy.

See Chapter 9.12 for the amendment of the Certificate Policy.

1.6 Definitions and acronyms

1.6.1 Definitions

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Included in certificates and points to the download URL of the Issuer certificate
Alárendelt szolgáltatás	Szolgáltató szabályzatai alapján működő nem minősített bizalmi szolgáltatás, mely számára Szolgáltató biztosít tanúsítványt.
Activation data	A code (password or PIN code) generated by the Service Provider or provided by the End-User that is known only to the End-User and is used for bringing the private key into a state ready for use. Unrelated to certificate activation.
Signature	See electronic signature
Signature / Seal Creation device	A Cryptographic device that is not suitable for creating qualified signatures / seals. (See also Chapter 1.6.2 Abbrevations SCD)
Signature service	The following services as defined by eIDAS: ● the creation, checking, and validation of electronic signatures and electronic seals, ● as well as the checking and validation of the related certificates. In the framework of this policy, the provision of these services is understood to mean “cloud-based,” by the Service Provider storing the end-user signature and seal keys and signing/sealing (including the affixing of an optional timestamp) the documents uploaded by clients via the web-based service/protocol and checking the above.
Signing Partner	A service partner that provides a signature service to its own clients, as part of which it can participate in the identification of End-Users (in regards to whom it has limited informational and administrative rights), that uses the signature service in an integrated manner with its own services to provide services, and that undertakes to pay fees on behalf of End-Users as a Subscriber.
Subject	See the definition in Article 1 point 43 of the Electronic Administration Act. In the framework of the present Policy, Subject is taken to mean the Subject and SAN fields and the data included therein, which can refer to a natural person and/or an organization and/or a trademark/product name or the identifier/other name of a device/system or to its pseudonym. See the Applicant, Subscriber, Client, and End-User entities.
Status change	The procedure that results in a change in the certificate’s status (valid, suspended) and receives a new value (valid, suspended, revoked).
Archiving service	According to Article 1 point 2 of the Electronic Administration Act: “A service for the long term storage of electronic documents, which also includes the trust service referred to in Article 3 point 16 c) of the eIDAS Regulation.” Within the framework of this Policy, it refers to a qualified trust service where the Trust Service Provider creates or supplements the entire certificate chain of the electronically certified (signed or sealed) documents it is provided for the purposes of archiving, affixes an archiving timestamp to the

	certificate chain, and securely stores the thus supplemented document or file.
Recipient	A person receiving one of the end-user's keys or devices (e.g. Client device) and its activation data from the Service Provider (in person, via traditional or electronic means of delivery); a person that can be an Applicant of the given certificate can be a Recipient.
Seal	See electronic seal
Trusted list	A list managed by an authority or software producer, which contains the identifiers (generally the certificates) of the trust services considered reliable. A software handling a given trust list accepts those signatures, seals, and timestamps for the services that can be traced back to it. It is generally used to refer to the EU trust list, which includes qualified and non-qualified services as defined by eIDAS on recommendation of the supervisory bodies of the various member states. See: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers
Trusted employee	A person in a trusted role at the Service Provider or at a Service Partner.
Trust Service Policy	NETLOCK Bizalmi Szolgáltatási Rend Minősített Tanúsítványszolgáltatásra (This policy.)
Supervisory Body	The body designated by the Electronic Administration Act to supervise trust services. Specifically the National Media and Infocommunications Authority.
Trusted role	The executive role generally responsible for the Service Provider's IT system. See Chapter 5.2.1 Trusted roles.
Trust service	According to Article 3 point 16 of eIDAS: "an electronic service normally provided for remuneration which consists of: - the creation, verification, and validation of electronic signatures, electronic seals or electronic timestamps, electronic registered delivery services and certificates related to those services; or - the creation, verification and validation of certificates for website authentication; or - the preservation of electronic signatures, seals or certificates related to those services." Within the framework of this Policy, it is used to mean the services that ensure the issuance of the Service Provider's certificates and lifecycle management related to electronic signatures, electronic seals, and website authentication, as well as timestamp services.
Security zone:	A (logically or physically) secured area that protects the privacy, integrity, and accessibility of the systems used by the Service Provider.
CAA check	A check where the Service Provider searches the DNS registry for CAA records as per RFC 6844. The certificate cannot be issued if it contains a record that shows that the domain name holder communicates with another Service Provider.
Eakta (container format)	Digital signature container format, which includes the documents, also include their meta data, digital signatures and contra signatures, and

	timestamp too. as described in the ETSI TS 101 903 (XAdES) specification. See detailed at: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html (hungarian content)
EV certificate Extended Validation Certificate (EVC)	A certificate for website authentication that meets EVCG requirements.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (Article 3 point 10 of eIDAS). For the purposes of this Policy: Electronic data created by a natural person with the pair to the signature certificate private key issued by the Service Provider, which data is attached to the electronic document that is to be signed (or to other electronic data) and that can be checked with the certificate and the public key included in it.
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. The equivalent to the electronic signature created by a legal person.
Subscriber	The Service Provider's contractual partner that undertakes to pay service fees. The Subscriber's rights and obligations are separately defined in the GTC and the Service Agreement. In the case of certificate creation services, if an organization has also been indicated as the Subject of the certificate or it names only one natural person, it is generally the same as such person(s).] In the case of of NLSign services equal to the Signing Partner or the End-User in the case of signature services.] See the Client, Applicant and End-User entities, as well as Chapter 1.3.3 Subscribers, End-Users, and Applicants.
Subscriber's agent	A person who is authorized to perform business-related transactions on behalf of the Subscriber. The representative (and also the agent) must sign an authorization document designates the person as an agent, allowing him to perform actions in the representative's stead.
Relying Party	A natural or legal person who does not enter into a contractual relationship with the Service Provider but receives one of its certification creation services (generally free of charge) (e.g. checks electronic signatures, seals, or timestamps and thereby checks the validity information of certain certificates or service provider regulations). See Chapter 1.3.4 Relying Parties.
Valid certificate	A certificate that is currently valid and that is presently neither suspended nor revoked (see Certificate Status).
Validity (period)	A period between a start and end date for which the certificate was issued.
Device-based certificate	A certificate where the private key is issued for a Cryptographic device.
Certificate chain	The electronic document or its hash and the series of information that can be linked to each other (thus especially the certificates, information

	pertaining to certificates, the data used to create the signature or seal, the information pertaining to the current status or revocation of the certificate, and the information pertaining to the validity data of the service provider that issued the certificate and to its revocation) which can be used to establish whether the advanced or qualified electronic signature, seal, or timestamp on the electronic document was valid at the time of affixing the signature, seal, or timestamp. In general, this means a hierarchy of certificates that authenticate each other, all the way to the root certificate.
Advanced electronic signature	An electronic signature that meets the requirements defined by Article 26 of eIDAS.
Advanced electronic seal	An electronic seal that meets the requirements defined by Article 36 of eIDAS.
Certificate Policy	According to Article 1 (24) of the Electronic Administration Act: a trust service policy that pertains to a certificate issued in the framework of a trust service. In the framework of the Service Provider's regulations, a standard procedural policy on the basis of which the Service Provider issues and manages certificates. The Service Provider's regulations contain more than one Certificate Policies, which differ in their applicable requirements and procedures.
Certification Authority	The Service Provider's organisational unit that performs issuance, publication, revocation, and suspension of certificates and the publication of the Certificate revocation list based on the request of the Registration Authority. See Chapter 1.3.1.
Certification Administrator	The employees in this position approve the issuance of the certificates within the Certification Authority.
Authorized Person	A Relying Party who has access free of charge to specific functions of the service for documents specified by, upon the request of, the Subscriber of the archiving service.
Applicant	In the case of certificate creation services, the natural person proceeding in the certificate issuance, certificate authentication, and status change procedure and that accepts the service agreement on behalf of the Client. The Applicant can be: ● the natural person indicated as the Subject of the certificate (in case of a pseudonym, the pseudonym's applicant); ● in absence of the above, the representative or authorized representative of the organization indicated as the Subject of the certificate; ● in absence of the above, the holder of the domain name, trademark, or product name; if the owner is an organization, the representative or authorized representative of such organization; or the person with control over the domain name. The same as the Subscriber if the Subject of the certificate is indicated as being a natural person (and no organization is indicated). In the case of NLSIGN service it's the same as the End-User. It's the Subscriber's representative/agent in the case of timestamping and archiving services.

Timestamp	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.
Timestamp Server	The Service Provider's technical system that issues timestamps.
Timestamp URL	The virtual token that provides access to the timestamp service and contains the unique identifier of the Subscriber, through which the End User may transmit timestamp requests to Service Provider, and Service Provider may transmit timestamp replies to End User on the basis of the request.
Delivery Agent	The Delivery Agent is a partner of the Service Provider, who carries out the delivery of the client device in relation to the Issuance of the Certificate upon the appointment by the Service Provider at a place and date agreed with the Applicant, if requested by the Applicant. The Delivery Agent may be identical to the Registration Agent, as the case may be.
Public Root Provider	Public Root Provider (Közigazgatási Gyökér Hitelesítés-Szolgáltató) See Article 1.3.5 and http://www.kgyhsz.gov.hu/
Central Registration Authority	The organizational unit operating within the organization of the Service Provider that processes the applications for services, identifies the Applicant and the Subscriber, verifies their right to act and their credentials.
Timestamp service	The Service Provider's service in the framework of which it provides a timestamp for the provided data hash on the basis of the submitted electronic data.
Initial suspension	A special case of Certificate suspension where the Service Provider immediately suspends a certificate after its issuance, thus protecting it from abuse until the time the Certificate and the private key are safely received by the Client.
Right of representation	Full or partial right of representation, or any legal relationship that can be understood as such (see Article 82 (9) of the Electronic Administration Act).
CA	The Service Provider's technical system that issues certificates. The Service Provider has an Intermediate CA that issues end-user and certain TSP certificates, as well as a Root CA with the highest level in the hierarchy that authenticates these units.
External Certification Authority	A Certification Authority operated by a separate organisation or person independent of the Service Provider (as a Service Partner) based on the Service Provider's requirements.
External Registration Authority	A Registration Authority operated by a separate organisation or person independent of the Service Provider (as a Service Partner) based on the Service Provider's requirements.
Terms and Conditions	Those of the Service Provider's documents that provide information on how the Service Provider meets which requirements pertaining to the provision of its services, as well as on the rights and obligations of the other participants. This includes the Service Provider's excerpt of services, Authentication Policy, Service Practice Statement , GTC, Service

	Agreement, and the aggregate of any other agreements concluded between them.
Cryptographic device	A secure hardware device that includes the End-User's private key, protects it from being compromised, and uses the key to conduct cryptography actions (e.g. signatures, encryption) on behalf of the End-User. It can be an SCD and QSCD, HSM or other, non-signature targeted device. It can be managed by both the Service Provider or the Client. In the latter case, it is referred to as a "Client device."
Critical services	The Service Provider's services pertaining to certificate and key creation, to providing Clients with devices, and to status changes.
Re-key	The process where the Service Provider issues a new Certificate and a private key to an already registered Client (or to itself) on the basis of an existing certificate. The end-user's public key is changed in the new certificate. See Chapter 4.7.
Key escrow service	A service that ensures the safekeeping of the end-user's private key and its handing over to the end-user (if the end-user's key were to become lost, destroyed, or inoperable for any other reason).
Private key	One of the keys in the pair generated by the Service Provider or the client, which is managed by the end-user. See public key. If the public key is included in a signature or seal certificate, it complies with the definition of electronic signature creation data and data used for the creation of electronic seals as defined by eIDAS.
Qualified Signature / Seal Creation device	A Cryptographic device that is suitable for creating qualified signatures / seals.
Qualified certificate	A certificate issued by a qualified TSP and that is in line with Annex I, III, or IV of eIDAS or Directive 1999/93/EC, depending on which was in effect at the time of the issuance of the certificate.
Qualified certificate for website authentication	According to Article 3 point 39 of eIDAS: "A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of eIDAS." A qualified certificate that ensures the visitors to a website with the authentication of the websites indicated in it that there is a real and legitimate organisation behind it.
Mobile Registration Agent	A registration agent, who carries out the identification of the Applicant at a place and time agreed with the Applicant upon the request of the Applicant if a personal meeting is necessary.
NL Sign service	A secure central key storage (managed SCD) and key management service, which makes possible the electronic signature/stamping (and timestamping) of documents uploaded on a web-based interface, as well as the verification of the signature/stamp of the document certified this way. The application for the certificates usable within the framework of the NL Sign service and the submission of the required registration details, and (the

	commencement of) use of the service after the issuance of the certificate shall take place on the web-based interface of the NL Sign service.
Public key	One of the keys of the pair generated by the Service Provider or the client, which the Service Provider includes in the certificate it creates. See private key.
Organizational Validation Certificate (OVC)	A certificate for website authentication that contains checked organisational data in the certificate.
Permanent Identifier	An identifier, which enables the unique identification of the user of the certificate. The implementation thereof in the certificate shall take place on the basis of RFC 4043. It may be generated by the service provider, or a unique identifier recorded in the official registry. The identifier generated by the service provider is an OID that consists of two parts: the unique identifier of the Service Provider (1.3.6.1.4.1.3555), which is followed by that of the Client. The unique identifier of the Client begins with a 5, which is followed by a number, which may have the following values: ● 1,6,8,10: in the case of personal or business certificates, where the identifier is generated from the data of the natural person. ● 2,7,9,11: in the case of organizational certificates, where the identifier is generated from the data of the organization. If applied, the Permanent Identifier is located in the Subject/SerialNumber field of the certificate.
Registration	An initial identification procedure that the Service Provider performs in the interest of identifying the Applicant and the Subscriber, verifying their right to proceed, and registering their data.
Registration Authority	The Service Provider's authority that conducts the processing of requests for services, the identification of the Applicant and Subscriber, and the checking of their right to proceed and the data to be included in the certificate. The Registration Authority can be both within the Service Provider (as an internal organisational unit) and outside of it (External Registration Authority).
Validation Specialist	Trusted role. See Chapter 5.2.1 Trusted roles.
Registration (and revocation) Administrator	The employee of the Service Provider who works in this position within the Registration Authority shall manage the applications for certification and verify the veracity of the data submitted in the application for certificate (lásd see chapter 4.2.1) as well as the processing and implementation of the requests for revocation (4.9).
SSL certificate	Certificate for website authentication
Organization	Legal person or private entrepreneur or independent attorney in the respect of the subject / subscriber of the certificate.
Service	For the purposes of this Policy, the Service Provider's trust services (see Chapter 1.1).
Software Certificate	A certificate, the private key of which is not issued onto a Cryptographic

	device.
Service Practice Statement	The statement of the trust service provider about the requirements and conditons of the procedural and operational requirements. (see ACT 1.§.41) which is the regulations containing the detailed procedural and other operational rules related to the Service Provider's activities.
Service Agreement	The Agreement concluded between the Service Provider and the Client, which contains the terms for the provision and use of the service. Its conclusion is a prerequisite of using the service.
Service Provider	NetLock, which provides trust and non-trust services in accordance with the present Trust Service Policy.
Service Provider's regulations	The present Trust Service Policy, the Trust Service Practice Statement, the GTC, the Service Agreement, and the Service Disclosure, as well as other private regulations.
Service Partner	An independent natural or legal person separate from the Service Provider that participates in the provision of the service on the basis of an agreement concluded with the Service Provider.
TSP system	The aggregate of the Service Provider's systems providing the service.
TSP certificate	Those of the Service Provider's certificates that it uses in the interest of providing the service (e.g. certificates for CAs and Timestamp Servers).
Certificate	The authenticated certification issued by the Service Provider that links the public key to the Subject and certifies the veracity of the data published in the Certificate.
Certificate Activation	The status change procedure that restores the validity of a suspended certificate. Following its activation, a certificate is also retroactively valid for the time of the suspension as if the suspension had not taken place.
Certificate Status	The valid/revoked/suspended status of the certificate registered by the Service Provider during the validity of the certificate, about which it informs its Clients and the Relying Parties by way of the Certificate Revocation List and the Certificate Status service.
Online Certificate Status Service (OCSP)	A service that provides real-time information on the status of a given certificate to Relying Parties. See also: Certificate Revocation List.
Certificate Suspension	The status change procedure in which the Service Provider temporarily terminates the validity of a still valid Certificate before the end of its originally planned expiration. Certificate suspension is a temporary state; suspended Certificates can be revoked or the Certificate can be revalidated within its original period of validity. If suspension is revoked, the Certificate becomes retroactively valid as if the suspension had never taken place.
Certificate enrolment	The process by which the Applicant enrols for a certificate, i.e. it provides the data required for preparing the certificate and certifies those to the Service Provider and then certifies its request with the signing of the Service Agreement by the Applicant and - if different than the Applicant - the Subscriber for the certificate being applied for, thus authorizing the Service Provider to issue the requested certificate.

Certificate Management Procedure	A procedure that results in the issuance of a new certificate based on the data of an existing certificate and the data of an earlier client registration (see Chapter 3.3 Authentication and certification in the course of certificate management procedure and Chapter 4 Lifecycle requirements).
Certificate creation service	Those of the Service Provider's services within the framework of which it creates a new certificate. This can be based either on an existing certificate (subsequent issuance with a certificate management procedure) or without any such precedent (original issuance).
Certificate renewal	The process by which the Service Provider issues a new Certificate for the same public key with the same Subject but for a new validity period. See Chapter 4.6.
Certificate modification	The process by which the Service Provider issues a Certificate to a previously registered Applicant on the basis of a Certificate issued previously, with the public key included in the latter, but with modified Subject or Service Provider data. See Chapter 4.8.
Certificate repository	The Service Provider's records containing issued certificates, through which the public certificates issued by the Service Provider and the Certificate Revocation List can be queried.
Certificate type	Differentiation between the various certificates issued by the Service Provider according to certain features, generally on the purpose of use. See Chapter 1.2.1 of the Service Agreement.
Certificate Revocation	The status change procedure in which the Service Provider terminates the validity of a Certificate before the end of its originally planned expiration. Certificate Revocation is irreversible and results in a permanent status change; a revoked certificate loses its validity at the time of its revocation and can never again be validated.
Certificate Revocation List (CRL)	An authentic list of the certificates that are temporarily or permanently invalid published regularly and following status changes by the Service Provider in the Certificate Repository. Accepting and using the certificates included in the list is not recommended. A type of certificate status service as defined by Article 17 of Decree 24/2016 of the Minister of the Interior.
Test Certificate	A Certificate issued by the Service Provider for testing purposes, the contents of which is the same as a specific certificate but its certificate policy field and the name of the Subject indicate that it is a test. Such certificates cannot be used to undertake commitments, result in no legal effects, and can only be approved for testing purposes. The Service Provider does not assume liability for the data contents or use of such certificates or for the availability of the connected services.
UCC website authentication certificate	A certificate for the certification of websites, which enlists various different domain names (in the SubjectAltName/DNSname record).
Client Menu	An interface accessible on the website of the Service Provider, which is provided for the submission of various applications related to certificates and the related services, and for monitoring the status of the applications in

	progress, where clients may log in by entering a unique user name and password (following the registration with the client menu). The management of the qualified certificates requires the registration with, and logging in, the qualified client menu, while the management of the non-qualified certificates requires the registration with, and logging in, the enhanced security client menu.
Client Menu Registration	The process, where natural or legal persons create their own Client Menu by submitting their data, as well as the login name and password required for logging in the Client Menu.
Client	The party that concludes a contract with the Service Provider. In the case of certificate creation services, the Applicant and Subscriber of the certificate (in certain cases, these may be identical).] In the case of NLSIGN signature services, the Signing Partner and the End-User.] See Chapter 1.3.3 Subscribers, End-Users, and Applicants
Client device	See Cryptographic device.
Client Registration	Validation of the identity of natural and non-natural persons, validation and recording of their data prior to entering into the first service agreement and issuing the first certificate. See Chapter 3.2 Initial Identity Validation.
End-User	The natural person who disposes over the private key pair to the public key included in the certificate (is the sole user or is responsible for its use).] In the case of NLSIGN signature services, the person who performs electronic signature/seal activities by activating the private key within the framework of the signature service, or who performs checks of the electronic signature/seal or is responsible for such activities.] See the Client and Subscriber entities, as well as Chapter 1.3.3 Subscribers, End-Users, and Applicants.
End-User Certificate, End-User Key	Indicates the Subscribers' certificate and key, as opposed to the Service Provider's own certificates and keys.
Certificate for Website Authentication	The certificate according to Article 3 point 38 of eIDAS.
Wildcard Certificate for Website Authentication	A certificate for website authentication that was issued by the Service Provider for the authentication of more than one subdomain (the domain name is indicated in the format *.domain.hu, meaning it includes all the subdomains that belong to domain.hu).

