NETLOCK
Service Practice Statement
for Non-eIDAS Certificate Services

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

[NETLOCK Informatics and Network Security Services Limited Liability Company]

Document name in Hungarian:	NetLock Szolgáltatási Szabályzat Nem-eIDAS Tanúsítványszolgáltatásokra
Document name in English:	NETLOCK Service Practice Statement for Non-eIDAS Certificate Services
Version:	20170721
Object identifier (OID):	1.3.6.1.4.1.3555.1.49.20170721
Date approved:	21/07/2017
Valid from:	21/07/2017
No. of pages:	117 pages included cover
Prepared by:	**Zoltán Szabó**, PKI Product Manager
	Viktor Varga, Chief Architect
Accepted by:	**dr Zsófia Fehér**, Chief Legal Officer

Table of content

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 Policy for non-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 present document is the statement of NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (hereinafter: Service Provider or TSP) regarding the detailed requirements of procedure and operation applied in relation to the provision of the qualified trust certification services (hereinafter: Practice Statement or Statement).

The procedures and the practical rules pertaining thereto, which are recorded in the present practice statement shall only apply to the services enlisted in chapter 1.1 hereof and related to the certificates complienat with the certification policies set out in chapter 1.2.1 Certificate Policies (LCP, NCP, NCP+, DVCP and Codesign) of the document entitled NETLOCK Service Policy for Non-eIDAS Certificate Services (hereinafter: Service Policy).

The certificates complient with each certificate policies and the short description thereof with the names used in the commercial communication of Service Provider are set out in Chapter 1.2.1 hereof.

For the definitions and abbreviations see chapter 1.6.

1.1. Overview

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

- According to LCP, NCP, NCP+ certificate policies:
    - Personal authentication
    - Business authentication
    - Layer authentication
    - Organizational authentication
    - Personel enchryption
    - Business enchryption
    - Layer enchryption
    - Organizational enchryption
    - Codesign (Non-EV) for private persons
    - Codesign (Non-EV) for organizations
- According to DVCP certificate policies:
    - DV SSL
    - DV SSL UCC
- certificate status services related to non-eIDAS certificate services.

See Chapter 1.2.1 Certificate policies for the connection between the various certificates and certificate policies.

In addition to details information on the Service Provider's procedural and operational rules, the present Statement also provides Relying Parties with recommendations for checking electronic signatures, seals, including the certificates of these, and for the use of certificates for website authentication and other certificates.

1.1.1. Standards and requirements

The Service Practice Statement was created in line with the structure of the NETLOCK Service Policy for Non-eIDAS Certificate Issuance Service and sets forth the method for meeting the requirements determined therein. 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 contents of the Statement meets the requirements and recommendations of eIDAS, the Electronic Administration Act, and the BM Decree, and makes use of the recommendations of standards ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412, and x.509.

In the case of website authentication certificates (DVCP) the NetLock conforms to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and this Guideline, this Guideline take precedence over this document

The laws, standards and requirements used and applied by Service Provider are detailed in Chapter 9.15.

1.1.2. The Service Provider

The entity referred to as the Service Provider in the present Statement is NETLOCK Kft.

Service Provider data:

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:	+36 (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 time indicated on the Service Provider's website.

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 Practice Statement establishes the requirements of the provision of non-eIDAS certificate service that is out of the eIDAS scope.

The public registry of the non-qualified service providers and qualified services under the eIDAS maintained by the Trust Services Supervisory Authority is available at:

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

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

Voluntary accreditations and other qualifications:

- The certification of the certificate creation service has taken place in accordance with the ETSI EN 319 401, ETSI EN 319 411, and ETSI EN 319 412-1 standards (2016).
- ETSI 102042 and ETSI 101456 (2015)
- ISO 9001 standard (continuous since 2001)
- BS 7799-2 (2005)
- ISO/IEC 27001 standard (continuous since 2005)

Also see Chapter 8.

1.2. Document name and identification

See the cover page for the name and OID identifier of the document (i.e. the first page without numbering, with the logo of Service Provider) – In the lines named “Document name in Hungarian” and “English name of document” and “ID number (OID)”.

On the remaining pages of the document, the Hungarian name of the document is set out in the footer, while the OID identifier of the document is set out in the header.

The present document is one of the documents issued by Service Provider, which provide for a uniform regulatory framework of the conditions of the services provided by Service Provider. Such documents are the General Terms and Conditions, the Service Agreement, the practice statements, as well as the other agreements made with the Clients and the Partners.

In the present document the entity referred to as the Service Provider shall mean NETLOCK Kft. – see chapter 1.1.2 for its details.

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

1.2.1. Certificate policies

In the CP (Certificate Policies) extension of end-user certificates, the Service Provider indicates the OIDs defined in Chapter 1.2.1 of the Service Policy as standard certificate policy identifiers. The Service Provider also applies secondary certificate policies.

The end-user certificate types distributed by the Service Provider and the compliance of the certificate policies (see Chapter 7.1 for the connection between certificate policies and certificate profiles).

Commercial names of NetLock certificates	**Certificate Policy ID[2]**	**Description**
personal encryption - sw	LCP	Encryption certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
business encryption - sw	LCP	Encryption certificate with business profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
organizational encryption - sw	LCP	Encryption certificate with organizational profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
personal authentication – sw	LCP	Authentication certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
business authentication – sw	LCP	Authentication certificate with business profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
organizational authentication – sw	LCP	Authentication certificate with organizational profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
personal authentication – SCD	LCP	Authentication certificate with personal profile with SCD key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
business authentication – SCD	LCP	Authentication certificate with business profile with SCD key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
organizational authentication – SCD	LCP	Authentication certificate with organizational profile with SCD key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
personal authentication – SCD/CAMS	LCP	Authentication certificate with personal profile with SCD key storage and with key generation by the TSP, the private key of which is capable of user authenticating in IT systems.
business authentication – SCD/CAMS	LCP	Authentication certificate with business profile with SCD key storage and with key generation by the TSP, the private key of which is capable of user authenticating in IT systems.

[2] See at Service Policy 1.2.1

organizational authentication – SCD/CAMS	LCP	Authentication certificate with organizational profile with SCD key storage and with key generation by the TSP, the private key of which is capable of user authenticating in IT systems.
Online SSL	DVCP	Website authentication certificate for the authentication of one domain name, of which subject field contains only the domain name.
Online SSL - UCC	DVCP	Website authentication certificate for the authentication of more than one domain name, of which subject field contains only the domain name.
Personal codesign - sw	-	Codesign certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
Organizational codesign - sw	-	Codesign certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
Personal codesign – SCD	-	Codesign certificate with personal profile with SCD key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
Organizational codesign - SCD	-	Codesign certificate with personal profile with SCD key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
Personal codesign – SCD/CAMS	-	Codesign certificate with organizational profile with SCD key storage and with key generation by the TSP, the private key of which is capable of electronic signing program codes.
Organizational codesign - SCD/CAMS	-	Codesign certificate with organizational profile with SCD key storage and with key generation by the TSP, the private key of which is capable of electronic signing program codes.

In case any specific procedure set out in the present practice statement does not apply to the application, issuance and management of all certificate types enlisted above, the different terms and conditions shall be separated herein on the basis of commercial names, and if necessary for the sake of clarity, the ID of the certificate policy shall also be indicated.

1.2.2. Revisions of the Document

OID	Validity	Description of change	Prepared by
1.3.6.1.4.1.3555.1.49.20170721	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 Practice Statement 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

The community that uses the issued certificates consists of the Service Provider, the Registration and other Cooperating Authorities in a contractual relationship with the Service Provider, certificate Applicants, End-Users, Subscribers, and the Relying Parties.

1.3.1. Certification Authorities

The Service Provider operates a Certification Authority and more than one CA managed by it.

The operation of the Certificate Authority compliant with the requirements covering the Authority set out in the Certificate Policy, the present Practice Statement and other Terms shall be ensured by the proprietary internal rules of operation of the Certification Authority. The employees working at the Certification Authority shall carry out their activities in accordance with the requirements set out in the internal rules of operation.

The Service Provider uses the following CAs:

- the Intermediate CA that certifies both end-user and TSP certificates, and
- the top-level Root CA

which operate in the form of a hierarchy.

The Service Provider may also authenticate Servers that are linked to Subordinated Services.

The Certification Authority is responsible for issuing certificates. The Certification Authority employs Certification Administrators who are responsible for executing the (non-automated) tasks related to the issuance, renewal, modification, and status change of certificates on the basis of the identification and data verification performed by the Registration Authority. See Chapter 9.6.1.