1.6.2 Acronyms

The acronyms of referenced legislation

eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Electronic Administration Act	Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services
Records Act	Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens
Free Movement Act	Act I of 2007 on the Admission and Residence of Persons with the Right of Free Movement and Residence
Third-Country Nationals Act	Act II of 2007 on the Admission and Residence of Third-Country Nationals
Information Act	Act CXII of 2011 on Informational Self-Determination and Freedom of Information
Regulation No. 24/2016 of the Ministry of Interior	Regulation No. 24/2016. (VI. 30.) of the Ministry of Interior on the detailed requirements of trust services and trust service providers.

Acronyms of technical terms

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CAA	Certification Authority Authorization
IP	Internet Protocol
IT	Information Technology
TSP	Trust Service Provider
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement / Service Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider

EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN SubjectAltName	Subject Alternative Name
SCD	Signature / Seal Creation Device
SSL	Secure Socket Layer
SP	Service Provider
TLS	Transport Layer Security
TSP	Trust Service Provider
QSCD (previously SSCD)	Qualified Signature / Seal Creation Device
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

See further Chapter 9.15 hereof.

2. Publication and repository responsibilities

The Service Provider is obligated to provide information in its Regulations on the data pertaining to the disclosure of various information (regulations, certificates, validity, and the organisations that make these public, if such different from the Service Provider) pertaining to certificates and to make such Regulations public.

2.1 Repositories

The Service Provider shall maintain a public certificate repository and systems that communicate certificate revocation information (CRL, OCSP), and shall ensure that the Terms and Conditions related to the certificates that may be issued under the present Service Policy.
Service Provider shall warrant that the availability of its systems that publish its service provider certificates, the public certificate respository and the revocation information shall be at least 99.9 per cent per annum, and that the length of the service outage shall not exceed 3 hours per occasion.

2.2 Publication of certification information

The Service Provider is obligated to create a certificate repository and to keep it up to date.
The Service Provider is obligated to disclose the certificates to Clients and Relying Parties. Thus especially:

- After its creation, the entire and exact certificate shall be made available to the End-User.
- End-user certificates can only be published if the end-user grants its consent.
- The requirements and conditions for the use of the certificate shall be made available to the Relying Parties both publically and on an international level;
- The requirements and conditions applicable in regard to the certificate have to be identifiable;
- The Service Provider has to ensure that published certificates and conditions are continuously accessible. The Service Provider has to take all measures to ensure that this information not be available for a period longer than indicated in the Service Practice Statement .
- Revoked, expired and valid website authentication certificates provided for testing purposes.

The requirements and conditions shall be made public with the contents and in the structure required by RFC 3647. Chapter 4.2 of the Service Practice Statement has to state whether the Service Provider reviews the CAA Record and, if yes, the procedure it uses to process domain names. If the Service Provider performs such activity, it shall create logs thereof.
The Practice Statement shall include the BRG[3] and EV statements[4], if applicable.
The Service Provider shall, at least 30 days before their entry into force, publish on its website (see Chapter 1.1.2) the new versions to be implemented of the Certificate Policy, the Practice Statement and other public documents pertaining to the services based on the present Service

[3] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.4.pdf (chapter 2.2)
[4] https://cabforum.org/wp-content/uploads/EV-V1_6_2.pdf (chapter 8.3)

Policy. Service Provider shall ensure that in addition to the terms and conditions in force, those earlier versions thereof shall also be available, on the basis of which any certfificate is still in force. Following the entering into of the service agreement, Service Provider shall provide the Client with the applicable practice statement and the Service Agreement on a durable medium.

2.3 Time or frequency of publication

The Service Provider shall publish on its website (see Chapter 1.1.2) the Terms and Conditions and the newer versions thereof at least 30 days before their entry into force, Service Provider shall ensure that in addition to the terms and conditions in force, those earlier versions of the documents shall also be continuously available, on the basis of which any certfificate is still in force.

At least once a year, the Service Provider shall review its Trust Service Policy and regulations and make any amendments as necessary. (see Chapter 9.12)

2.4 Access controls on repositories

The Service Provider has to make its repository and Requirements and Conditions publically available with read access.
Service Provider shall make its public certificate repository, the certificate status service and the Terms and Conditions publicly availabve with read access.
Service Provider shall make these services, repositories and information available for Clients and Relying Parties without any restriction. However, Service Provider may restrict access on grounds of the protection of service in case of excessive use. The terms and conditions of restriction shall be published on the website of Service Provider.

3. Identification and authentication

The Service Provider shall follow the requirements of the identification and authentication requirements pertaining to the use of certificate creation services and also the Service Provider shall describe these processes in Chapter 3.

3.1 Naming

The certificate’s Issuer identifier and Subject identifier fields shall meet the ITU-T X.509, RFC 5280, and ETSI EN 319 412 name format requirements. The meaning of The Issuer and the Subject identification fields also included into the Practice Statement.

3.1.1. Types of names

When creating the Subject field for a certificate, the Service Provider has to follow the X.500 distinguished name requirements in accordance with the RFC 5280 standard (or, in the case of emails, the RFC 822 standard). Within the above, it differentiates between several types of names in the case of end-user certificates
The Service Provider should publish detailed description about the types of names, their meaning, thein interpretation rules, and other information.

3.1.2. Need for names to be meaningful

The Subject field of signer certificates (QCP-n, QCP-n-qscd) issued to natural persons have to include the following data:

- countryName (country code);
- givenName+surname or pseudonym (first and last name or pseudonym)
- commonName (name)

In case only a legal person is specified as the Subject of the certificate, Service Provider shall specify the unique identifier of the organization in the Subject/organizationIdentifier field of the certificate.
In case both a natural person and an organization is specified as the Subject of the certificate, the Service Provider shall set out the cases in the practice statement where the identifier is mandatorily specified.
The SAN field of the website certifying certificates (QCP, EVCP) shall include the domain name set out in the commonName field.
Only one field shall be used from among the above mandatory fields.

The Subject field of certificates issued to legal personshave to include the following data:

- countryName (country code);
- commonName (name)
- organizationIdentifier (organization VAT number)

The name of the natural and legal person included in the certificate shall be indicated identically to authentic records or, in absence of such, official identification documents, or the articles of association, as applicable.
The Subject fields of test certificates can take the form of any of the certificates issued by the Service Provider; however, the commonName field is always to clearly and legibly indicate the nature of the test, ensuring that its contents not be misleading and that it cannot be confused with an actual person.
The Subject/organizationIdentifier field is to include a unique identifier received in a pre-set semantic format from an official national or other identification system, as defined by ETSI EN 319 412-1 5.1.4 (included in the *REFCO-organisation* identifier format, where REF and CO shall be replaced by three and two characters, respectively, as set forth below).
Instructions for filling out:

1. If the organisation has a tax number, the field is to be filled out accordingly: if the tax number is Hungarian, use the value “VATHU”, if the tax number is an EU tax ID, use the value “VATEU.”
2. If the previous point is not applicable, use the commercial register code with the value “NTRHU”.
3. If the previous points are not applicable, the value “XX:HU” is to be used based on the national registered semantics, where “XX” is the two characters of the national or EU identification schema.
4. If the above points are not applicable, another individual official identification can also be used.
5. If none of the mentioned forms of identification are available, the ID of the deed of foundation and the name of the founding document can also be used.

In the case of the identification systems of other countries, the HU country code is to be replaced with the respective ISO 3166 country code.

If the contents of the Subject/Serialnumber field is an official (checked on the basis of a document) national identifier, the Service Provider fill it out in a standard format. The field can be filled out on the basis of the passport, personal identification card, driving license, tax identification number, or other individual identification systems, in accordance with ETSI EN 319 412-1 5.1.3.
In accordance with the above, if a national identifier is used, it takes the following compulsory format: <REF>HU-<documentnumber>, where <REF> is replaced by three characters as set forth below:

- “PAS” for a passport number
- “IDC” for a personal identification card or driving license number
- “TIN” for a tax identification number

In the case of individual identification systems, the Service Provider uses the standard format, where <REF> is replaced by a series of characters in the format “XX:”, where “XX” is the two-character designation of the national or EU identification schema.
If the serialnumber field is filled out on the basis of other than the above documents, there is no formal requirement, with the exception of the special cases discussed.

3.1.3. Pseudonyms

The Service Provider does’t issue pseudonym certificates.

3.1.4. Rules for interpreting various name forms

The contents of the present document are applicable to the interpretation of identifiers (see especially Chapter 7). The Issuer and Subject Distinguished Name fields shall be interpreted in accordance with standard X.500 and the ASN.1 syntax (see RFC 2253 and RFC 2616).
The certificates issued by the Service Provider to natural persons do not aim to provide for the identification of the person indicated as the Subject on the basis of the data included in the certificate. Certificates issued to natural persons that also include an organization do not aim to certify the relationship between the natural person and the organization or the natural person’s right of representation,unless an indication expressly to this effect is used, which indication detailed in the Practice Statement.
If the Relying Parties require help with the interpretation of any data included in the certificate, they can also contact the Service Provider directly. In such case, the Service Provider may not provide additional information on the Client’s other data (unless required by relevant legislation) and can only provide information that help in the interpretation of the data included in the Certificate.

3.1.5. Uniqueness of names

All Subjects in the Service Provider’s certificate repository shall have unique names (Subject field) to ensure they can be unequivocally identified. In the interest of the above, the Service Provider has to provide all persons with a unique subject identifier (OID-based permanentID) in its registry; the Service Provider is obligated to include this identifier in the certificate’s Subject/Serialnumber field (if the Subject is a person). This identifier is used as a unique identifier of the natural person included in the certificate or, in lack of such, the legal person included in the certificate; however, one client can have more than one identifier. This identifier may never be assigned to another natural or legal person.

In addition, the Service Provider may also include another individual identifier (e.g. personal identification card number, tax identification number, organisational ID) in another Subject/Serialnumber field (see point 3.1.2.).

3.1.6. Recognition, authentication, and role of trademarks

The DBA or Trademark or product name and product identifier owned by the Client can also be included in certificates issued to legal persons. This can be included in the Subject/CN field or the subjectAltName/dirname field.
See Chapter 3.2.2 for the requirements pertaining to checking these data.

3.2. Initial identity validation

The client registration (identity validation and certification) procedures related to the issuance of the end user qualified certificates, which procedures are detailed in the Practice Statement, shall comply with Section 82 of Electronic Administration Act (Eüt).

If the Service Provider has not yet checked the following or the previous check no longer ensures suitable security, the present initial authentication procedure shall include a check of the following:

1. the identity of the Applicant, and, if different from the above, the representative or principal of the Subscriber (see point 3.2.3);
2. the authorisation of the Applicant, and the authorisation of the Subscriber's principal to provide representation/authorisation (see point 3.2.5);
3. the veracity, validity, and rightful use of the data that the Applicant, as the Subject of the certificate, wishes to indicate, and
4. the data pertaining to the Applicant (as the End-User) and the Subscriber that it wishes to store (see points 3.2.2, 3.2.3, and 3.2.5);
5. and the possession of the private key paired to the public key to be included in the certificate (see point 3.2.1).

To points 1-5: The Service Provider shall use certified and valid official documents and/or reliable data sources for the check, which shall provide suitable security in certifying the veracity and validity of the data.
To point 3: If the Subject of the certificate is not a natural person, the Service Provider shall check at least the Subject's full name and unique identifier as set out in the certificate. If the Subject of the certificate is a person registered in Hungary, the Service Provider shall check the veracity and validity of the above data on the basis of authentic records or, in absence of such, of the public document certifying the record.
The Service Provider is obligated to check the data to be included in the certificate, thus especially:

- the identity of the (natural and/or legal) person indicated as being the Subject,
- the veracity of the identification data used to establish identity and - if available - their conformity to the data in authentic records or other reliable central registries,
- the authorisation of the Applicant to proceed,
- the existence of the right of representation to be included in the certificate (based on relevant legislation, authentic records, an instrument of incorporation, or, in absence of the above, an authorisation),
- the right of disposition over the address range (domain) certified by the certificate,
- the right of disposition over the IP address to be included in the certificate,
- the existence of the organizational unit to be included in the certificate,

- if the regulated profession to be included in the certificate is named, the authorisation to practice the profession.

Before the Service Provider starts using any data source as a reliable data source, it shall be evaluated as regards reliability, accuracy, and resistance to change and falsification. During the evaluation, the Service Provider shall take the following into account:

1. The date of the provided information,
2. The frequency of updates to the information source,
3. The purpose of the data provider and data collection,
4. The public accessibility of the data,
5. The relative difficulty of falsifying or changing the data.

The database maintained by the Service Provider (or its owner or subsidiary) does not qualify as a reliable data source if its primary purpose is to collect information to meet the present authentication requirements.

The practice statement to be prepared on the basis of the present Service Policy shall include all practical rules, which ensure the operation compliant with the expectations detailed in the present Chapter 3.2, and under which the organizational Units of the Service Provider may establish their own internal rules of operation.

3.2.1. Method to prove possession of private key

Prior to the issuance of the end user certificate the Service Provider shall ensure, and shall check that the Applicant (End User) in fact possesses and controls the private key of the key pair generated for the certificate in the course of the application. The mean thereof shall be set out by the Service Provider in the practice statement.

In case the private key of the end user is generated and managed by a third party, Service Provider shall ensure that the private key of the certificate to be issued by using its public key is in fact managed by the third party indicated by the Applicant, and is under the exclusive control of the Subscriber, and the key management procedure is compliant with the requirements set out in the present Service Policy, and with other rules and regulations set out in the practice statement based on the present Service Policy.

If the Service Provider did not generate the end-user key pair, the Service Provider has to verify that the private key paired to the public key it was provided with is in the possession of the Client.

Service Provider shall ensure that the generation of the private key of the QSCD-based certificates issued by the Service Provider (QCP-n-qscd és QCP-l-qscd) shall take place on a qualified client device (QSCD).

If the Service Provider generated the end-user key pair, the Service Provider has to identify the Receiver of the private key and has to establish its authorisation to receive the key (see point 3.2.3). The handover shall be documented.

3.2.2. Authentication of organization identity

If the certificate includes an organization (in the CN, O, OU, or any other field), the respective data shall be identified and checked, with especial regard to the name and address to be indicated in the certificate. The Applicant has to have the right to proceed on behalf of the organization (see point 3.2.5).

If possible, an authentic database shall be used to check the organization’s data. If the database is not accessible, another regularly updated and reliable database may also be used, or the

person's registered address is to be contacted. A bank statement, public utility bill, official tax document, or other document can be used to check the address.
If the name or identifier of an asset, system, or product, a DBA / Trademark, or other unique name is indicated as the Subject of the certificate (independently or with a natural or legal person), it has to be ascertained that, in addition to that set out in point 3.2, the Client is in rightful possession of the name and identifier and that these are not misleading (if these conditions are applicable). The check has to be based on an official document, reliable data source, or discussions with the official body that manages the identifier, if any of the above are available.

Identification of organizations in the case of governmental certificates

In the case of public administration certificates, the Provider shall request from the Applicant The data to be included in the certificate and required for the clear identification of the government body that performs administrative tasks and is requesting the registration and of the device paired to the electronic seal used for administrative purposes has to be provided, including the contact information for the person responsible for communication at the government body providing the administrative service.

3.2.3. Authentication of individual identity

The following methods can be used to check the identity of the Applicant:

a. Verification of the identity of the Applicant

If the certificate includes the identification data of a natural person, or natural person requests certificate for a legal person, the natural persons identification shall be verified with the following methods.

1. the presence of the natural person; or
2. remotely, using electronic identification means, for which the physical presence of the natural person was ensured and which meets the requirements set out in Article 8 of eIDAS with regard to the assurance levels 'substantial' or 'high' and the device described in the Practice Statement; or
3. with a certificate issued with a QCP electronic signature or qualified electronic seal in compliance with the above (The provider keeps the right to decide the limits, which certificate is acceptable or not); or]
4. by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence, the equivalence of which is certified by a conformity assessment body and method of use described in the Practice Statement

During the checking of the Applicant's identity:

- in the case of natural persons subject to the Records Act, official identification suitable for certifying identity as defined by the Records Act shall be used, and both its validity and the correctness of its data shall be checked against the official authentic records;
- in the case of natural persons who are not subject to the scope of the Records Act, personal identity is primarily to be checked on the basis of the travel documents defined by the Free Movement Act and the Third-Country Nationals Act, and the validity (authenticity) of the document and the conformity of the data included therein to the central registry are also to be checked. If such records are unavailable, is inaccessible to the Service Provider, or the price for access and performing the check is disproportionately high, the Service Provider

will record this fact and may decide on the basis of other evidence available to it on whether to issue the given certificate to the Client.

b. Validation of the identity of the representative, agent of Subscriber

Service Provider shall also validate the identity of the representative(s) of Subscriber or the agent(s) of the representative(s). In this case no personal meeting is needed for the validation of the identity. Service Provider shall validate the identity of the representative or agent on the basis of reliable data sources.
In case Applicant and Subscriber are the same person, Service Provider does not carry out a separate validation as to the identity of the Subscriber.

c. Validation of the identity of the Recipient

If the Receiver and the Applicant are different persons or if the Application and Receipt take place at different times, the Service Provider also has to identify the Receiver and has to check its right of receipt. If the receipt takes place in person or via traditional methods of delivery, an official certificate suitable for certifying identity shall be used, and authorisation shall be established on the basis of the Applicant's/Subscriber's authentic provisions. If delivery takes place by electronic means, a method is required that is suited to the certificate class, to the identification level required for the Applicant, and that can be traced back to the latter.

d. Further requirements of the validation of the identity of the natural persons

If the certificate includes a natural or legal person, the data to be indicated in the certificate shall be determined on the basis of the data included in the authentic documents and records used for personal identification. Furthermore, the Service Provider has to determine the Applicant's and the Subscriber's data as stored in its own records, with especial regard to the personal identification data (e.g. name, place and date of birth, mother's maiden name).
If the natural person is included in the certificate together with an organization, authentic certification of the representative-agent of the organizationis required for the natural person to be included.
The Subscriber and the Applicant have to acknowledge the trueness of the data they provided by providing their (handwritten or electronic) signatures. The Service Provider may limit the scope of electronic signatures and seals it accepts.
The Service Provider does not have to indicate a natural or legal person as the Subject of the test certificate (if the contents of the certificate unequivocally indicate that it is a test certificate); the checking of such (non-existent) Subjects is therefore obviously not an expectation.
The Service Provider has to document (by recording the hard-copy or electronic evidence) the identification of the Applicant's, Receiver's, and Subscriber's representative, the information used to verify the data (e.g. types of documents, their identification numbers, validity), and the data necessary for contacting the Subscriber (e.g. postal address, phone number). The Service Provider is not authorised to store any other information that is not required for identification and contacting the Subscriber and the Applicant (see Chapters 9.3 and 9.4 for data management).
During the term of the Service Agreement Service Provider is not obliged to re-validate the identity of the representative/agent of the Applicant and the Subscriber. In case Applicant requests the issuance of another certificate during this time interval, Service Provider shall accept the result of the former validations in relation to the new application, as well. Nevertheless, in this case Service

Provider shall validate the accuracy and veracity of the details of Applicant and Subscriber set out in the application and to be included in the certificate.
In the case of an application for the issuance of a certificate during the term of the service agreement, Service Provider may verify the accuracy and veracity of the details of Applicant and Subscriber set out in the application and to be included in the certificate on the basis of the data stored in the own database of Service Provider, the credibility of which is based on the validation of the data based on authentic or public instruments prior to the execution of the prevailing service agreement.
In the practice statement Service Provider shall set out in detail the methods of identity and data validation methods used by Service Provider, as well as the process of the validation procedures.
In the practice statement Service Provider shall set out in detail the process of the validation procedure, and shall, in the course of the registration, allow the administrator issuing the certificate to supervise the validation of the veracity and accuracy of the data under the present Chapter and the result thereof before the approval the issuance of the certificate. The approval of the issuance of the certificate shall be carried out only by a person, who has not participated in the validation of the veracity and accuracy of the data and the validation of the identity of the Applicant in the course of the registration process (see Clause 5.2.4).

3.2.4. Non-verified subscriber information

Only such data may be indicated as the Subject of the certificate issued by the Service Provider that the Service Provider has verified, or about the authenticity of which the Applicant or Subscriber has provided a written statement in full knowledge of their liability under criminal law.

3.2.5. Control of eligibilities and delegation

If the Subscriber is proceeding by way of a representative or its delegate at the Service Provider (e.g. as an Applicant or Receiver), the Service Provider always has to unequivocally verify the identity of the representative/delegate (see 3.2.3) and has to check the authorisation of the person to proceed at the Service Provider on behalf of the Subscriber for the given certificate enrolment or status change procedure.
The right of representation shall be verified with the use of an authentic document or reliable database.
The identity of the principal and the authenticity and validity of the authorisation also have to be verified (see also points 3.2.2 and 3.2.3).
In its practice statement the Service Provider shall set out in detail the procedure of the validation.
In its practice statement the Service Provider shall enable the legal person Subscriber to appoint one or more administrator(s) within its organization, who are entitled to submit applications related to the organization of the Subscriber and to act on behalf of the Subscriber in relation to such applications for certificates, in the course of the execution of the service agreement, the acceptance, approval and management of the certificate issued (status change, renewal, modification etc.). The administrator may be appointed by a person entitled to represent the Subscriber.

Validation of rights and powers in the case of website authentication certificates (QCP-w and EVCP)

If the Subject (Subject or SAN field) of the certificate is a domain name or IP address, the Service Provider has to verify also that the Subscriber has rights over the domain name / IP address.

The Provider must not issue certificate for domain name contains any wildcards,
If the Subscriber does not have exclusive control over the domain name, the certificate can only be issued if all owners have granted their consent.

3.2.6. Criteria for interoperation

During the provision of services, the Service Provider may cooperate with other Service Providers, who will acknowledge the requirements of the present Trust Service Policy as binding upon themselves.
The Service Provider has to disclose all cross-certified certificates that it is the Subject or issuer of.

3.3 Identification and authentication for managing certificates

In case of proceedings that result in the issuance of a new certificate, the Service Provider has to perform identification in accordance with the initial identity validation described in Chapter 3.2. If the procedure has already been conducted at an earlier time

- as regards the identification of the Applicant, Subscriber, and Receiver, and
- as regards the Applicant's and the Receiver's right to proceed,
- for establishing the identity of the Subscriber's representative or principal,
- in order to verify the data indicated as the Subject of the certificate and stored in the Service Provider's records, and
- as regards the possession of the private key,

then the Service Provider is only obligated to repeat these procedures in accordance with the initial identity validation if the previous process is no longer valid or reliable, or if the previous Applicant, Subscriber, Receiver, or Subject data have changed.
The repeated verification process can take the form of a method different than that used for initial identity validation or can extend to only a part thereof (if only certain data of the affected individual have to be confirmed, e.g. due to the expiration of the validity of certain documents).
If the application contains a new signatory or seal public key, the provisions set out in 3.2.1 shall be kept.
For managing website authentication certificates (QCP-w and EVCP) the identification and authentication procedures should be repeated, if the last procedure was earlier than 13 months.

3.3.1. Identification and authentication if the certificate is valid

No stipulations.

3.3.2. Identification and authentication if the certificate is invalid

The Service Provider may not accept any applications to be authenticated with an invalid certificate.

3.4. Identification and authentication for status change request

The Service Provider shall receive and process the requests for the change of the status of the certificates issued by Service Provider, as well as the notifications related to the events that entail

the revocation of certificates (e.g. compromising or corruption of the private key; incorrect use of the certificate or other misuse of the certificate or its keys).
Service Provider shall ensure that it accepts status change requests only submitted by persons entitled to do so. To this end, Service Provider shall validate the identity of the applicant requesting the status change and shall establish whether the applicant is entiteled to request the change of the status of the subject certificate or not. Service Provider shall validate the identity of the Applicant at least with a password or by automatized authentication within the IT system of Service Provider with the submission of the user name and password.
Service Provider shall furthermore ensure that it will process and fulfil the requests as soon as possible (preferably before processing other service requests).
In the case of electronically certified applications for revocation or suspension, Service Provider shall not accept the application certified with the private key of the certificate subject to the application for revocation or suspension.
In case of procedures that change the certificate status but do not result in the issuance of a new certificate, the Service Provider has to identify the Applicant and has to ascertain its authorisation for the given action. The Applicant shall be identified with the use of at least a code word or by way of automatic identification in the Service Provider's IT system, which requires its user name and password.
The circumstances, terms and conditions of submitting the applications for status change shall be set out in the practice statement.

4 Certificate life-cycle requirements

The present chapter 4 of the Service Policy sets forth the requirements related to the application for, and issuance of, certificates, and to other operations that may be carried out within the lifecycle of the certificate. In its practice statement the Service Provider shall set out in detail the processes that ensure that the services enabling the management of the certificates meet the above requirements.

4.1 Certificate application

The Applicant has to submit a certificate application to the Service Provider in order to be issued a new certificate. Based on the certificate application, the Service Provider shall prepare the service agreement to be concluded with the Applicant and the Subscriber, which the latter shall certify with its own signature or that of its representative and then send to the Service Provider. The agreement shall include the Applicant's and Subscriber's statement pertaining to the fact that they have familiarized themselves with their obligations and undertake to keep those.
The Service Provider is obligated to keep the agreement together with the data pertaining to the certificate.
If the service agreement is drawn up in an electronic format, the Client shall provide it with at least an advanced electronic signature / seal.
Prior to the conclusion of the service agreement, the Service Provider has to provide the Applicant with comprehensive information on whether the service is qualified, on the exact contractual conditions pertaining to the use of the services, including any restrictions application to use, on the terms and conditions regarding the use of the certificate, and on applicable legislation. The Service Provider has to publish the above information and the related documents on its website in a format affixed with an electronical signature; at minimum after the conclusion of the

agreement, the service agreement, Trust Service Policy, and the Trust Service Practice Statement have to be made available on a durable medium.

4.1.1 Who can submit a certificate application

Certificate applications can be submitted by natural person Applicants on behalf of themselves or of a legal person Subscriber, if granted authorisation.
The Service Provider may manage a risk list of the persons for whom it registers a risk related to certificate application, and may also use external data sources for its risk assessment. Based on the risk assessment, the Service Provider can reject the certificate application.
In the case of managed SCD service the registration of the End Users and the application for the NL Sign signature service may also take place together with the appropriate procedures pertaining to the certificate service provision, respectively (see Chapter 4).

4.1.2 Enrollment process and responsibilities

The Service Provider has to apply the method set out in Chapter 3 to verify the Applicant's identity, right to proceed, and the veracity of the data included in the Application.
The Applicant and the Client shall provide all information necessary for performing the identification and verification procedures. The Service Provider shall include in its records all information pertaining to the identity of the Applicant and the Client and that are required for the provision of the service and for communication; the records are also to include the service agreement.
The data recorded as above shall be retained for at least the time required by relevant legislation.
The service agreement has to include the following statements on behalf of the Applicant:

- the data provided in the certificate application are true and accurate;
- it grants its consent for the publication of the Certificate;
- it is the authorized user of the data indicated in the Certificate and such data do not infringe the rights of others.

Request for web authentication certificates (QCP-w and EVCP)
The certificate application has to include at least an FQDN or IP address that is to be included in the certificate's Subject/CommonName field and the subjectAltName extension.

4.2 Certificate application processing

4.2.1. Performing identification and authentication functions

See Chapter 3.2.
The identification and authentication functions can be performed by the Registration Authority of the Service Provider proceeding in representation of the Service Provider and in accordance with the Service Provider's Practice Statement .
The Service Provider has to provide reliable identification of Registration Administrators.
The certificate application has to include all Subject information included in the certificate, as well as all additional information that the Service Provider requires for the issuance of the certificate in accordance with its Regulations. If the certificate application does not include all the required information, the Service Provider has to acquire the missing data from the Applicant or from an independent reliable source, which is then to be confirmed by the Applicant.

The Service Provider has to have a documented process to regulate the verification of the data to be included in the certificate, the identification of high-risk certificate applications, and the rules applicable to supplemental verification procedures.

4.2.2. Approval or rejection of certificate applications

The Service Provider has to reject any Certificate applications if it is unable to comprehensively verify their compliance.
The Service Provider has the power to pass a decision on denying the issuance of a Certificate being applied for; the Service Provider does not need to provide justification but has to inform the Applicant.
In order to avoid the conflict of interest, Service Provider is obliged to ensure its personal and organizational independence from the Subscribers. No conflict of interest arises if Service Provider issues certificates for its own employees, agents or partners.
In the case of managed SCD, the End User shall approve the application for the issuance of a certificate. Service Provider shall forward the public key to the certification service that the link to the respective registration data shall be provided and that the key shall not be altered. Within the framework of the signature service, Service Provider shall clearly link the certificate made on the basis of the public key to the end user data, after validating that these data belong to the end user.

Acceptance or refusal of applications for the issuance of website authentication certificates (QCP-w and EVCP)

Additionaly the Service Provider has to reject any Certificate applications that belong to gTLDs that are in the consideration phase at the ICANN, and the ones that belong to internal IP addresses.

4.2.3. Time to process certificate applications

In its Service Practice Statement , the Service Provider has to define the deadline by which it undertakes the processing of approved Certificate applications.

4.3 Certificate issuance

The Service Provider can only issue a certificate after the approval of the Certificate application. The certification issuance process shall be connected to the registration, application, and lifecycle management procedures, which includes the use of the public key generated by the Client or the Service Provider, in a secure manner. The issued Certificate may only include the data provided in the Certificate application and verified by the Service Provider during the evaluation process. In the case of certificates that certify a right of representation, the Service Provider informs the representative in writing.
Certificate issuance by the Root CA
Certificates can only be issued by the Root CA under the control of the Service Provider employees granted authorisation by the Service Practice Statement.

4.3.1. TSP actions during certificate issuance

The TSP has to ensure the security of certificate issuance in order to prevent the falsification of certificates.

Service Provider shall ensure that the processing of the applications for the issuance of certificates, as well as the issuance of certificates shall be carried out by different persons.
A natural person authorised by the Service Provider shall initiate the issuance of certificates by the Root CA.

4.3.2. Notification by the TSP of issuance of certificate

The TSP shall inform the End-User on the issuance of the Certificate at the email address indicated in the certificate or registered separately, and shall make the Certificate available for recovery.

4.4 Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The contents of the certificates issued by the TSP have to be checked by the Client, and those have to be accepted prior to first use. The Client has to reject any faulty certificates - by providing suitable justification - and its use (and the use of the connected private key) cannot be commenced. Acceptance can take place both directly and indirectly.

4.4.2. Publication of the certificate by the TSP

If the Subscriber or Applicant grants its consent, the TSP is obligated to make the issued certificate public by way of the public certificate repository.

4.4.3. Notification of certificate issuance by the TSP to other entities

In case the issued signature certificate also certifies signatory right (i.e. right of representation), the contact person of the Subscriber shall also be notified of the fact of the issuance without any delay.

4.5 Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The End-User

- may only use its private key belonging to the certificate for the purposes indicated in the certificate (in accordance with the fields “key use” and “extended key use”).
- The private key of the certificate issued to a natural person (QCP-n and QCP-n-qscd) can only be used for electronic signatures.
- The private key of the certificate issued to a legal person (QCP-l and QCP-l-qscd) can only be used for electronic seals.
- The private key generated in a Cryptographic device (SCD) can only be used in a Cryptographic device
- The private key generated in QSCD (QCP-n-qscd and QCP-l-qscd) can only be used in a QSCD.
- controls the use of the seal private key and maintains sole control of the signature private key;

- may not use a private key belonging to an expired, revoked, or suspended certificate;
- is obligated to provide for the suitable protection of its private key and the activating data to prevent their unauthorised use;
- if it makes a copy of the private key, it shall handle the copy with the same level of diligence as the original copy;
- it informs the Service Provider immediately if any of the following events transpire prior to the expiration of the certificate, and shall immediately terminate the use of the private key, with the exception of data decryption;
    - the loss or theft of the private key, or if the private key becomes compromised,
    - the loss of sole control over the private key, e.g. due to the activating data becoming compromised,
    - the inaccuracy of or a change to the data included in the certificate;
- shall terminate the use of the private key and the certificate if the Service Provider's key becomes compromised;
- irrevocably deletes the private key and copies of it at the end of the validity of the certificate belonging to the private key or if such certificate is revoked.

The private key shall be under the sole control of the End-User.
The restrictions set out in Chapter 1.4 shall be applied during the course of use.

4.5.2. Relying Party public key and certificate usage

In the Service Practice Statement, the Service Provider has to publish those procedures and conditions on which the Relying Parties can rely on in the certificates.

4.6 Certificate renewal

In the interest of the simplified issuance of certificates, the Service Provider has to offer certificate renewal services.
The Service Provider has the power to renew the certificate at its own discretion, and the process can also be initiated by the Client. The Client is authorised to request the renewal of its certificate if the certificate will expire within 30 days.

4.6.1. Circumstance for certificate renewal

The procedure, if requested by the Client, is a process that starts with the request for the procedure being received by the Service Provider and ends with the issuance of a new end-user certificate or, if the application is incorrect, with the rejection of the application.
If the Service Provider issues the new certificate according to different regulations or with a different CA as compared to the original certificate, it has to implement measures to ensure that the newly issued certificate also meets all new or more stringent requirements.
When issuing the renewed certificate, the Service Provider has to proceed in the manner applied at the time of the initial certificate issuance when creating and publishing the Certificate and when notifying the Client and the Relying Parties.
Following the issuance of the new certificate, the Service Provider can revoke the original certificate and can suspend the original certificate for the duration of the procedure.

4.6.2. Who may request renewal

Certificate renewal may be requested by submitting a Certificate application to the Service Provider. Those persons are authorised to apply for a renewal who are authorised to initially apply for a certificate. Prior to fulfilling the application, the Applicant shall be identified in accordance with the contents of Chapter 3.3, and information shall be provided regarding the terms and conditions pertaining to the use of the Certificate, which the Applicant shall accept.
In the application for renewing the certificate, the Applicant shall declare that the data included in the Certificate are still valid.

4.6.3. Processing certificate renewal requests

When processing the Certificate application submitted by the Client, the Service Provider has to verify that:

- the submitted application is authentic (in the case of applications with electronic signatures, that the signature is valid);
- the Applicant is authorised to submit the application in representation of the Subscriber (unless the application is signed with the private key belonging to the certificate in question);
- the application is complete (all required data have been filled out) and does not contain errors;
- the certificate in question can be unequivocally identified;
- based on the currently available information, the cryptographic algorithms used during the planned term of validity of the Certificate to be issued will be in use;
- the Certificate is still valid (it is not expired, suspended, or revoked);
- the private key belonging to the certificate has not been compromised (client statement);
- the documents used to verify the data during the course of the certificate application are still valid;
- the service agreement is still valid;
- the process is executable.

If the above conditions are not met, the Service Provider will reject the application and the Client can apply for a new certificate in an initial certificate application procedure.
The Service Provider may limit the number of times a given certificate can be renewed and can also set additional requirements as conditions for renewal.

4.6.4. Notification of new certificate issuance to subscriber

Chapter 4.3.2 is applicable.

4.6.5. Conduct constituting acceptance of a renewal certificate

Chapter 4.4.1 is applicable.

4.6.6. Publication of the renewal certificate by the TSP

Chapter 4.4.2 is applicable.

4.6.7. Notification of certificate issuance by the TSP to other entities

Chapter 4.4.3 is applicable.