The name and SHA256 hash of the Root CAs of the Service Provider:

NetLock Arany (Class Gold) Főtanúsítvány	6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:98
NetLock Platina (Class Platinum) Főtanúsítvány	EB:7E:05:AA:58:E7:BD:32:8A:28:2B:F8:86:70:33:F3:C0:35:34:2B:51:6E:E8:5C:01:67:3D:FF:FF:BB:FE:58

Main data of the non-eIDAS intermediary CAs:

Name of CA	link to CA certificate	link to CRL
NETLOCK Trust CA	www.netlock.hu/index.cgi?ca=trust	www.netlock.hu/index.cgi?crl=trust
NETLOCK Üzleti (Class B)	www.netlock.hu/index.cgi?ca=cbca	www.netlock.hu/index.cgi?crl=cbca
NETLOCK Expressz (Class C)	www.netlock.hu/index.cgi?ca=ccca	www.netlock.hu/index.cgi?crl=ccca

More information and other CAs can be found on the website of the Service Provider[3].

[3] https://www.netlock.hu/html/cacrl.html and https://www.netlock.hu/docs/dokumentumok/NETLOCK_ca_hierarchy.pdf

1.3.2. Registration Authority

Service Provider operates a central Registration Authority. The Registration Authority employs Registration Administrators, Mobile Registration Associates, and Validation Specialists, and work together with Registration and Approved Agents.

The Registration Authorities are responsible for identifying the entity(-ies) indicated as the subject of the certificate and involved in the application, checking their data and authorisation to proceed, recording the certificate application and forwarding it to the Certification Authority, coordinating the certificate issuance procedure, documentation, performing additional certificate management and status change requests, and handing over the Client device.

The Service Provider's customer service employees take care of customer service tasks and communicate with Clients. Customer service is a separate group within the Central Registration Authority. The Service Provider publishes their contact information on its website.

The operation of the Registration Authority compliant with the requirements covering the Authority set out in the Certificate Policy, the present Practice Statement and other Terms shall be ensured by the proprietary internal rules of operation of the Registration Authority. The employees working at the Registration Authority shall carry out their activities in accordance with the requirements set out in the internal rules of operation.

See Chapter 9.6.2.

1.3.3. Subscribers, End-Users, and Applicants

The Subscriber and the Applicant are the Clients of the Service Provider, with whom the Service Provider enters into contractual relationship.

The person of the End User shall be determined by the Subscriber.

See the respective definitions in Chapter 1.6 of Definitions and Abbreviations.

The Service Provider, any employee, organizational unit or service partner may also become a Client of Service Provider. The same terms and conditions shall apply to such clients as the ones apply to the remaining clients; Service Provider shall not diverge from the requirements and rules of the certificate policy and the present practice statement. In the case of such an application for certificate, Applicant, Subscriber, End User and Recipient shall not participate in the activities of Service Provider made in the course of the processing of such related application (registration, validation of identity, activities related to client devices, approval of application, certificate issuance etc. – for further details see Chapter 4) and shall not exercise any influence thereto.

1.3.4. Relying Party

The Relying Parties are typically not in contractual relationship with the Service Provider, but the present Practice Statement prepared on the basis of the present Certificate 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 communicates with Relying Parties by way of the certificate repository.

See further the definition of Relying Party in Chapter 1.6.1.

1.3.5. Other participants

Encrypting partners

Creating encrypted message with public key of encryption certificate is available for anyone.

Before encryption the participant who do encryption shall convinced of revocation status of the certificates used.

1.4. Certificate usage

The certificates issued as per the LCP, NCP, NCP+ and Codesign certificate policies are non-eIDAS certificates:

- encryption certificates whose private keys are capable of decoding data encrypted with the public key;
- authentication certificates whose private keys are capable of user authentication with doing PKI signature operation but are not capable of creating legally accepted electronic signature;
- codesign certificates whose private keys are capable of ensuring authenticity and integrity of codes.

The certificates issued according to the DVCP certificate policy 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

a. End user certificates

The private keys belonging to the end user certificates issued under the present Service Policy shall be used only for encryption, user authentication or website authentication.

The private key that belongs to the certificates issued in accordance with the NCP+ certification policy is protected by a cryptografic device (SCD).

The private key that belongs to the certificates issued under the NCP certification policy is stored by software key storage.

In case of certificates issued under the LCP certificate policy there is no similar requirement as to the storage of keys.