4.7 Certificate re-key

The Service Provider shall offer a Re-key service within the validity period of certificates in the interest of ensuring their use.
The Service Provider has the power to re-key at its own discretion, and the process can also be initiated by the Client without any need for justification. The Service Provider shall initiate a re-key ex officio if the public key included in the certificate does not meet the requirements of relevant legislation, governing standard descriptions, or the applicable decision of the Supervisory Body.
Re-keys are possible for both valid and invalid (e.g. revoked due to a compromised key) Certificates.
In the new Certificate issued during the re-key, the data in addition to the End-User's public key will also be changed (e.g. certificate serial number and start of validity) and can be changed (e.g. certain Service Provider data, such as CRL and OCSP references, or the Service Provider's key used to sign the Certificate); however, the Client may not request any changes other than the key.
See Chapter 5.6 for information on the replacement of Service Provider keys.

4.7.1. Circumstance for certificate re-key

Chapter 4.6.1 is applicable.

4.7.2. Who may request certification of a new public key

Chapter 4.6.2 is applicable.

4.7.3. Processing certificate re-keying requests

Chapter 4.6.3 is applicable, with the difference that the given certificate does not have to be valid and its private key does not have to be uncompromised (except if it was used to sign the application).
If, during the re-key process, the Service Provider found out that the key has been compromised, it has to implement measures for its revocation and will then evaluate the application accordingly.

4.7.4. Notification of new certificate issuance to subscriber

Chapter 4.6.4 is applicable.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Chapter 4.6.5 is applicable.

4.7.6. Publication of the re-keyed certificate by the TSP

Chapter 4.6.6 is applicable.

4.7.7. Notification of certificate issuance by the TSP to other entities

Chapter 4.6.7 is applicable.

4.8 Certificate modification

In the interest of ensuring that the data contents of certificates continuously remain authentic and applicable, the Service Provider has to offer certificate modification services.
The Service Provider has the power to modify the certificate at its own discretion, and the process can also be initiated by the Client.
The Service Provider has to initiate the modification of the Certificate if it comes to know of any changes to the data included in the Certificate, including data pertaining to itself or any other data (e.g. as a result of a change in relevant legislation, standards, or policy). The Service Provider is authorised to modify end-user certificates if the Service Provider signature key used for the issuance of the Certificate has to be replaced.
The Client can request a Certificate modification if its data included in the certificate have been changed.

4.8.1. Circumstance for certificate modification

Chapter 4.6.1 is applicable.

4.8.2. Who may request certificate modification

Chapter 4.6.2 is applicable, with the difference that the statement that the Subject data are unchanged obviously does not apply to the modified data.

4.8.3. Processing certificate modification requests

Chapter 4.6.3 is applicable.
During the course of verifying the Subject data, the Service Provider shall proceed in accordance with the Initial identity validation procedure set out in Chapter 3.2.

4.8.4. Notification of new certificate issuance to subscriber

Chapter 4.6.4 is applicable.

4.8.5. Conduct constituting acceptance of modified certificate

Chapter 4.6.5 is applicable.

4.8.6. Publication of the modified certificate by the TSP

Chapter 4.6.6 is applicable.

4.8.7. Notification of certificate issuance by the TSP to other entities

Chapter 4.6.7 is applicable.

4.9 Certificate status change

The Service Provider has to offer status change (certificate revocation, suspension, and activation) services in the interest of managing the validity of the certificates it issued. The Service Provider has the power to perform these actions at its own discretion, and the process can also be initiated

by the Client, the Court, or the authorities. The Service Provider has to provide non-stop (24/7) customer service for receiving Client requests.
The Service Provider has to ensure that authorised third parties can interpret the data included in the registry of revoked and suspended certificates.
Certificate suspension and activation services cannot be provided in the case of certificates for website authentication. (QCP-w and EVCP)
]

4.9.1 Circumstances for revocation and suspension

The following circumstances can lead to the revocation or suspension of end-user certificates. In the following cases, the Service Provider has to revoke or suspend the certificate within 24 hours of having received the Application:

- a proper application filed by the Client (Status change client request);
- the Client indicates to the Service Provider that the original certificate application was unauthorised and it does not grant authorisation subsequently, either;
- the Client fails to keep its obligations;
- a third party has reported finding a client device;
- other conditions imposed by the Service Practice Statement and the General Terms and Conditions;
- the private key paired to the public key included in the certificate has been compromised;
- the Service Provider’s private key used to authenticate the certificate has been compromised;
- the renewal, modification, or re-key of the certificate;
- unauthorised use of a name or data;
- the data included in the certificate were recorded incorrectly or are untrue, have changed, or are misleading;
- the Client did not request the activation of the certificate within the suspension period;
- the certificate was used in bad faith;
- a final and enforceable decision has been issued to this effect by a Court or other authority;
- based on the governing professional recommendations, the certificate’s technical parameters pose too great a risk for any of the parties (e.g. inadequate key length);
- the service agreement is violated or terminated;
- the certificate was not issued in accordance with applicable policy;
- the Service Provider discovered that the Client is not authorised to use any of the names (e.g. FQDN) included in the certificate;
- the Service Provider discovered that the right of representation indicated in the certificate has been terminated;
- the information services for the validity of the certificate are no longer maintained;
- the trust service has been terminated, unless if the Service Provider has previously provided for the maintenance of the CRL and OCSP services in respect of the certificates it issued;
- required by law.

The possible reasons for suspending a certificate:

- an initial suspension following the issuance of the certificate in order to increase the security of delivery;
- a justified presumption that any of the conditions resulting for the revocation of the

certificate is applicable.

The Service Provider is obligated to take measures to revoke the Service Provider's certificate within 7 days if:

- properly requested in writing by the Certification Authority (in case of an external CA);
- the Certification Authority indicates to the Service Provider that the original certificate application was not authentic and it does not authenticate or authorise the application subsequently (in case of an external CA);
- the private key paired to the public key included in the certificate has been compromised;
- the Service Provider's private key used to authenticate the certificate has been compromised;
- the certificate was used in bad faith;
- the data included in the certificate were recorded incorrectly or are untrue, have changed, or are misleading;
- the information services for the validity of the certificate are no longer maintained;
- based on the governing professional recommendations, the certificate's technical parameters pose too great a risk for any of the parties (e.g. inadequate key length);
- a final and enforceable decision has been issued to this effect by a Court or other authority;
- the trust service is terminated;
- required by law;
- other conditions imposed by the Service Practice Statement.

4.9.2 Who can request status change

The following parties are authorised to submit an application for a certificate status change:

- Client;
- Registration Authority;
- Service Provider;
- in justified cases, any third parties.

4.9.3 Procedure for revocation, suspension and activation

The Service Provider shall provide Clients with the possibility to revoke or suspend end-user certificates. The Service Provider's policies shall include the descriptions for revocation, suspension, and activation, and it shall provide a non-stop (24/7) service for requesting certificate status changes.

The Service Provider has to inform Clients about the method for reporting cases when the private key is compromised, when a certificate is abused, and other types of fraud.

The revocation or suspension can pertain to an end-user certificate or one of the Service Provider's intermediate CAs.

The Service Provider may not revoke or suspend a certificate for the time preceding the notification of the revocation of suspension.

In its Service Practice Statement, the Service Provider provides for the legal consequences of revocation or suspension of the certification prior to the end of its planned validity.

The new status of the certificate has to be recorded in the certificate repository (certificate status database) immediately following the implementation of the measure, thus enabling real-time verification of certificate status. Within no later than 1 hour following the revocation or suspension of an end-user certificate, a new certificate revocation list (CRL) will also be issued, which also includes the changed status of the certificate.

If a private key held by one of the Service Provider's CAs is compromised, the Service Provider should take all reasonable measures to ensure that the Relying Parties are notified. The Service Provider shall publish TSP certificate status changes on its website.

4.9.4 Revocation request grace period

The Service Provider has to start processing applications for certificate status changes immediately after their receipt; they shall be given priority and processed (thus fulfilling applications submitted by authorised persons) before performing any other activities (thus especially the creation or issuance of certificates).
When processing the Certificate status change application submitted by the Client, the Service Provider has to verify that:

- the submitted application is authentic (in the case of applications with electronic signatures, that the signature is valid, except if the application is signed with the private key of the affected certificate);
- the Applicant is authorised to submit the Application on behalf of the Subscriber;
- the application is complete (all required data have been filled out) and does not contain errors;
- the certificate in question can be unequivocally identified;
- the process is executable.

The verification of eligibility for application takes place as outlined in 3.4. Identification and authentication for status change request.
If the above requirements are not met, the Service Provider has to reject the application; otherwise, it has to take measures to revoke, suspend, or activate the certificate without any further consideration.
The Service Provider can also handle the application for revocation by temporarily suspending the certificate in the interest of clarifying the circumstances that led to the revocation.
The Service Provider will inform the Applicant and the Subscriber via email about all executed and rejected applications for suspension, revocation, and certificate activation.

4.9.5 Time within which TSP must process the status change request

Valid certificate revocation applications have to be registered and the certificate's revoked status has to be published within 24 hours of the receipt of the application.

In case of revocation or suspension, the certificate's revoked or suspended status is recorded in the certificate repository without delay following the execution of the application, and a new CRL is also issued no later than 1 hour following the application, which shows the certificate status as

- "onHold" state, if the certificate was suspended;
- the corresponding RFC 5280 revocation reason code, if it was revoked.

In the case of an application for the activation of a suspended certificate, the Service Provider will execute the activation application without delay if it has verified that the circumstances for suspension are no longer applicable; the certificate's valid status will then be recorded in the certificate repository without delay, and a new CRL (which no longer contains the certificate) will also be issued no later than 1 hour following the activation application.

4.9.6 Certificate status checking requirement for Relying Parties

Prior to the acceptance and use of the information included in the Certificate, the Relying Parties have to proceed with the proper level of diligence in order to maintain the security level guaranteed by the Service Provider; it is accordingly especially recommended that they check the validity of Certificates in the Certificate chain in accordance with the applicable technical standards.
This check should include verifying the validity of the Certificates, the conditions of the regulations and for key use, and the verification of the CRL or OCSP-based revocation status information referred to in the various Certificates.

4.9.7 CRL issuance frequency

The Service Provider shall issue a new Certificate Revocation List at least once a day for the CAs that issue end-user Certificates. The validity of Certificate Revocation Lists thus issued cannot exceed 25 hours. Cross-certificates issued by the SP, the CARL should be issued at least every 31 days.
At least once a year, or within 24 hours in the case of a revocation, the Service Provider shall issue a new Certificate Revocation List for its Intermediate CAs. The validity of Certificate Revocation Lists thus issued cannot exceed 12 months.
The CRL has to include the planned date of the issuance of the subsequent CRL; however, the Service Provider can also issue a new CRL prior to this date. The Service Provider has to certify CRLs with its own electronic signature.

4.9.8 Maximum latency for CRLs

The revocation or suspension of the Certificate should appear on the CRL simultaneously to the execution of the application for revocation or suspension.

4.9.9 On-line status checking availability

The Service Provider has to provide a (real-time) Online Certificate Status Service (OCSP) for the verification of the statuses of certificates issued in the framework of trust services.
See Chapter 4.10.

4.9.10 On-line status checking requirements

The OCSP responses provided by the Service Provider have to be in line with the recommendations of RFC 6960 and/or RFC 5019. OCSP responses have to be signed by

- the CA that issued the Certificate to be verified,
  or
- an OCSP responder that issued a certificate signed by the CA that issued the certificate to be verified. (In this case, in accordance with RFC 6960, the certificate used to sign the OCSP has to include an “id-pkix-ocsp-nocheck” extension[5].)

The Service Provider has to support OCSP requests[6] that use the GET method.
The OCSP response issued by the Service Provider can only contain “good” status information for the Certificates signed by the CA and included in the Service Provider’s Certificate repository. An

[5] This extension means that the OCSP responder’s certificate cannot be revoked and therefore its validity does not have to be verified.
[6] See the description of the HTTP (HyperText Transfer Protocol)

OCSP response pertaining to an as-yet unpublished certificate cannot contain “good” status information. The Service Provider has to check OCSP requests in accordance with the requirements set out in Chapter 6.5 Computer security controls.
The OCSP response pertaining to CA certificates that do not meet the requirements of Chapter 7.1.5 Name constraints cannot contain “good” status information.

4.9.11 Other forms of revocation advertisements available

The Service Provider can also publish revocation information in other manners in the framework of certain trust services, if provided for by the present Policy.

4.9.12 Special requirements re-key compromise

The Service Provider has to develop a solution on how to inform its Clients if their private key has become threatened (e.g. if a new vulnerability is uncovered or if established by the Service Provider at its own discretion). If it is not disputed that the key has become compromised, measures shall be taken to revoke the involved Service Provider or end-user certificate without delay.
If a private key is compromised, the certificate for the connected public key shall be suspended or revoked by the Service Provider in accordance with the contents of point 4.9.1 Circumstances for revocation and suspension.
See Chapter 5.7.3. if a Service Provider key has become compromised.

4.9.13 Limits on suspension period

The suspension period cannot exceed 30 calendar days (240 hours). Following the expiration of this time, the Service Provider is authorised to revoke the suspended certificate without providing separate notification. During the suspension period, the Subscriber is authorised to apply for the activation of the certificate (Status change client request).

In the case of web authentication certificates (QCP-w and EVCP) suspension is not supported.

4.10 Certificate status services

The Service Provider has to provide services that enable the checking of the status (valid, suspended, or revoked) of the certificates that it issued.

4.10.1 Operational characteristics

The Service Provider has to inform Relying Parties on the validity of the certificates it issued and on their suspended status. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.
The Service Practice Statement shall include information on the method for accessing validity information, including the possibility for access following the end of a certificate’s validity.
During the management of certificate status services, the Service Provider has to fulfil the following requirements:

- Certificate status information shall be continuously accessible 24/7.
- In the case of any internal or external errors that hinder access to certificate status information, the Service Provider has to take all measures to ensure that the information is accessible within the maximum blackout time indicated in the Service Practice Statement.
- The integrity and authenticity of certificate status information has to be guaranteed.
- Information on revocation has to be included amongst certificate status information for at least the certificate's original validity period.
- Both CRL and certificate status services shall be provided.
- The CRL and OCSP services have to harmonize with each other: the information on a certificate status change has to be available in both of these services.
- Certificate revocation information has to be publicly and internationally accessible.
- For web authentication certificates (QCP-w and EVCP) the revocation list has to be downloadable within 3 seconds with the use of an analogue phone line.[7]]

4.10.2 Service availability

The Service Provider has to ensure the continuous (24/7) availability of the Certificate repository, the Certificate status service, and the Terms and Conditions for revocation management and the use of issued Certificates with at least a 99% level of availability on an annual level. The duration of any single service disruption cannot exceed 24 hours. The response time of certificate status services can be no more than 10 seconds under normal loads.
The Service Provider has to continuously (24/7) be able to provide responses to high priority error reports pertaining to certificates and to forward those to law enforcement authorities as necessary and/or revoke the involved certificate.
[PTC
The response time of CRLs cannot exceed 10 seconds under normal loads.]
[QCP The qualified Service Provider has to provide a 99.9% availability on an annual level for the Certificate repository, the Online Certificate Status Service, and the management of revocations. The duration of any single service disruption cannot exceed three hours.]
See also 4.9.9 On-line status checking availability.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

The same level of security requirements apply to copies of end-user private keys as to the original private key. The number of copies of an end-user private key should not exceed the amount necessary for maintaining the service.

[7] assuming a 20MBit/sec ADSL connection

4.12.1 Key escrow and recovery policy and practices

The Service Provider may not provide key escrow services for the private keys of signature, seal and website authentication certificates.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. Facility, management, and operational controls

The Service Provider has to ensure that it applies physical, procedural, and personnel security safety precautions, including administrative and control procedures that ensure these are validated, that meet the requirements of recognised standards.
The Service Provider shall meet the following requirements:

- It has to have a risk assessment in place that is checked regularly (see point 5.4.8 for details).
- The Service Provider has to have a documented information security policy that is approved by management and regularly maintained, which shall extend to security controls and actions for those of the Service Provider's premises, systems, and information tools that cooperate in the provision of its services. The Service Provider shall have all involved persons and all employees keep its information security policy.
- The Service Provider is liable for adherence to the procedures set forth in the information security policy, even if those are not implemented by the Service Provider's own staff. The Service Provider shall determine the liability of cooperating parties and has to ensure that they follow the required procedures.
- The information security policy and inventory shall be reviewed regularly or whenever significant changes take place, which ensures that they remain continuously applicable, compliant, and successful. All changes that affect security levels shall be approved by the Service Provider's management. The configuration of the Service Provider's systems shall be checked regularly in order to filter out any changes that are in violation of the security requirements.

5.1 Physical controls

The Service Provider shall ensure that physical access to critical services is controlled and that these minimize the physical risk of the tools used for physical services.
The Service Provider shall ensure that the loss of and damages to values are avoided, that values are not compromised, and that operating activities are not disturbed.
The Service Provider has to implement controls that prevent information and information processing systems from being compromised or stolen.

5.1.1 Site location and construction

When constructing the site and managing the security if its environment, the Service Provider has to take into account the recommendations and requirements pertaining to fire and water protection, uninterrupted power supplies, air conditioning, the prevention of physical access, the development of security zones, access to telecommunication networks, and radiation protection.

5.1.2 Physical access

The Service Provider shall provide a clearly defined and physically delineated security zone for the critical components of safe operations; it shall physically protect this zone from intrusion, control access to it, recognize unauthorised access, and set off an alarm as required. All zones that are shared with other organisations or organizational units shall be outside this area. Other activities can be performed within this security zone if they can be performed by the persons authorised to access it.
The physical and environmental safety programs of these critical services shall deal with the regulation of physical access, protection against natural catastrophes, the factors of protection against lightning and fire safety, the faults of support equipment (including electricity and climate control equipment), the collapse of the building, leaky water pipelines, protection against groundwater, protection against theft and breaking and entering, and restoration after catastrophes.
The Service Provider shall put in place security measures

- in order to protect the equipment used to support physical and environment security system resources and their operation;
- to prevent the equipment, information, data medium, or software necessary for electronic signature-related services from being lost, damages, or taken from the premises by unauthorized persons.

The Service Provider will limit physical access to the equipment related to its critical services to individuals with proper authorisation, and will operate such equipment in an environment that provides physical protection to the services that prevent them from being compromised through unauthorised access to the systems or data.
Access to security zones shall be supervised; unauthorised persons may only stay within the zone with the supervision of authorised persons. Entry and exit to the zone shall be logged, including their time and the purpose of access.
Service Provider root keys can be kept separately from normal operations, with access being limited to only trusted employees.

5.1.3 Power and air conditioning

The Service Provider shall use an uninterrupted power supply at the place of service that provides an adequate amount of electricity to the systems for a short interruption of power; in case of a longer blackout, an electric generator shall provide for the continued operation of the systems.
A suitable filtration system shall be used to ensure the cleanliness of the air inducted into the service location, which filters out various pollutants and also provides the Service Provider’s employees with the air they require. The humidity and temperature of the ventilated air has to be set in accordance with the needs of the IT systems.
The performance of the air conditioning system shall provide the cooling required by the IT systems.

5.1.4 Water exposures

The Service Provider’s service locations shall be protected from leaks and floods.

5.1.5 Fire prevention and protection

The Service Provider’s service locations shall be protected from fire.

Fire and smoke detectors as well as manual and automatic fire extinguishers shall be installed that meet the respective fire protection regulations; the location of manual fire extinguishers and escape routes shall be clearly indicated.

5.1.6 Media storage

The Service Provider shall handle its data media safely to avoid damage, theft, unauthorised access, and obsoleteness. The Service Provider shall handle all data media in a secure manner, in accordance with the requirements of the data qualification system. The media shall be protected from becoming obsolete or damaged during the entire term of data storage.
The Service Provider shall dispose of data media that contain sensitive data in a secure manner, if such are no longer necessary. The contents of disposed equipment have to be permanently deleted - with the use of widely accepted methods - or the media has to be irreparably destroyed by other means.
The Service Provider has to have more than one backup copy of critical data, one copy of which shall be stored at an external location outside the service location; the backups shall be provided the same level of protection as the service location.

5.1.7 Waste disposal

In case of disposing of IT tools, the Service Provider has to securely and irrevocably delete the stored data or, if this is not possible, the part containing such elements shall be destroyed in a manner that prevents readability.
When disposing of documents, the suitable measures shall be taken to render documents containing personal data illegible.
Service Provider shall follow Hungarian Act 185 of 2012 and referred Governmental Decree regarding disposed electronic equipment.

5.1.8 Off-site backup

In the interest of providing for the continuity of business and of avoiding data loss, the Service Provider has to make backups and has to ensure that the entirety of the IT system can be restored if necessary. Backups shall be protected from unauthorised changes, deletion, destruction, and unauthorised access. Preparation for extraordinary situations includes the application and testing of plans for specific situations.

The Service Provider can provide for the secure storage of the data by using write-only media, saving backups in a remote location, or concurrently storing those in more than one place.

5.2 Procedural controls

The Service Provider shall ensure that its system operate securely, in accordance with applicable rules, and with a minimal risk of error. In the interest of the above, it has to employ a suitable number of staff with appropriate skills, technical knowledge, and experience.
The service provider has to operate an internal management and control policy, including the connected responsibility system, that is up to date and meets the requirements of relevant legislation and standards. The control activities of an independent system controllers have to ensure that the system operated suitably.

The Service Provider has to have a quality assurance and information security management system in place that is continuously monitored by an external, independent system controller.
The Service Provider has to classify the managed data created during the provision of qualified services into a security class on the basis of the risk assessment defined by relevant legislation and in the Service Practice Statement; it furthermore shall ensure that they are suitably recorded, checked, and protected, and that the required responsibility system is used.
]

5.2.1 Trusted roles

Only those persons can fill trusted roles at the Service Provider for whom it can certify with technical experience, education, and vocational qualifications that they are protected from corruption and have the necessary expertise.
The role that is generally responsible for the IT system has to be filled by a person who has a vocational higher education degree[8] and at least three years of experience in IT security.
The qualified service provider is obligated to employ the person fulfilling a trusted role in the framework of employment; moreover, the person in the trusted role has to be free of all interests that can negatively affect the reliability or security of the qualified service. The qualified Service Provider has to ensure that the person dealing with the provision of qualified services has the required and suitably up-to-date skills and experience. The qualified service provider shall ensure that all trusted roles are filled, and all trusted roles shall be named.

The following are considered trusted roles:

- Security Officer: The person generally responsible for the security of the service.
- System Administrator: The person who installs, configures, and maintains the Service Provider's IT system.
- System Operator: The person performing the tasks pertaining to the continuous operation, backup, and restoration of the Service Provider's IT system.
- Independent System Controller: The person who examines the Service Provider's logged and archived data files and who is responsible for checking adherence to the control measures implemented by the Service Provider in the interest of regular operations, for the ongoing examination of existing procedures, and for monitoring
- Validation Specialist: the person responsible for approving the creation, issuance, revocation, and suspension of certificates

Trusted roles can only be filled by persons employed by the Service Provider after being formally appointed by the Service Provider's upper management. A trusted role cannot be filled on the basis of a contracting agreement.
A current registry shall be kept on trusted roles; in case of any changes, the fact of the change shall be reported without delay to the Supervisory Body.

5.2.2 Number of persons required per task

The Service Provider generates, it's Root and Intermediate CA keys in a hysically protected environment, and also the backup and restore of these keys shall be performed in the physical presence of at least two designated trusted employees with direct authorisation,:

- Saving, and restoring private keys in the caase of NLSIGN service;

[8] A vocational higher education degree means a university degree in mathematics or physics, or a college or university degree in an engineering major of a technical science.

- The generation of the Service Provider's own service key pair.

5.2.3 Identification and authentication for each role

The Service Provider is obligated to personally identify all users of its IT systems and all actors of administrative processes, with the exception of users with read-only authorisation for public data services.
Only authorised persons can access the Service Provider's IT systems. The Service Provider has to provide for the administration of access by system administrators, system operators, and Independent System Controllers, including the management and ad hoc modification of user accounts or the termination of access.
The Service Provider has to have the ability to limit access to the various applications. The system has to be able to differentiate between the various trusted roles, thus especially access by system administrators and system controllers.
Staff has to be identified and authenticated before they are allowed to use applications critical to services, and they shall be held accountable for such activities.

5.2.4 Roles requiring separation of duties

In order to decrease unidentified or unintentional modifications made to the Service Provider's tools and systems and the possibility of other abuse, the Service Provider has to separate the tasks and responsibilities that are exclusive of each other.
In the interest of separating roles

- the Security Officer may not perform the tasks of the Independent System Controller, the System Administrator and the manager generally responsible for the IT system, and
- the Independent System Controller may not perform the tasks of , the System Administrator the manager generally responsible for the IT system.

Qualified service providers shall strive to fully separate the staff in trusted roles. In addition to the above, the following roles also have to be separated:

- the Security Officer may not perform the tasks of the System Administrator, and
- the Independent System Controller may not perform the tasks of the Validation Specialist and the System Administrator.

The Service Provider has to ensure that registration tasks are separated, i.e. the data required for the issuance of certificates should not be validated by the same trusted employee who approves the issuance of the certificate. The control policy should be auditable.

5.3 Personnel controls

The Service Provider has to ensure that its employees and contractual partners support the reliability of its services. The Service Provider's personnel employed in trusted roles have to be free of all conflicts of interests that could infringe upon the impartially of the tasks performed in the course of service provision.
Personnel have to implement administrative and management procedures in line with IT security policies.
The security roles and responsibilities identified in the information security policy have to be documented in job descriptions or other documentation accessible to Relying Parties. Trusted roles shall be clearly defined, have to be filled, and the appointment has to be approved by both the management and the Relying Parties.

Personnel (including permanent and temporary employees) have to have job descriptions that are based on the principle of separating tasks and the principle of least privilege; the trusted nature of the position is based on tasks, access levels, background checks, and the employee's training and knowledgeability.

5.3.1 Qualifications, experience, and clearance requirements

All of the Service Provider's employees have to have the education, practice, clearance, expertise, and experience required for the filling of the respective position. The Service Provider may fill trusted roles with people who have no criminal records, which shall be certified during the hiring process with a Certificate of Good Conduct that is no older than 3 months.
The qualified service provider may fill trusted roles with people whose independence (i.e. exeption from influence) and expertise required for the trust position can be supported by the qualified service provider with experience, qualification and professional qualification.

The position with general responsibility for the information technology system shall be filled by a person, who possesses the specialization in tertiary education set out in Decree no. 24/2016 of the Ministry of Interior, and professional expertise of at least three years gained in relation to information technology security.

Service Provider shall employ the persons in trusted roles within the framework of employment relationship. Service Provider shall, before the commencement of the employment of the person nominated for the trusted role, ensure that the prospective employee is independent of any interest that might adversely affect the reliability and security of the qualified service.

Service Provider shall ensure that the person related to the provision of qualified services has the necessary and properly up-to-date knowledge and experience (see Chapters 5.3.3 and 5.3.4).

Service Provider shall ensure that all all trust positions are filled and that the trust positions shall be enlisted (itemized) in the practice statement.

In the interest of fulfilling its management tasks, the Service Provider's management has to have adequate experience regarding the trust services offered by the Service Provider, IT security, and risk management; in addition, the manager responsible for security has to have the necessary experience in security measures.
The Service Provider has to provide the Validation Specialist with training that provides the skills necessary for filling the position. The Service Provider shall test the knowledge of Validation Specialists as regards the registration requirements set out in the regulations.

The Service Provider is obligated to employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards.

5.3.2 Background check procedures

The Service Provider has to identify the personal identities of persons to be employed in trusted roles (regardless of the contractual relationship) while in their physical presence or by checking photographic personal identification documents. The Service Provider also has to check their clearance, which includes checking the information pertaining to previous employers, relevant

education, and professional references. Persons cannot receive access to the Service Provider's systems before these checks have been performed.

5.3.3 Training requirements

The Service Provider has to make sure that the persons employed in trusted roles have the knowledge necessary for the performance of their tasks. In the interest of the above, they have to take an examination to prove they have the necessary knowledge. Only persons who pass the above examination can receive access to the Service Provider's systems that provide trust services. The exam shall be documented. Prior to the exam, the Service Provider has to support the person in question in gaining the required knowledge to the extent required for the performance of their task. The exam and the training have to extend to the following:

- PKI basic knowledge;
- authentication and control rules and procedures;
- security and data protection rules;
- general threats to information authentication processes (including data fishing and other social engineering tactics);
- the requirements of the present Trust Service Policy, the Service Practice Statement, and other regulations;
- the legal consequences of certain acts;
- the unique features of the Service Provider's IT system and the method for its management;

5.3.4 Retraining frequency and requirements

The Service Provider has to ensure that the person filling the trusted role has the knowledge required for the performance of the respective tasks and shall provide retraining or repeated courses as required. Accordingly, it shall provide retraining if any changes take place in its regulations or IT system that involved the activities of these roles. Personnel have to be informed at least every 12 months on -every collegue about the new threats – in the last 12 months - and current security procedures.
Retraining shall be suitably documented in a manner that makes it possible to determine the topic and participants of the training.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

The Service Provider has to employ suitable disciplinary penalties to the faulty employees or the cooperating natural or legal persons for the unauthorised use of its service systems and for errors, omissions, or damages during the provision of services. The respective agreement concluded with such person shall provide for the sphere of possible sanctions.

5.3.7 Independent contractor requirements

The expectations of these regulations are applicable to persons cooperating as the Service Provider's independent contractors just as to its employees.

5.3.8 Documentation supplied to personnel

The Service Provider shall continuously ensure that the current regulations and documentations necessary for persons participating in the provision of services are available to them.

5.4 Audit logging procedures

[QCP In the interest of providing for the continuity of business, avoiding data loss, presenting evidence during court procedures, and ensuring IT security, the qualified Service Provider has to continuously log all events pertaining to its IT system and the provision of the qualified service, as well as to all substantial information pertaining to the data that it issued or that was issued to it. The log file has to comprehensively cover the entire process of providing the qualified service and has to be suitable for reconstructing all events pertaining to the qualified service, to the extent that is required for evaluating the true state of affairs.
The log file has to include the calendar date and exact time of the logged event, the data required for traceability and reconstructing the event, and name of the user or other person that caused the event.
All records in the log file have to be protected from changes and unauthorised access. The log shall be handled in a manner that excludes the possibility of its destruction, the deletion or modification of its records, and modifying the order of records in any way; such protection should also extend to the period following the termination of the Service Provider's activities. The qualified Service Provider shall prepare backups of the log at regular intervals.
The qualified Service Provider has to ensure that log data are continuously evaluated and controlled.
The Service Provider has to document the method of accessing logged information and the time for which it must be stored.
]
In the case of QSCD based certiticats (QCP-n-qscd and QCP-l-qscd) based certificates the Service Provider has to log the events related to the preparation of QSCD Client devices.
]
The Service Provider has to record and continuously make available for a certain amount of time - even after the termination of its activity - all substantial information, including received and provided data, especially for the purpose of use as evidence in court procedures, as well as for the purpose of ensuring the continuity of services and for conformity assessment.
In addition to log entries, the following also have to be stored

- the date and time of the entry (and, if different, of the event);
- the type of event;
- the successfulness or unsuccessfulness of the execution of the event;
- the identifier of the user or system who/which caused the event.

If any serious anomalies occur in the operations of the logging and log analysis tool, the Service Provider's operations shall be suspended until corrections are made.
The time information logged with the events have to be synchronized at least daily with an authentic time source.

5.4.1 Types of events recorded

The following events have to be stored in the automatically and manually recorded log files:

1. Security events

   a. Changes in security profile
   b. System start-up and shutoff
   c. Firewall and router activities
   d. The method and results of attempts to access the Service Provider's system (successful and unsuccessful)
   e. Entry to and exit from the Service Provider's premises
2. TSP system settings
   a. System installation
   b. System configuration changes (e.g. updates, patches, settings)
   c. Changes in certificate and CRL profiles;
   d. Saves and restores of the system or system data
3. Lifecycle actions of Service Provider and end-user keys
   a. Key generation, making copies, storage, restoration, archiving, and destruction
   b. Lifecycle actions of cryptographic devices
4. Lifecycle actions of certificates
   a. Applications, renewals, re-keys, suspensions, activations, revocations
   b. Check events affecting lifecycle actions
   c. The acceptance and rejection of applications
   d. Issuance of certificates
   e. Generation of revocation lists
5. Events affecting the exact time
   a. Clock synchronization events
   b. Exceeding the required time accuracy threshold
6. Log events
   a. Stopping and restarting the logging system;
   b. Modifying log settings
   c. Archiving/deletion of logging data;
7. User management actions (as regards Service Provider systems)
   a. Adding and deleting users
   b. Allocation and revocation of roles and rights
   c. Status changes (e.g. locks, blocks, permits)
   d. The settings of the required identification method
   e. Replacement of authentication data (e.g. password)
8. Irregular or threatening events
   a. System crashes and hardware errors;
   b. Any errors of software actions;
   c. Software integrity errors;
   d. Attempts at network attacks;
   e. Disturbances in the electrical network;
   f. Uninterruptible power supply errors;
   g. Communication disturbances.

The following information has to be recorded pertaining to client requests and actions regarding certificates:

- The date and exact times of the actions;
- The types and identification data of the presented documents
- The copies of the presented documents and the signed service agreement, or tis's copy and storage location of the copies
- Any changes made by the client to the service (e.g. to the service agreement)

- The identifier of the person processing the Client request
- The method for controlling documents - if more than one method can be used
- The identifiers of the authenticator and registration authority units participating in processing;
- The time of the check and the data of the person contacted as part of the check (e.g. phone number)

5.4.2 Frequency of processing log

The Service Provider has to ensure that the created log files are regularly evaluated. An Independent System Controller with the suitable expertise and rights has to evaluate the log entry within 1 week of its creation. Software tools can also be used for their evaluation.
During the evaluation, the authenticity and integrity of the examined log files have to be ascertained.
During the evaluation, the following have to be analysed:

- the error messages generated by the systems,
- significant changes to the traffic data,
- any exceptional trends that differ from the ordinary,
- suspicious activities.

The fact and results of the evaluation, as well as any uncovered problems and the measures implemented to avert the risks, have to be documented.
The automatic evaluation processes have to alert the personnel when any events are discovered that seem critical from the aspect of security.

5.4.3 Retention period for audit log

The information recorded in the log files have to be kept for the same time as the affected certificates, but for a period of at least 7 years (in the Service Provider’s system or in an archived format).
The logged information has to be made available to the Independent System Controller at any time.]

5.4.4 Protection of audit log

It has to be ensured that the log files and the information stored therein cannot be simply deleted or destroyed. The confidentiality and integrity of the recorded information (also including events that have not yet been archived and that have already been archived) has to be maintained until the end of the retention period. Only authorised persons (primarily Independent System Controllers) may be granted access to log files. In case of a legal procedure, the involved information has to be made available to the persons involved in the proceedings and to authorised persons.

5.4.5 Audit log backup procedures

Log files have to be stored in 2 copies in physically different locations. If the log entry is created in one place, it has to be ensured that a copy be made of it at another location within 24 hours. See *5.1.6 Media storage* and *5.1.8 Off-site backup.*

5.4.6 Audit collection system

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

The Service Provider has to prepare a risk assessment every quater with the help of which

- It identifies foreseeable internal and external threats that can enable the unauthorised access, disclosure, modification, destruction, or other abuse of certificate data or Certificate issuance, management, or status change processes.
- It assesses the probability of these threats actually taking place and the damages that can be expected if they take place.
- It evaluates the suitability of the processes used to prevent the uncovered threats, of protective measures, and of IT systems.

5.5 Records archival

The Service Provider is obligated to keep records of the data pertaining to the various certificates, thus also including personal data (see Chapter 5.5.2 Retention period for archive for the retention period). Together with the retention, the Service Provider is also to provide a tool with which the contents of the issued certificate can be determined.
The Service Provider has to protect all entries in archived data files from unauthorised modification, deletion, destruction, and access. Archived data files stored electronically have to be affixed with at least advanced electronic signatures or seals and with timestamps. The qualified Service Provider shall ensure that for the time that it stores the data, they remain authentic and accessible and interpretable to authorised persons.
]

5.5.1 Types of records archived

The Service Provider has to keep the information - also including information pertaining to generation - pertaining to the various certificates as well as the related personal information. This extends to, e.g.:

- the information and documentation requested and acquired during the certificate application process (4.1 Certificate Application);
- the information disclosed during the certificate status change procedure (4.9.3 Procedure for revocation, suspension and activation);
- the information logged in accordance with the present Trust Service Policy (5.4 Audit logging procedures).

5.5.2 Retention period for archive

The Service Provider is obligated to retain the data archived in relation to the various certificates in accordance with the present Trust Service Policy for the following durations:

- 10 years from the expiration of the certificate;

- In the case of a legal dispute regarding the authenticity or validity of any data included in the certificate, until the legal dispute is closed with a final decision.

The Service Provider is obligated to retain or have retained other logged data for 10 years from their creation and the Service Practice Statement and its amendments for 10 years following their having been repealed.

5.5.3 Protection of archive

The procedure set out in 5.4.4 Protection of audit log shall be followed.

5.5.4 Archive backup procedures

The procedure set out in 5.4.5 Audit log backup procedures shall be followed.

5.5.5 Requirements for timestamping of records

The data to be archived have to be affixed with time data or timestamps.

5.5.6 Archive collection system

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The Service Provider shall replace its key if any TSP certificates expire or if any of the used keys have become obsolete; in addition, it can also decide to implement a key changeover at its own discretion in other cases.
In the case of a new certificate generated with a new key, its profile and data have to be aligned with current regulations and best practices.