The private keys belonging to the end user certificates issued under the Codesign certificate policy shall be used only for signing program codes.

In the case of the website authentication certificates issued under the DVCP certification policies, there is no similar requirement as to the storage of keys. The website authentication certificates are capable of certifying websites.

b. TSP certificates

TSP certificates are usable for signing end user certificates exclusively after the publishing of the certificate.

1.4.2. Prohibited use of certificates

c. End user certificates

The certificates issued under the present Service Policy and the related keys are prohibited to be used for purposes other than proper use written above.

d. 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. Regulation administration

The issuance and maintenance of the present Service Practice Statement shall be carried out by that organizational unit of the Service Provider, which is responsible for the practice statement. The permanent members of the responsible organizational unit are those employees of the Service Provider, who are designated as such by the management of the Service Provider. The operation of the Unit is regulated by the internal, non-public rules of operation of the Policy Adopting Authority.

1.5.1. A dokumentum adminisztrációját végző szervezet

The name of the organizational unit of the Service Provider that is responsible for the policies (terms) is NETLOCK Policy Adopting Authority. 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 (see Chapter 1.5.1) 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 the course of processing the query the Authority or the member shall identify the section(s) of the document affected by the query, 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 Certificate 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 resplsible for the compliance of the present practice statement with the certificate policy

The compliance of the Practice Statement – which contains the detailed practical requirements of the provisioning and use of the certification service under the Certificate Policy – with the Certificate Policy shall be monitored by the NETLOCK Policy Adopting Authority. The practice statement prepared on the basis of the Certificate Policy may be approved by the Policy Adopting Authority if practice statement is in complete compliance with the the present Certificate Policy. The Certificate Policy or its public draft may be published only upon approval.

1.5.4. Adoption of the Practice Statement

In case the practice statement is needed to be amended, the modified new version shall be drafted, adopted and issued under the uniform (rules of) procedure under Chapter 9.12.1 and in accordance with the rules of operation of the Authority. In case the employee responsible for the adoption of the new version has ensured that the Practice Statement will continue to comply with the requirements of the Certificate Policy, the responsible employee shall approve the practice statement and shall arrange for the publication thereof without any delay, but at least 30 days prior to the effective date of the new version.

1.6. Terms & Abbreviations

1.6.1. Definitions

AIA	CAI (Authority Information Access:Certificate Authority Issuers): The certificate field containing the address (URL) of the CA certificate applicable to the given certificate.
Subordinated service	Non-qualified trust service operated on the basis of the Service Provider's Statements, for which the Service Provider provides a certificate.
Trust Service Policy	The NETLOCK Trust Service Policy for Certificate Creation, Timestamping, Archiving, and Signature Services
Eakta (format)	An electronic signature container format that can include documents and the connected profiles (metadata), signatures, countersignatures, and timestamps, in accordance with the standards of the ETSI TS 101 903 (XAdES) specification. See also: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html

Certification Administrator	Within the Certification Authority, the Certification Administrators take part in the certificate issuance.
Approved Agent	A partner to the Service Provider who, based on a contract by the Service Provider (in case of the Applicant's request), hands over the client device to the Applicant in the Certificate Issuance process, at the place and time agreed on with the Applicant. If applicable, can agree with the Registration Agent.
KGyHSz	Közigazgatási Gyökér Hitelesítés-Szolgáltató [Public Administrative Root Authentication Service Provider] See http://www.kgyhsz.gov.hu/
External Registration Authority	The Service Provider's service providing partner that conducts the processing of requests for services, the identification of the Applicant and Subscriber, and the checking (in part or in whole) of their right to proceed and the data to be included in the certificate.
Central Registration Authority	The Service Provider's organizational unit operated within its own organisation that processes applications for services, identifies their Applicants and Subscribers, and checks their rights to proceed and their data.
Mobile Registration Associate	A registration administrator who identifies the Applicant - in case of such request and if a personal meeting is required - at the time and place agreed on with the Applicant.
Permanent identifier	An identifier that provides for the individual identification of the certificate owner. Implementation in the certificate takes place on the basis of RFC 4043. This can be an individual identifier created by the Service Provider or as included in an official registry. The identifier created by the Service Provider is an OID that consists of two parts: the Service Provider's individual identifier (1.3.6.1.4.1.3555.5) and the Client's individual identifier, which follows it. The Client's individual identifier starts with 5 and a number that can have one of the following values: ● 1,6,8,10: for personal or business certificates where the identifier is created from the natural person's data. ● 2,7,9,11: for organisational certificates where the identifier is created from the organisation's data. ● 3: for pseudonym certificates where the identifier is created from the pseudonym data. If used, it is entered in the certificate's Subject/SerialNumber field.
Registration Agent	A Service Provider partner (or its employee) that performs identification tasks related to Certificate Issuance on-site at the Applicant as contracted by the Service Provider.