5.7 Compromise and disaster recovery

The Service Provider shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services it provides. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.
The Service Provider shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.
Where the breach of security or loss of integrity is likely to adversely affect a natural person or organization to whom the trusted service has been provided, the Service Provider shall also notify the natural person or organization of the breach of security or loss of integrity without undue delay.

5.7.1 Incident and compromise handling procedures

The Service Provider shall continuously monitor the system activities pertaining to logging on to IT systems, to IT system users, and to requests for the provision of services. In doing so, the following factors shall be taken into account:

1. When checking these activities, the sensitivity of the collected and analysed data shall be considered.
2. The Service Provider has to identify and report irregular system activities (including intrusions into the Service Provider's network) that imply potential damages to security.
3. The service provider's IT systems have to check the following events:
    a. the initiation and cessation of logging functions;
    b. the availability and operability of trust services.
4. The Service Provider has to proceed promptly and in a coordinated manner in the interest of responding to the event as quickly as possible and to restrict the effects of security damages. The Service Provider has to identify those alarms and potentially critical events that have to be tracked by trusted employees and about which reports shall be filed in accordance with the internal regulations.
5. The Service Provider will define procedures in the interest of notifying Relying Parties about events that infringe security or integrity and have a significant effect on trust services and the personal data handled therein.
6. The Service Provider addresses any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery. If this is not possible, it will create and put into action a plan with which it can mitigate the threat of the critical vulnerability, and shall also document the facts if the security hole does not require such measures.
7. The Service Provider will enact incident reporting and reaction procedures that allow the damages caused by the security incidents and disruptions to be minimised.

The Service Provider shall have an Incident management and catastrophe recovery plan.
In its business continuity and catastrophe recovery plan, the Service Provider shall document the procedures with which it notifies and, if possible, protects Clients and the Relying Parties in the case of a catastrophe, security compromise, or business failure. The Service Provider is not obligated to disclose its business continuity and catastrophe recovery plan, but shall make such available at the request of the Independent System Controllers. The Service Provider has to test, review, and update these procedures once a year.
The business continuity plan shall contain:

1. The conditions for activating the measures set out in the plan,
2. Emergency procedures,
3. Downtime procedures,
4. Restart procedures,
5. Scheduling the maintenance of the plan,
6. Awareness and training requirements,
7. Individual responsibilities,
8. Recovery time objective (RTO),
9. The regular examination of standby plans,
10. The Service Provider's plans for the maintenance or restoration of its business activities in case of damages to or interruption of its critical business processes,
11. The storage of critical cryptographic devices (keys, key storage tools, activation codes) in the wrong location;
12. Acceptable downtime and recovery times,

13. The frequency of preparing backups of important business information and software,
14. The distance of recovery installations from the primary business location,
15. The procedures aimed at protecting equipment following a catastrophe and before recovery at the original or at a remote location.

5.7.2 Computing resources, software, and/or data are corrupted

The Service Provider's IT systems shall be made of reliable hardware and software components. Redundant system elements shall be used to provide for critical functions in a manner that ensures they can continue operations even if an element becomes faulty.
The Service Provider shall create a backup of the entire system with a frequency that ensures that the entire system can be recovered after a catastrophe.
The Service Provider's business continuity plan shall include requirements for the tasks to be implemented in case of a fault of critical system components.
After averting the error and restoring the integrity of the system, the Service Provider has to restart the service as soon as possible. During recovery, the system components that provide certificate status information shall be given priority.
Data saving and recovery

- The data necessary for recovering the Service Provider's operations shall be saved and stored in a secure, preferably a remote, location that is suitable for the recovery of the Service Provider's operations following an incident or catastrophe.
- Backups shall be regularly made of important business information and software. Suitable tools shall be used for the backups in the interest of ensuring that all significant information and software can be recovered after a catastrophe or damages to media. The backup system has to be regularly tested in order to ensure its compliance with the business continuity plan.
- The backup and recovery functions shall be performed by the staff in the relevant trusted roles defined by point 5.3.
- If the requirements require double control for the management of the data, a double control shall also be used for their recovery.

5.7.3 Entity private key compromise procedures

End-user key compromise
See Chapter 4.9.12 Special requirements re-key compromise.
Service Provider key compromise

- The Service Provider's business continuity plan (or its catastrophe recovery plan) has to extend to the case where the Service Provider's key has become compromised or suspicion arises of such - as a catastrophe; planned procedures shall be put in place for these situations.
- Following the catastrophe, the Service Provider shall take steps in order to avoid the repetition of the catastrophe.

The Service Provider shall take at least the following steps if the Service Provider key has become compromised:

- It shall inform its Clients, Service Provider partners, the Relying Parties, and its Supervisory body.
- It has to indicate that the certificates issued with the affected Service Provider keys and the certificate status information are no longer valid; and

- It has to revoke the affected TSP certificate.

If any algorithms (or related parameters) used at the Service Provider or by the End-Users do not meet the requirements for the remaining time of the planned period of use, the Service Provider shall be obligated to:

- Inform its Clients, Service Provider partners, the Relying Parties, and its Supervisory body; and
- Revoke all affected certificates.

5.7.4 Business continuity capabilities after a disaster

The Service Provider shall have a business continuity plan in place that it can put into effect in case of a catastrophe. In case of a catastrophe (including if any of the Service Provider's signature private keys or other authenticating data are compromised), the Service Provider's normal operations shall be reinstated within the time included in the plan, and it shall also be ensured that the errors do not happen again.

In case of a catastrophe (including if the Service Provider's key or authentication data are compromised or if the TSP system's critical components are faulty), business as usual shall be restored as quickly as possible.

In the interest of ensuring the continuity of its services, the Service Provider shall have a procedure for extraordinary operating events that enable it to restore the qualified service as soon as possible. In case of an extraordinary operating event, the recovery of the reliable operation of certificate status services receives priority over the recovery of all other services and activities.

If the duration of the extraordinary operating event exceeds the three hour that set forth in Articles 36 of Decree 24/2016 of the Minister of the Interior, the qualified service provider is obligated to inform the Supervisory Body without delay, including the provision of the following information pertaining to the event:

- the start of the extraordinary operating event, a description of the event, and, if different, the time it was discovered,
- the effects of the extraordinary operating event (which include, in the case of a security event, a description of the affected services, IT components, and personal data, as well as the number of affected trust service clients),
- the expected duration of the extraordinary operating event,
- the measures taken and planned in the interest of preventing the extraordinary operating event in the future, and
- the end of the extraordinary operating event.

5.8 CA or RA termination

If the Service Provider wishes to terminate the provision of its services, it shall inform its Clients, Service Provider partners, Relying Parties , and the Supervisory Body at least sixty days prior to the termination. The Service Provider can then no longer issue new certificates in relation to the given trust service.

Service Provider shall fulfil the statutory requirements upon the termination of the service.

The Service Provider shall minimize the disruptions stemming from the termination of the Service. For this purpose:

- It has to have an up-to-date plan pertaining to the termination of the service in order to ensure the continuity of the service;

- It has to irrevocably destroy the Service Provider private keys (including their backup copies).
- The Service Provider has to provide for the costs of termination even if it were to go bankrupt or is unable to cover its own costs due to any other reason.
- The authorisations of all Service Provider partners have to be terminated that pertain to participation in the Certificate Issuance activity.
- The Service Provider shall provide for the fulfilment of its obligations, the continuous availability of the data required for checking certificates, and the handling of stored data (including registration data and log files) even after such termination (either on its own behalf or by handing those over to another Service Provider which takes over the service as written in Article 88 of EAA.[9]).
- The Service Provider shall revoke the as-yet unrevoked certificates it issued at least twenty days before the termination of its activity.
- When terminating its activity, the Service Provider shall provide a comprehensive backup (affixed with a timestamp) of all data in its IT system. Saved data files shall be protected from unauthorised modifications and access, and it shall be ensured that the data can only be accessed and interpreted by the authorised persons within the data retention period.

6. Technical security controls

The Service Provider shall take appropriate measures against forgery and theft of data; to this end Service Provider shall ensure that the systems and products used for the provision of the service – primarily for the management of the cryptographic keys and the activation data thereof – are reliable and protected against modifications during their entire lifecycle.

6.1 Key pair generation and installation

The Service Provider shall apply suitable controls for the handling of cryptographic keys and devices during their entire lifecycles.
QSCD based scertificates for sign/seal (QCP-n-qscd and QCP-l-qscd)
When issuing a certificate and during the entire term of the certificate's validity, the Service Provider has to make sure that it has a Cryptographic device QSCD certificate.

- The certificate enrolment process has to ensure that the public key included in the certificate is part of a key pair that was generated in QSCD.
- If the cryptographic device or the Client's private key is handled by a third party, the Service Provider has to ensure during the entire lifetime of the certificate that such party meets the necessary conditions (e.g. conformity assessment, supervisory records).
- If the Service Provider generates the key pair on its device (followed by importing the key to the Client device), the environmental requirements and security goals pertaining to the QSCD have to be kept.
- If the Client's private key is transferred from one device to another, the resulting security risks have to be uncovered and suitable measures shall be taken to handle these.

[9] See Article 88 points 3, 4, and 6 of the Electronic Administration Act for more information.

If the device's certificate were to become invalid, the Service Provider has to take the measures necessary as regards the certificates issued for the device; these measures shall be documented in the Service Practice Statement.

6.1.1. Key pair generation

The Service Provider has to generate the keys in a secure manner and has to ensure that private keys remain confidential.
The following requirements apply to the generation of key pairs:

- The generation of TSP key pairs - and the certification of public keys shall take place in a protected environment with the joint participation of at least two trusted employees and. The number of employees authorised to perform this action shall be kept at a minimum, and their activities shall be performed in line with applicable regulations.
- Only those algorithms and key lengths can be used to generate TSP keys that meet the standards applicable to the intended use in question and the decision issued by the National Media and Infocommunications Authority pertaining to algorithms and minimal key lengths, valid during the term of the certificate.
- Only those cryptographic modules can be used for TSP key generation that meet the technical and other requirements published in the Service Provider's regulations. The keys cannot be imported to devices that do not meet the requirements pertaining to application.
- The Service Provider shall include the actually used algorithms in the Service Practice Statement.
- Prior to the expiration of TSP certificates that provide for the signing of end-user certificates, the Service Provider has to generate a new certificate and has to take all measures in its power to ensure that the replacement of the certificate does not cause a disturbance to Relying Parties.
- These actions shall be performed in a manner that provides adequate time for all TSP partners and Relying Partners to implement their transition-related tasks. This does not apply to the case when the Service Provider terminates its activity.
- The Service Provider shall have documented procedures in place for the generation of TSP keys; these shall include at least the following:
    - The job roles that participate in the procedure (including both internal and external participants);
    - The tasks to be performed by the various roles in the individual phases;
    - Responsibilities during the procedure and thereafter;
    - The administrative tasks that have to be implemented during the procedure (which also serve as evidence of compliance).
- During the course of the procedure, the Service Provider shall generate a report that proves that the procedure was in line with regulations and that the integrity and confidentiality of the key pair was guaranteed. The report shall be signed by:
    - In case of a Root CA, the person filling the trusted role that is responsible for key generation and an auditor who is independent of the Service Provider's management and who followed the procedure to ensure that the report documents the executed procedure.
    - In case of an Intermediate CA, the person filling the trusted role that is responsible for key generation and who followed the procedure to ensure that the report documents the executed procedure.

If the end-user keys were generated by the Service Provider or the End-User:

- In case of end-user keys generated by the TSP, the applied algorithms must meet the intended use as defined by the certificate policy during the whole validity period of the certificate.
- Only those algorithms and key lengths can be used to generate end-user keys that meet the standards applicable to the intended use as defined by the certificate policy and the decision issued by the National Media and Infocommunications Authority pertaining to algorithms and minimal key lengths, valid during the term of the certificate.
- If the secondary CP OID displays, that the key generated on a Cryptographic device (see Chapter 1.2.1) then the keys shall be generated in the cryptographic device.
- The TSP has to reject all applications that do not meet the key requirements set out in Chapters 6.1.5 and 6.1.6.
- The end-user keys generated by the TSP shall be generated and kept in a secure manner for the entire time they are handled by the Service Provider.
- In the Case of NLSign Service the Service Provider shall generate the End-User key pair on a cryptographic device in a secure manner. The cryptographic device has to meet the requirements pertaining to the Service Provider's private key cryptographic device (see Chapter 6.2.1).

TSP keys be generated in a secure cryptographic module that meets the requirements set out in Chapter 6.2.1 Cryptographic module standards and controls.

A qualified auditor also has to observe the generation of new Root CA keys in order to check compliance with the above requirements and the integrity and confidentiality of the key pair. The auditor has to issue a certificate stating that:

- The TSP has documented its Root CA key generation and protection procedures in its regulations;
- The key generation procedure is suitably in-depth;
- The TSP has put effective control measures in place to ensure that key generation is implemented at a security level that is in line with relevant requirements;
- All procedures of the key generation procedure have been executed.

6.1.2. Private key delivery to subscriber

The end-user's private key shall be delivered to the end-user devices or to the TSP that will be managing it in a manner that ensures confidentiality and integrity. If the private key is delivered to other than its Receiver, all certificates belonging to the private key shall be returned to the TSP.
After its delivery to the Receiver, the TSP shall delete all instances of the end-user private key, with the exceptions set out in 4.12 Key escrow and recovery.
The TSP shall provide for the security of the Client devices during its generation, storage, and delivery to the Receiver.
In the case of managed SCD, the service provider does not provide the user with a key, the user is just given a notice that the user may obtain his key with the previously submitted activation data.

6.1.3. Public key delivery to certificate issuer

In the case the key pair and the certificate request is generated by the end user, with the submission of the request to the service provider, the end user proves having both components of the key pair (the request technically supports the possession of both components of the key

pair). In the case of managed SCD, TSP does not deliver any key to the user, the user is notified that he may start using his key with the previously submitted activation data.

6.1.4. TSP public key delivery to Relying Parties

The TSP shall make the TSP public key - including timestamp keys - accessible to Relying Parties on the internet as part of a TSP certificate.

6.1.5. Key sizes

In the case of web authentication certificates (QCP-w and EVCP) additonaly to the Chapter 6.1.1 the following applies.
The certificate has to be based on one of the following algorithms:
Hash algorithm: SHA-256, SHA-384, SHA-512
Coding algorithm: RSA-2048, DSA-2048-224, DSA-2048-256 or NIST P- 256 / P- 384 / P- 521 ECC]

6.1.6. Public key parameters generation and quality checking

The key generation parameters are set to values that correspond to the Algorithm Resolution of the National Media and Telecommunications Authority of Hungary.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

The key issued by the Root CA can be used only for the following purposes:

- Signing Root CA certificates (self-signed certificate)
- Signing and cross-certifying Intermediate CA certificates
- Signing internal TSP certificates (e.g. OCSP responder)
- For testing, if the signature of the Root CA is required for live use

6.2 Private key protection and cryptographic module engineering controls

The Service Provider has to implement physical and logical protection that prohibit unauthorised Certificate issuance.

The qualified TSP has to store its private key in a secure manner. Access by unauthorised persons to and use by unauthorised persons of the TSP private key has to be prevented.
The qualified TSP shall store the TSP private keys used for the generation of certificates, for the registry containing issued certificates, and for the certificate status services in a physically protected environment and only for the purposes defined for the given key.
In the course of the management of the hardware cryptographic devices, the signature or stamp private keys stored on the devices withdrawn from use shall be deleted in a way which prevents the restoring of the deleted data.

If the qualified TSP itself provides for the generation of the data used for the creation of the electronic signature or seal and its application in a device that generates electronic signatures or seals,

- the data used for the creation of the electronic signature or seal shall be generated in a physically protected environment with the participation of only persons who fill trusted roles;
- the data used for the creation of the electronic signature or seal can only be stored in the device that created the signature or seal for the subject of the certificate, if the data used for the creation of the electronic signature or seal is created outside of the electronic signature or seal creation device, all copies of the data outside of such device shall be deleted immediately in a manner that ensures that the deleted copy is unsuitable for continued use, as soon as the data used for the electronic signature or seal is entered in the electronic signature or seal creation device;
- it shall ensure that the data used to create the electronic signature or seal are inaccessible to others;
- it can only record the data monitoring the access rights of the subject of the certificate which are necessary for using the device that created the electronic signature or seal (thus especially the PIN code) for the purposes of being able to hand it over to the subject of the certificate (without keeping any copies);
- it can only transfer the data that monitors the electronic signature or seal creation device, as well as the access rights of the signatory, directly to the Client or the natural person (Receiver) authorised by the Client, also logging the time of the transfer.

]

6.2.1. Cryptographic module standards and controls

TSP private keys have to be stored and used on secure cryptographic devices that

- Have at least a EAL4 certification in accordance with the ISO/IEC 15408 or equivalent IT security requirements; or
- Meet the level 3 requirements of ISO/IEC 19790 or FIPS PUB 140-2 [12].

[QCP Qualified TSPs have to handle and operate separately

- the product used to provide a trust service as part of the qualified service from products used for its other activities;
- its products used to provide trust services as part of the qualified service from its products used for the provision of non-qualified services.

The products used by the qualified service provider for its other activities cannot influence the reliable operation of the products that provide trust services.

In its Service Practice Statement, the qualified Service Provider has to classify its products that provide trust services into security classes based on specific risk assessments, and shall keep records on these.

Before the qualified service provider uses its products that implement trust services used to provide a qualified service for any other purposes besides its own provision of services, it has to ascertain that the product does not contain any data linked to a trust service and that such data cannot be recovered. The qualified Service Provider shall log this examination and the measures taken on its basis.

The storage and use of the end user private key on the managed SCD device shall take place on a secure cryptographic device, which:

- shall have at least EAL4 certification under the ISO/IEC 15408 or an equivalent IT security system of requirements; or
- shall comply with the requirements of ISO/IEC 19790 or the FIPS PUB 140-2 at level 3.

6.2.2. Private key (n out of m) multi-person control

The internal Security Policy of Service Provider shall include the detailed description of the method of the multiple person management of the private keys. In case the present Service Policy or the Practice Statement requires the multiple person management of a private key, the employees in trust positions empowered to carry out the subject operation shall act in accordance with the above referred description.

6.2.3. Private key escrow

See Chapter 4.12.

6.2.4. Private key backup

The Service Provider shall make backup copy of its keys. The backup (copying), storage, and recovery of TSP private keys has to be implemented by the Service Provider in a physically protected environment with the joint participation of at least two trusted employees The number of employees authorised to perform this action shall be kept at a minimum, and their activities shall be performed in line with applicable regulations.
At least one backup/backups of the service provider private key shall be stored at a place different than the place of provision of the service.

The TSP private key is to be provided the level of protection guaranteed by the device even without the cryptographic device. An algorithm and key size shall be used for encryption that ensures protection for its entire remaining validity. The copies of the TSP private key not being used have to be protected with a level of security equal to the productive key.

6.2.5. Private key archival

No stipulation.

6.2.6. Private key transfer into or from a cryptographic module

The transfer into a cryptographic module of TSP private keys - thus also including timestamp private keys - has to be implemented by the Service Provider in a physically protected environment, in accordance with the rules of the multiple person management of private keys with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons.

6.2.7. Private key storage on cryptographic module

If the TSP private key is stored on a dedicated cryptographic device, it shall be ensured that the keys cannot be accessed from outside the device.
In the case of cryptographic devices, protection shall be provided against forgery even during transport and storage, and correct operation shall be ensured.

6.2.8. Method of activating private key

The activation of TSP private keys - thus also including timestamp private keys - has to be implemented by the Service Provider in a physically protected environment, in accordance with

the rules of the multiple person management of private keys with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons.
The submission of the activation code of the device/service is required for the use of the end user private key, provided that the private key is stored on the device.

6.2.9. Method of deactivating private key

No stipulation.

6.2.10. Method of destroying private key

All instances (live, saved, and archived) of expired or unused TSP private keys shall be destroyed in a manner that makes them unrecoverable and unusable.
When destroying a cryptographic device, it shall be ensured that the private keys that it was used to store are also destroyed (this regulation does not pertain to all instances of the key, just to those on the device).
The end-user (or, in the case of a signature service, the TSP) has to irrecoverably destroy the private keys of end-user signature / seal / website authentication certificates if the certificate has been revoked or its validity expires and no new certificate is issued with the use of the public key paired to the private key.
In addition to the above cases, the Service Provider shall irrecoverably destroy the private key of the managed SCD based certificate in case of the resetting of the activation data.

6.2.11. Cryptographic Module Rating

See Chapter 6.2.1.

6.3 Other aspects of key pair management

The Service Provider has to use the signature / seal keys in a suitable manner and cannot use those after their validity has expired.

- Keys used to sign / seal certificates and validity information cannot be used for any other purpose.
- Keys used to sign / seal certificates can be used exclusively in locations that provide physical protection.
- The TSP private key shall be compatible with the hash and signing procedures and key lengths used to sign certificates, in accordance with Chapter 6.1.1.
- If the Service Provider issues a self-signed certificate, ITU-T X.509 requires that the certificate’s attributes meet the type of key use in question.

In the case of managed SCD, Service Provider shall furthermore ensure

- The inactivation of the active users. No inactive user shall access the signature service, but the status of their certificates shall not change;
- The activation of the inactive users. Only active users shall have access to the signature service;
- Resetting of the activation code of the end users, which means the deletion of the private keys of the end user, and the revocation of the certificates.
- Deletion of the end users, which mean the deletion of the user and certificate data in

addition to the resetting of the activation code.
The end user shall be deleted following the expiry of the service agreement.
The end user data pertaining to the certificate service, which data have been recorded within the framework of the signature service (submitted within the application for certificate) shall not be stored by the Service Provider within the framework of the signature service; the data shall be forwarded to the certificate service in an unchanged form.

- The data shall be destroyed by the Service Provider upon the revocation of the end user certificate (see Chapter 6.2.10);
- Such data shall not be used for the creation of signature or stamp.

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

The validity of web authentication certificates (QCP-w and EVCP) certificates cannot exceed 27 months.
The validity of qualified sign or seal certificates cannot exceed the time during which the applied cryptographic algorithms can be securely used, and can be no more than 2 years from issuance.
The validity of timestamp certificates cannot exceed the time during which the applied cryptographic algorithms can be securely used.
The validity of test certificates cannot exceed 12 months, which the Service Provider can limit at its own discretion.
In the case of managed SCD the service agreement may limit the frequency and number of the use of the certificate for signature/stamping.

6.4 Activation data

The following chapters describe issues related to activation data.
Only employees working in trusted roles providing double control can install and restore TSP key pairs on the cryptographic device.
The Service Provider shall ensure that the End-User can change the activation code in possession of the current activation code. The Service Provider may under no circumstances store the End-User activation code, with the exception of storage in memory for the duration of the signature process.
In case managed SCD is used (certificate requested via the NL SIGN service) the end user shall also be provided with the opportunity to change the activation code in possession of the current activation code.

6.4.1 Activation data generation and installation

Activation data shall be securely prepared and distributed separately from the secure cryptographic device or the private key.
In the case managed SCD is used (certificate requested via the NL SIGN service) the activation code shall be given by the client upon the submission of the application. (The activation code shall not be restored by the service provider.)

6.4.2 Activation data protection

Only the end-user is authorised to learn end-user activation data.

6.4.3 Other aspects of activation data

The activation and deactivation of Client devices shall take place in a secure manner.

6.5 Computer security controls

The Service Provider has to restrict access to its systems to authorised persons. For this purpose

- It shall protect the boundaries of its internal zones in order to prevent unauthorised access (including access by Clients and Relying Parties).
- Sensitive data (including registration data) shall be protected from discovery during the reuse of data media.

The following requirements apply to the various activities:

Certificate generation

- Local area network devices shall be placed in a location that is both physically and logically secure, and their compliance with the Service Provider's requirements shall be regularly checked.

Publication

- Adding certificates to the certificate repository, deleting certificates therefrom, and modifying the related information shall only be possible for authorised persons.

Certificate revocation

- Modifying certificate revocation information shall only be possible for authorised persons.

Certificate issuance and status changes

- The Service Provider shall continuously provide monitoring and alarm tools in the interest of detecting, recording, and providing a timely response to any attempts at unauthorised or irregular access to its resources.

6.5.1. Specific computer security technical requirements

The Service Provider shall use multi-factor authentication for all users authorised to issue Certificates.

6.5.2. Computer security rating

No stipulations.

6.6 Life cycle technical controls

6.6.1 System development controls

An analysis of security requirements shall be performed in the planning and requirement determination phase of system development projects (performed or contracted by the Service Provider) in the interest of integrating security into IT systems.

Change management procedures shall be applied in the case of issuing new versions of the Service Provider's software, of software modifications, and software repairs, as well as in regard

to configuration changes that affect the Service Provider's internal rules. Updating the documentation shall also be included amongst the procedures.
The Service Provider shall ensure regulated change management and reliable operation for the provision of qualified services, as well as the separation of operation from development.

6.6.2 Security management controls

The Service Provider shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

- The Service Provider's systems and information shall be protected from viruses, malware, and unauthorised software.
- Procedures shall be determined and performed for all reliable and administrative roles that affect the provision of services.
- The Service Provider shall determine and apply procedures in order to ensure that
    - security repairs are applied within a reasonable amount of time (within no more than 6 months) after their publication;
    - Security repairs shall not be applied if they contain additional security holes or cause instability that are less advantageous than the offered repairs; the reason for failing to use the repair shall be documented.

The Service Provider shall use trustworthy systems to store data provided to it, in a verifiable form so that:

- they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained;
- only authorised persons can make entries and changes to the stored data;
- the data can be checked for authenticity;]

6.6.3 Life cycle security controls

The Service Provider has to monitor resource requirements and has to prepare forecasts on expected changes in future capacity requirements in the interest of ensuring that suitable performance and storage space is available to offer stable service.
Service Provider shall ensure the protection of the protection of the cryptographic hardware device used in the course of the provision of the service during the entire lifecycle of the devices, and Service Provider shall ensure the followings:

- The cryptographic hardware device used shall have proper, valid certification during its entire lifecycle.
- Upon the takeover of the cryptographic hardware device the Service Provider shall ensure that the device has been protected, during its shipment, against the cracking of the cryptographic hardware devices.
- Service Provider shall ensure the protection against the cracking of cryptographic hardware devices during storage.
- Service Provider shall ensure that the requirements set out in the documentation of the device and in the certification report are continuously fulfilled in the course of the operation of the cryptographic hardware device.
- The private keys stored in the unused cryptographic hardware device shall be irrevocably deleted in accordance with Chapter 6.2.10 Method of destroying private key.

6.7 Network security controls

The Service Provider has to meet the following network security requirements:

- The Service Provider's systems have to be located within a secure zone and the Service Provider has to implement security procedures to provide for the security of communications with these systems and with high security zones.
- In the case of service systems, the user accounts, applications, services, connections, protocols, and ports not used for the provision of services shall be blocked or removed. The defined rules shall be regularly reviewed.
- The Service Provider may grant access to the secure zone and the high security zone only to employees with trusted roles.
- Based on risk assessments, the Service Provider shall separate its systems into various networks or zones, taking into account the functional logical and physical connections with reliable systems and services.
- A separate network shall be provided for service systems. The systems used for the validation of information security regulations may not be used for other purposes. The productive systems have to be separated from development, test, and other systems.
- The communication between the various reliable systems has to take place in a reliable channel that is logically separated from other communication channels and ensures the reliable identification of endpoints as well as the confidentiality and integrity of distributed data.
- If high-availability external access is required for the service, the network connection shall be redundant in order to ensure that the service is accessible if any of the connections go down.
- The Service Provider has to regularly perform a vulnerability check on its public and private IP addresses and has to record evidence proving that the check was performed by an independent person or organisation with suitable knowledge, experience, and tools that guarantee that the report is reliable. The check shall be performed quarterly or if any significant changes take place to the network.
- The Service Provider has to regularly perform an intrusion test and has to record evidence proving that the check was performed by an independent person or organisation with suitable knowledge, experience, and tools that guarantee that the report is reliable. The check shall be performed annually or if any significant infrastructural changes or application modifications take place.

6.8 Timestamping

TSP shall use timestamp issued by a qualified trust service provider if using timestamps is required in the framework of certificate service.

Timesources used by the Service Provider shall be synchronized to UTC timesource at least once a day.

7. Certificate, CRL, OCSP and profiles

7.1. Certificate profile

The Certificates issued by the Service Provider shall meet the specifications of RFC 5280, RFC 6818 and ITU-T X.509.
The qualified service provider may limit the use of the issued qualified certificate in accordance with the subjects, times, areas, or other restrictions set out in the certificate; this restriction shall be clearly defined by the certificate. The qualified service provider is obligated to inform the certificate subject of the limitation and its consequences.
Qualified certificates shall include the term for which the qualified service provider shall retain the available information pertaining to a certificate.

7.1.1. Version number(s)

The Service Provider shall issue “V3” certificates in accordance with the X.509 specifications.

7.1.2. Certificate extensions

The Service Provider may use the certificate extensions defined in the X.509 specifications by indicating the critical fields as necessary.
The certificate shall contain all qcStatements fields applicable to it, in line with the ETSI EN 319 412-5 standard. It can only have an esi4-qcStatement-4 value if a QSCD is used.
In the case of QSCD based certificate (QCP-n-qscd and QCP-l-qscd) In its qcStatement field, the certificate shall contain the esi4-qcStatement-4 value, in line with standard ETSI EN 319 412-5.

7.1.3. Algorithm object identifiers

The certificate shall indicate the name and parameters of the algorithm used for the authentication of the certificate.

7.1.4. Name forms

See Chapter 3.1.1 Types of names for the name forms of the Subject.
The value in the certificate’s “Issuer” field has to be the same as the “Subject” value in the issuing CA certificate.

7.1.5. Name constraints

The Service Provider shall indicate any name constraints in the “nameConstraints” field, which shall then be marked as critical.

7.1.6. Certificate policy object identifier

In the Certificates issued on the basis of the present Trust Service Policy, the Service Provider shall include the non-critical Certificate Policy extension, which shall include the used Certificate Policy OID-based identifier (see Chapter 1.2.1 Certificate Policies).

7.1.7. Usage of Policy Constraints extension

No stipulations.

7.1.8. Policy qualifiers syntax and semantics

The Service Provider can include some information regarding the usage of the Certificate in the Certificate Policy extension's Policy Qualifier field. The field shall also include the online address (URL) at which the Service Practice Statement is available.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulations.

7.2. CRL profile

7.1.2. Version number(s)

The CRLs issued by the Service Provider shall conform to the "V2" CRLs defined by the RFC 5280 and ITU-T X.509 specifications.

7.2.2. CRL extensions

The Service Provider shall support the CRL number non-critical revocation list extension by providing serial numbers to CRLs that sequentially increase by a value of one.

7.3. OCSP profile

The Service Provider shall operate the certificate status service defined by RFC 6960.

7.3.1. Version number(s)

The Service Provider shall support "V1" certificate status requests and responses as defined by RFC 6960.

7.3.2. OCSP extensions

No stipulations.

7.4 Timestamp certificate profiles

The timestamp certificate has to meet the requirements set out by ETSI EN 319 412-3. The Subject's countryName attribute has to indicate the country in which the time stamp provider was registered. The organisationName field has to include the entire name of the service provider as officially registered. The commonName field has to include the CA's unique name.
The timestamp certificate has to meet the requirements imposed by the National Media and Infocommunications Authority's decision on authorised algorithms and minimal key lengths.

8. Compliance audit

The Service Provider has to conduct its activities in line with

- relevant and applicable European Union and Hungarian regulations,
- the requirements of the present Trust Service Policy, and
- it has to be included in the registry of Trust services kept by the Supervisory Body with competence at its place of operations.

The Service Provider's activities are supervised by the National Media and Infocommunications Authority, which holds a comprehensive on-site audit at least once a year.
the Service Provider shall have its activities audited by an external conformity assessment body in accordance with the relevant standards.
The following requirements shall apply to the Service Provider's external conformity assessment audit:

- all of the unique features of the Service Provider's trust services to be audited shall be taken into consideration;
- it shall be ensured that the audit covers all service activities related to the subject of the audit;
- the audit shall be performed on the basis of applicable standards, publically available specifications, and/or legislative requirements.
    - 910/2014/EU
    - Eüt. (CCXXII.trv)
    - 24/2016 Korm rendelet
    - ETSI 319411-2
    - ETSI 319412
    - ETSI 319403
    - ETSI 319401

8.1. Frequency or circumstances of assessment

The Service Provider is obligated to continuously check adherence to the contents of the present Trust Service Policy and the Service Practice Statement, and is to closely monitor the quality of its service by performing self-audits. In the interest of implementing the above, the Service Provider shall hold an internal audit once a year.
For the time that the Service Provider offers qualified certificate creation services, it shall be obligated to examine compliance with applicable standards by performing internal audits and external conformity assessments at least annually.
At least once a year, the Service Provider shall also audit the operations of the External Registration Authority, unless the External Registration Authority has an external audit report to certify its conformity to the applicable standards. The same requirements apply to the External Registration Authority as to the Service Provider's Internal Registration Authority.
The Service Provider shall exert strict control over the quality of its web authentication certificate services. In the interest of the above, it shall audit at least 3% of the certificates (selected with random sampling) it has issued since the previous self-audit.]

8.2. Identity/qualifications of assessor

Service Provider may carry out the internal audits with its employees employed in the role of independent system auditor.

External conformity assessments shall be performed by a natural or legal person or a group of natural persons who or that have suitable authorisation granted by a national accreditation organisation of an EU Member State.

- is capable of performing an audit as regards the standards set forth in Chapter 8 Compliance audit;
- meets the requirements set out in Chapter 8.3 Assessor's relationship to assessed entity;
- has/have suitable experience regarding Public Key Infrastructures (PKI), IT, IT security solutions, technologies, and audits, and the functions of audits performed at the External Registration Authority;
- in the case of audits performed on the basis of ETSI standards, has/have
    - the accreditation defined by ETSI EN 319 403, *or*
    - equivalent accreditation as defined by a national standard, *or*
    - ISO 27006 accreditation provided by the National Accreditation Authority in accordance with ISO 27001;
- in the case of WebTrust audits, has/have the license to perform WebTrust audits;
- whose activities are governed by legislation or a professional code of ethics;
- has/have insurance of at least USD one million to cover any omissions or errors in the auditor’s activities.]

8.3. Assessor's relationship to assessed entity

External conformity assessment shall be performed by an auditor who or which is independent of the Service Provider’s owners, executives, and management.

8.4. Topics covered by assessment

The Service Provider’s internal conformity assessment shall cover the following areas:

- the compliance of regulations with relevant legislation and standards;
- the compliance of applied processes with regulations.

In case of external conformity assessment, the person performing the conformity assessment shall evaluate the fulfilment of the requirements and criteria defined by the given audit system.

8.5. Actions taken as a result of deficiency

The results of the conformity assessment shall be summarized in an evaluation report. The report shall set forth the deficiencies uncovered by the audit and the deadlines set for their correction.

8.6. Communication of results

The Service Provider is not obligated to publish its internal conformity assessment report and may handle the information contained therein confidentially.

Within three (3) months after the audit period, the Service Provider shall make the external conformity assessment report public. The Service Provider is not obligated to make public the general findings of the audit report that do not affect the audit results.]

9. Other business and legal matters

9.1. Fees

The Service Provider is obligated to make service fees available to Subscribers by way of a public price list.
The Service Provider may not charge for the use of the following services if used in accordance with the regulations:

- the use of the certificate repository;
- access to certificate status information (CRL and OCSP).

9.1.1 Certificate issuance or renewal fees

The Service Provider may charge the Subscriber for the use of the certificate creation services on the basis of the public price list or may deviate from it if agreed on with the Subscriber beforehand. The certificate creation service fee shall include certificate issuance, registry for the entire validity period (in the certificate repository or in CRLs), and archiving in accordance with relevant legislation.
The Service Provider may charge the Subscriber for certificate request and handling procedures and for optional services related to certificate renewal and certificate creation services.

9.1.2. Certificate access fees

The Service Provider may not charge the Relying Parties for the use of the certificate repository services if used in accordance with the regulations.

9.1.3. Status changes or status information access fees

The Service Provider may not charge the Relying Parties for certificate status changes and the use of the certificate status information services if used in accordance with the regulations.

9.1.4. Fees for other services

The Service Provider may charge for the use of additional (for example: optional) certificate services in accordance with the public price list or other individual agreements.

9.1.5. Refund policy

No stipulations.

9.2. Financial responsibility

The Service Provider is liable for damages caused by its services in accordance with the rules of responsibility for breaches of contract set out by the relevant Civil Code, the Service Practice

Statement, its general contracting terms and conditions, and in its certificates, to the degree defined in the relevant decree on the detailed conditions pertaining to trust services and the providers of such services.
The Service Provider may limit the value of the assumption of its risk and shall inform its clients and the Relying Parties by way of its website or in the certificate if it opts to do so.

9.2.1. Insurance coverage

In the interest of ensuring reliability, the Service Provider shall have liability insurance. Such liability insurance shall extend to all damages and costs related to the trust services offered by the Service Provider:

- the damages caused to trust service clients in regard to a breach of the trust service agreement,
- the damages caused to trust service clients and third parties irrespective of the agreement,
- the costs set out by the Electronic Administration Act and incurred by the trust service client as a result of a failure to fulfil the obligations set out by the Electronic Administration Act, and
- the costs of the procedures of the Conformity Assessment Bodies commissioned by the Supervisory Body on the basis of the applicable provisions of the eIDAS Regulation, if such are validated by the Supervisory Body as procedural costs.