Registration Administrator	These employees are responsible for managing certificate applications and verifying the veracity of the data provided in the certificate application (see Chapter 4.2.1) within the Service Provider's Registration Authority.
Service Agreement	An Agreement prepared in the Service Provider's system on the basis of the data provided by the Client; and enters into force when signed by the Client and accepted by the Service Provider (see Chapter 4 of the GTC).
Software certificate	A certificate where the private key is not issued for a Cryptographic device.
UCC Certificate for Website Authentication	A certificate for website authentication that includes more than one different domain names (in the SubjectAltName/DNSname field).
Client Menu	An interface accessible via the Service Provider's website that is provided to the Service Provider's clients for the purposes of performing various applications regarding certificates and the related services and for checking the status of current applications; access is provided with an individual user name and password (following registration in the client menu). Registration and login in the qualified client menu is required for managing qualified certificates; the advanced client menu has to be used for managing non-qualified certificates.
Client Menu Registration	The process where a natural or legal person creates an own Client menu by providing his/its data and logging into the Client menu with the applicable user name and password.

See Chapter 1.6.1 of the Trust Service Policy.

1.6.2. Abbreviations

1. The acronyms of referenced legislation
2.

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 certificate repository

Service Provider shall publish the various information pertaining to the chertificates (certificates, expiry information, policies and other terms).

2.1. Repositories

The Service Provider shall maintain a public certificate repository and systems that communicate certificate revocation information (CRL, OCSP), and shall publish the Terms and conditions related to the certificates that may be issued under the present Practice Statement in downloadable PDF format on its website. (See Chapter 1.1.2)

2.1.1. Publication of certification information

Service Provider shall provide the Clients and Relying Parties with certificate revocation information (CRL, OCSP) via HTTP protocol, with an availability level of at least 99% per annum, and that the length of the service outage shall not exceed 24 hours per occasion.

Service Provider shall make available the public certificate repository on its website, via HTTPS protocol – the public certificate repository shall consist of the subject data of end user certificates of the clients who consented to the publication in the service agreement. The certificates published in the public repository are downloadable by the public. Service Provider maintains websites for the purposes of checking revoked, expired, and valid certificates for website authentication certificates (DVCP) (testing)[4].

The certificate repository's TSP certificates, as well as the valid end-user certificates for the publication of which the Client has granted its consent, can be queried on the Service Provider's websites (see Chapter 4.4.2).

The Service Provider applies the following procedure for the publication of the various certificates:

- It publishes CA certificates on its website (Chapter 1.1.2)
- It displays valid end-user certificates in the public certificate repository immediately following their issuance and - if applicable - activation.
- The Service Provider ensures that all of the certificate types it issues can be tested by issuing test certificates (see Chapter 7.1).

The Service Provider publishes the status information pertaining to certificates with the use of the following methods:

- The status information pertaining to the end-user certificates issued by the Service Provider and to TSP certificates are immediately accessible within the certificate status service following the status change.
- The information on certificate status changes are also displayed in certificate revocation lists (CRLs). The CRLs can be queried on the Service Provider's website and are also accessible by applications via http protocol.

When logging into the client menu, the end-user can access information pertaining to its respective certificates and their current status.

The KGyHSz publishes, in accordance with its own regulations, the status information pertaining to its own root certificates and to certificates of service providers that it endorsed; the information is available in accordance with relevant legislation in the certificate repository which, at the time of the publication of this Statement, is found at http://www.kgyhsz.gov.hu/.

Service Provider shall inform its Clients and the Relying Parties on the various terms and conditions applicable to various types of certificates (see Chapter 1.1.2).

[4] The Service Provider publishes the addresses of these websites in its own website (see Technical data).

2.1.2. Publication of Terms and Conditions

The present Practice Statement and the underlying Certificate Policy shall be published by Service Provider with the contents and in a structure conform with RFC 3647, save for the derogations specific to the Service Provider.