The Service Provider shall ensure that the insurance policy it concluded explicitly states that it extends to the above.
The amount of the assumption of liability included in the insurance policy cannot be less than HUF 3,000,000 (three million forints).
In the case of the website authentication certificates (QCP-w and EVCP), Service Provider shall have the insurance coverage of an amount set out in the EV requirements.

9.2.2. Other assets

In the interest of providing for the costs related to the termination of the service and for reliability, the Service Provider shall

- have an unconditional and irrevocable bank guarantee of at least twenty five million forints OR
- establish a security deposit of at least twenty five million forints at a financial institution OR
- be provided with the joint and several suretyship of an undertaking registered in the European Economic Area and having an amount of subscribed capital equal to at least one hundred million forints.

9.2.3 Insurance or warranty coverage for Relying Parties

The Service Provider shall make available the information on the extent to which the guarantees and sureties it provides extend to damages caused by third parties.

9.3. Handling of business information

The Service Provider is obligated to store and handle the confidential information that comes into its possession in accordance with the act on informational self-determination and freedom of information.

9.3.1 Scope of confidential information

The Service Provider shall consider all data pertaining to any Clients and not included in Chapter 9.3.2 to be confidential information.

9.3.2 Information not within the scope of confidential information

The Service Provider shall not be obligated to consider confidential information the data that have been stripped of their personal nature (e.g. anonymised) or that which it makes public as part of its service by way of its certificate repository:

- the data included in the certificate, and
- the data pertaining to certificate status.

The Service Provide may disclose non-confidential information, may share such with its partners, and is not liable for their becoming public knowledge.

9.3.3 Responsibility to protect confidential information

The Service Provider is liable for the protection of the confidential information that it handles. These data may be learned only by those of its employees and partners who require such for their work. Access by other persons shall be excluded by legal means and, as far as possible, technical and safety measures.
In the following cases the Service Provider shall disclose the sensitive data it possesses to the authority or other body requesting the disclosure as set out in the following statutory provisions:

- on the basis of Article 88 of the Electronic Administration Act, upon the termination of all of its trust services (see Chapter 5.8) Service Provider shall hand over the data related to the services to the statutorily specified recipient service provider or in the lack of the above, to the Trust Service Supervisory Authority under Article 89,
- to the investigating authority or national security services within the framework of mandatory disclosure under Article 90(1) and 90(2) of the Electronic Administration Act for the purpose of detection or prevention of criminal offenses or in the interest of national security,
- in the course of civil litigious or non-litiguous proceedings within the framework of mandatory disclosure under Article 90(3) of the Electronic Administration Act,
- to the Trust Service Supervisory Authority within the framework of mandatory disclosure under Articles 93(5)-(7) of the Electronic Administration Act.

The Service Provider shall set out the means of the above disclosures in its Practice Statement in itemized form.

9.4. Privacy of personal information

The Service Provider shall handle personal information in accordance with the relevant provisions of the Electronic Administration Act and the Information Act.
During the course of the provision of its trust services, the Service Provider shall handle the data that are technically essential for the provision of the service.
If the certificate issued by the Service Provider in the framework of the trust service also certifies a right of representation, the Service Provider:

- shall notify the represented person on the issuance of the certificate without delay,
- shall revoke the certificate indicating the right of representation at the request of the represented person or the representative if the right of representation has been terminated,
- may only include a pseudonym in the certificate if granted the authorisation of the represented party.

In accordance with relevant legislation, the Service Provider is obligated to retain the electronic information pertaining to certificates (and to their creation) and the connected personal information for at least 10 years after the validity of the certificate or until the legal dispute in connection with an electronic signature or with an electronic certificate including an electronic signature has been closed with a final ruling; for this same period, the Service Provider shall ensure tools that allow the contents of issued certificates to be identifiable.
The Service Provider shall ensure that unauthorized persons may not access any data that are made available to it. The Service Provider's principals on data management are included in the document "The Principles of the Confidential Handling of Personal Information," the current version of which is available on the Service Provider's website.

9.4.1 Privacy plan

The Service Provider shall handle data that comes into its possession in accordance with the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information.
The Service Provider may only request the personal information that is necessary for the provision of its services, in line with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
The Service Provider shall have a data management policy in place, which shall contain detailed requirements on the treatment of personal information. The current version of the public part of the Data management regulations shall be made available on the Service Provider's website.

9.4.2. Private information

The Service Provider only handles data that is essential for realizing the purpose of such data management, is suitable for achieving this goal, and concerning which it has informed the involved persons. Private information may only be handled to the extent and for the time required for implementing the given goal.
With the exception of the private information provided under points 9.3.2 and 9.4.3, the Service Provider shall handle all private information confidentially.

9.4.3. Information not deemed private

Based on the written consent of the Client, the Service Provider shall disclose the personal and organisational data of the certificate's Subject and the certificate's status information.

9.4.4. Protection of personal data

The Service Provider shall store the personal information pertaining to Certificate issuance but not included in the certificate in a secure manner and shall protect it. Suitable measures shall be implemented to protect the data from unauthorized access and modifications, especially when forwarding those between the Client and the Service Provider's various units. They shall

furthermore be protected against data loss, damage, and unauthorized processing. See also: Chapters 5.3.1, 5.5.1, 5.7.1, and 5.7.4.

9.4.5. Usage of private information

The Service Provider may only disclose the information included in the certificate if provided the preliminary written consent of the Client.
The Service Provider may only use the personal information in a manner and to the extent that is required for the actions related to the certificate (e.g. issuance, suspension, revocation).

9.4.6. Data management

The Service Provider shall adhere to the provisions of the act on informational self-determination and freedom of information. The Service Provider may only handle personal information if granted preliminary consent by the involved party.
The Service Provider may also handle personal information if acquiring the consent of the involved party is impossible or would result in disproportionate costs and the handling of the personal data is required for the Service Provider to meet its legal obligations or for the Service Provider or a third party to validate its rightful interests, and the validation of such interest is proportionate to the restriction of the rights for the protection of personal data.
Without the consent of the Client, the Service Provider may only disclose personal information stored on behalf of the Client in the cases defined by relevant legislation.

9.4.7. Other information disclosure circumstances

In the interest of uncovering and preventing crimes with the use of the trust services that it provides, as well as for reasons of national security, the Service Provider shall forward data free of charge to investigating authorities and national security services if the conditions for data requests set forth in separate legislation are met; the above extends to data certifying the personal identity of the involved parties and other data. The fact of the data provision shall be recorded; however, the Service Provider may not inform the Client of the data provision.

9.5. Intellectual property rights

The Subscriber is the owner and the End-User is the user with full rights of the public and private keys issued by the Service Provider to its clients. The Service Provider is the owner and the End-User is the user with full rights of the certificates issued by the Service Provider to its clients.
The Service Provider may publish, reproduce, revoke, and manage by other means the end-user certificates (including the public keys and other data in them) that it has issued.
The Service Provider is the owner of the CRL and status information, both of which it may make public. The object identifier (OID) issued by the Service Provider to Clients is owned by the Service Provider.
The present Trust Service Policy and the Service Provider’s other regulations and documents are owned exclusively by NETLOCK. Clients, End-Users, and other Relying Parties may use these documents only in line with the present requirements; all other use (e.g. for commercial purposes) is strictly prohibited. Public documents can be freely disseminated, but only in an unchanged format, in their entirety, and by indicating their source.

Rightholders have the right of disposition over the proprietary names included in the Trust Service Policy, the Service Provider's other regulations and documents, and in certificates. The copyright of the works referred to herein (standards, legal sources) are owned by the rightholder. During its operations, the Service Provider may not infringe upon the intellectual property rights of third parties.
The software and hardware components used during the service activities are owned by the Service Provider or it uses those legally.

9.6. Representations and warranties

The Service Provider is responsible for adherence to the provisions of the present Trust Service Policy and Service Practice Statement, even if it outsources any of its activities.

9.6.1. CA representations and warranties

The CA shall guarantee that certificates are issued in accordance with the present Trust Service Policy and the applicable Service Practice Statement.

9.6.2. RA representations and warranties

The Service Provider shall have its cooperating External Registration Authorities fully comply with the provisions of the present Trust Service Policy and the applicable Service Practice Statement.
The RA's responsibilities:

- establishing the (personal) identities of Applicants and the entities marked as Subjects and verifying the data made available to the Service Provider;
- establishing and checking the organisational identity of the represented Organisation and the identity and right of representation of the person proceeding in representation of the represented Organisation;
- guaranteeing the veracity of entered registration data;
- informing the Client prior to the conclusion of the Service Practice Statement on the contents and availability of the Trust Service Policy and Service Practice Statement and on the conditions for using the service;
- performing certificate status change requests;
- fully adhering to its general obligations.

9.6.3. Client representations and warranties

The General Terms and Conditions and the service agreement define the Client's additional obligations and liabilities.
The Client is obligated:

- to conclude a service agreement with the Service Provider or to conclude an agreement in line with the General Terms and Conditions;
- to provide true data when applying for a certificate, and to inform the Service Provider without delay of any change in the following data: the personal identification data included in the certificate and required for identification; in the case of a certificate issued as regards the right of representation of a third person, the person authorised to provide representation and the data of the represented person; other data included in the certificate;

- to use the certificate key pair in accordance with the present Trust Service Policy and the Service Practice Statement and to handle such securely (see chapters 4.5.1);
- to check the data included in the issued certificate;
- to inform the Service Provider without delay of any irregularities discovered regarding the trust service or the certificate, as defined in separate legislation, the service agreement, or the Service Practice Statement, or any other events affecting the trust service, this especially if unauthorised persons use the Client devices or private keys provided by the Service Provider and necessary for the use of the trust service;
- to initiate the revocation, modification or key changeover of the certificate if:
    - the certificate contains inaccurate or incorrect information,
    - the private key belonging to the certificate has been compromised or lost,
    - the right of representation indicated in the certificate has been terminated,
    - the right of representation/procedure of the end-user of a seal certificate has been terminated;
- to inform the Service Provider without delay on the commencement of any legal disputes related to the trust service.

End-Users may only use certificates for the purposes and with the restrictions indicated therein. The private keys belonging to test certificates cannot be used for actual commitments.

9.6.4 Relying Party representations and warranties

As regards the acceptance and use of certificates, Relying Parties shall proceed in accordance with the usages and other information and restrictions indicated in the certificate. In addition to the above, they can decide on whether to accept certificates at their own discretion and/or on the basis of their regulations. When examining validity, the Relying Party's circumspect procedure is a requisite for maintaining the security level guaranteed by the Service Provider.
Test certificates cannot be used to accept true commitments.

9.6.5 Representations and warranties of other participants

If the representative of the organisation does not personally proceed when applying for a certificate, the represented organisation is liable for the certifications it issued, especially for the certifications in which it certifies that the Applicant is authorised to proceed in the application for, status change of, renewal of, etc. a Certificate that also includes the Organisation's name.

9.7. Disclaimers of warranties

The Service Provider excludes the possibility of warranty if:

- the Relying Party did not proceed with circumspection in the use or checking of certificates, i.e. it did not proceed in accordance with the present Trust Service Policy, the Service Practice Statement, or relevant legislation;
- Clients fail to adhere to the requirements pertaining to Client devices and key management;
- the regulations issued by Relying Parties or others do not meet the requirements of the present Trust Service Policy or the Service Practice Statement;
- the Service Provider is unable to fulfil its obligations regarding communication due to a fault of the internet or a part thereof;

- the damages are a result of the fault or weakness in the cryptographic algorithms approved by the Supervisory Body.

9.8. Limitations of liability

The Service Provider can limit its liability to provide compensation in accordance with Chapter 9.2 of the Trust Service Policy.

9.9. Indemnities

Service Provider shall set out in its Practice Statement drafted under the present Service Policy the detailed rules of its obligation to provide damages and indemnification related to the services provided under the present Service Policy. Further stipulations of the obligation of the Service Provider to provide damages and indemnification may also be set out in the General Terms and Conditions, the service agreements and/or contracts and agreements of other type concluded with the Clients.

The Service Provider shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the undertaken obligations.
The intention or negligence of the qualified TSP shall be presumed unless that qualified TSP proves that the damage occurred without the intention or negligence of that qualified Trust Service Provider.
Where the Service Provider duly informs its customers in advance of the limitations on the use of the services it provides and where those limitations are recognisable to third parties, the Service Provider shall not be liable for damages arising from the use of services exceeding the indicated limitations.
In all other cases, the relevant provisions of the Hungarian Civil Code shall be governing.

9.10. Term and termination of Policy

The term of the current version of the Trust Service Policy shall commence with the date indicated on the cover and shall remain in force until revocation.
The personal scope of the Trust Service Policy shall extend to the Service Provider, to its employees participating in the Services, and to Clients.
The material scope of the Trust Service Policy extends to the Services provided by the Service Provider and to the certificates issued as part of such Services, as well as to the Service Provider's subjects and tangible assets related to the above Services.

9.10.1. Term

The day the current version of the Trust Service Policy enters into effect is indicated on the cover.

9.10.2. Termination

The validity of the present Trust Service Policy shall lapse with the entry into effect of a new Trust Service Policy or when the service activity is terminated.

9.10.3. Effect of termination

If the present Trust Service Policy is revoked, the Service Provider shall publish on its website the detailed rules for revocation and the rights and obligations that remain in effect thereafter.
The Service Provider undertakes to guarantee that the regulations pertaining to the protection of confidential information as defined by relevant legislation shall remain in effect even if the Trust Service Policy is revoked.

9.11. Individual notices and communications with participants

In the interest of communicating with its Clients, the Service Provider shall operate a customer service office and telephone service.

9.12. Amendments

If any changes occur in normative regulations, security requirements, the market environment, or other circumstances, the Service Provider shall amend its Trust Service Policy and applicable regulations. In extraordinary cases, such amendments may even enter into effect immediately.
The Service Provider is obligated to report to the Supervisory Body immediately if any changes occur to its operations or the provision of trust services as compared to the reported and registered data.

9.12.1. Procedure for amendment

The Service Provider collects requests for changes, performs the amendments, fulfils internal and external information provision obligations, and has the changes enter into effect. During the collection of the changes, the Unit creates private internal working documents that will be subjected to an internal review prior to publication. The Service Provider shall bundle these changes together to create a new Policy and shall endeavour to issue new Policies as seldom as possible.
Before its approval, the Service Provider shall examine the Trust Service Policy and the service regulations to examine whether their contents and form meet the requirements of relevant legislation. The Service Provider has final competence and liability for the approval of the Trust Service Policy and the regulations.
The versions of the amended Trust Service Policy and regulations shall always be published with new version numbers. Compliance with the Trust Service Policy, the regulations, and relevant legislation and standards shall be examined at least annually. The regulations shall be reviewed and amended whenever justified by changes in relevant legislation. The Service Provider shall also apply its practical experience when reviewing the Trust Service Policy and the regulations.

9.12.2. Notification mechanism and period

The Service Provider that provides qualified trust services shall inform the Supervisory Body of any planned changes to its operations or the provision of the trust service as compared to the data reported to and registered by the Supervisory Body, at least 30 days before such change.
Simultaneously with the notification the Service Provider shall send to the Trust Service Supervisory Authority the new version of the Certificate Policy and Practice Statement with the amendments approved.

In case Service Provider plans to launch a new service as a result of, and simultaneously with, the change, Service Provider shall notify the Trust Service Supervisory Authority at least 30 days prior to the planned launch of the new service. The notice shall be made by filling the form published by the Trust Service Supervisory Authority, in accordance with Decree No. 26/2016 of the Ministry of Interior. The Service Provider shall attach the followings to the form

- the amended and approved new version of the Certificate Policy;
- the amended and approved new version of the Practice Statement;
- the other instruments and documents set out in Decree No. 26/2016 of the Ministry of Interior.

9.12.3. Circumstances under which OID must be changed

In case of any changes to the Trust Service Policy, the Service Provider shall give the document a new version number, which therefor also results in a change in the OID: two documents with different contents cannot have the same OID.
The amended Policy can pertain only to certificates that are to be newly issued (and not ones that have already been issued). The Service Provider shall publish new Policies on a different internet address than the previous version.

9.13. Dispute resolution provisions

The Service Provider is obligated to provide contact information for reporting complaints, complaint management, and information on the litigious and non-litigious means for initiating legal disputes related to the service, including the conditions therefor, the legal basis for turning to a conciliatory body, and the names and contact information of the authorities authorised to proceed and the conciliatory body or other dispute resolution organisation.

9.14. Governing law

The Service Provider shall perform its activity in accordance with the relevant Hungarian and European Union legislation. Hungarian law is governing regarding the Service Provider's agreements and policies and for their fulfilment, and they are to be interpreted in accordance with Hungarian law.

9.15. Compliance with applicable law

The Service Provider shall provide its trust services in accordance with the relevant European Union and Hungarian regulations. The Service Provider shall set out the applicable legislation and the method for ensuring compliance with those in its Service Practice Statement.

Applicable laws and regulations in force at the effectiveness date of the present Service Policy:

- 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
- Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services

- Decree No. 24/2016. (VI. 30.) of the Ministry of Interior on the Detailed Requirements Pertaining to the Trust Services and Trust Service Providers
- Decree No. 25/2016. (VI. 30.) of the Ministry of Interior on the Administrative Service Fees Payable to the Trust Service Supervisory Authority
- Decree No. 26/2016. (VI. 30.) of the Ministry of Interior on the Contents of the Registries Maintained by the Trust Service Supervisory Authority and the Submissions Related to the Provision of Trust Service
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI);
- General Policy Requirements for Trust Service Providers
- Act CXII of 2011 on the Right of Informational Self-determination and on Freedom of Information
- Act V of 2013 on the Civil Code of Hungary

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulations.

9.16.2. Assignment

Any service providers operating in accordance with the present Trust Service Policy may only assign its rights and delegate its obligations to third parties if granted the Service Provider's preliminary written consent.

9.16.3. Severability

If any provisions of the present Trust Service Policy become invalid for any reason, the remaining provisions shall remain in effect unchanged.

9.16.4. Enforcement

In the interest of receiving compensation for the damages, losses, and costs they caused, the Service Provider may claim compensation and the reimbursement of attorneys' fees from Clients. If the Service Provider does not exercise its right of validating compensation, this does not mean that it renounces its right to validate compensation for damages in any future cases or if any other provisions of the Trust Service Policy are violated.

9.16.5. Force Majeure

The Service Provider is not liable for the faulty or late performance of any requirements set out in the Trust Service Policy or its Service Practice Statement if the fault or delay was caused by an unforeseen circumstance outside its scope of inspection.

9.17. Other provisions

The Service Provider's units that deal with the creation and status change of certificates (authenticating and registration authorities) shall be independent of other organisations as regards

the suitable handling of certificates in accordance with the applicable policies. These units shall have a documented structure that prevents partial operations.
Executive employees shall be independent of any business, financial, and other influences that can have a negative influence on trust in the services.