The Service Provider shall, at least before their entry into force, publish the new versions to be implemented of the Certificate Policy, the Practice Statement and the General Terms and Conditions pertaining to the services based on the present Certificate Policy and affected by the subject modification. In addition to the documents in force, those earlier versions thereof shall also be continuously available on the website, on the basis of which any certfificate is still in force

Following the entering into of the service agreement, upon the issuance of the certificate, Service Provider shall provide the Client with the Practice Statement and the Service Agreement attached to the e-mail, which shall be deemed as a durable medium under the laws of Hungary in force.

2.1.3. Declarations

BRG Declaration

NETLOCK is compliant with the actual version of the document entitled “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, which is published at http://www.cabforum.org website. In case of any diecrepancy, the Baseline document shall prevail in the case of the DVCP certificates.

2.2. Time or frequency of publication

Service Provider shall publish on its website the public draft of the new version of the Practice Statement at least before entering into effect, in order to allow its Clients and the Related Parties to get acquainted with it and to make comments to the Service Provider before the draft enters into effect (see Chapters 1.5.2 Contact person of the document and 9.12.1 Amendments).

The Policy Adopting Unit of Service Provider shall revise the Practice Statement and the Certificate Polcy at least once in every year and shall modify them if necessary (see Chapter 9.12).

The publication of new versions regarding the present Statement takes place as set out in Chapter 9.12. See Chapter 9.12 for the publication of new versions of the Trust Service Practice Statement.

The Service Provider’s other policies and contractual terms, as well as their new versions, will be issued as required.

When necessary, the Service Provider shall publish extraordinary information in accordance with the requirements of relevant legislation or, in absence of such, without delay.

The certificates of the Authenticator CAs will be published no later than when commencing the service.

See Chapter 4.9.7 for the frequency of publishing CRLs.

2.3. Access controls on repositories

The Terms and Conditions, extraordinary information, certificates, and status information published by the Service Provider are public information. Read access to these is made publically available in accordance with the features of the media used for publication.

The Service Provider's certificate repository is accessible via standard HTTP or HTTPS protocols.

The Service Provider continuously ensures the access of the certificate repository (24/7, every day of the year), with the exception of the time required for scheduled maintenance. As far as possible, the Service Provider will schedule maintenance outside work hours. The certificate repository can only be accessed lawfully through the Service Provider's website, by way of individual manual requests. Other requests (e.g. automated) are only possible with the Service Provider's written consent.

Online services (certificate repository, OCSP) do not have any restrictions on access, but requests can be limited for security reasons if a certain limit is exceeded. The conditions for restrictions will be published on the Service Provider's website.

See Chapter 2.1.1 and 4.9.9 for the availability of services.

3. Performing identification and authentication functions

The Service Provider uses Client identification and data verification steps outlined in the following points for issuing certificates and concluding the service agreement in the framework of certificate creation services.

3.1. Naming

The Issuer and Subject fields of the certificates issued by Service Provider are conform with the name format requirements of the recommendations ITU-T X.509 and RFC 5280.

The Subject (Subject and SAN) fields in the certificates identify the entity for which the certificate was issued. The Subject fields contain more than one type of identifiers, the contents of which are as follows:

Name and ID of data (Standard name, OID, English name)	Content
Subject field	
CN id-at-commonName 2.5.4.3 Name	In case of personal and business certificates, this includes the full name of the natural person Applicant in the form used in the data source.
	In case of a pseudonym certificate, this is the same as the contents of the pseudonym field.
	In case of an organisational certificate, the organisation's full or short name /DBA / Trademark / Product identifier

	In case of a DBA, its contents can be: 1. A company name including the company type It can include the verified company name's long or short form without the indication of the company type (Kft., Bt., etc.) 2. Domain name 3. Product ID Product name preceded by a company name / DBA / Trademark
	The website name in the name of certificates for website authentication The commonName can only contain an FQDN, which also has to be included in the SAN/DNSName field.
SN Id-at-surname 2.5.4.4 Last name	The last name of the natural person's full name as indicated in the certificate CN field. The delineation between the names is performed in accordance with the MELASZ recommendation.
G id-at-givenName 2.5.4.42 First names	The first name of the natural person's full name as indicated in the certificate CN field. The delineation between the names is performed in accordance with the MELASZ recommendation.
Id-at-pseudonym 2.5.4.65 Pseudonym	In case of pseudonym certificates, the certificate contains the pseudonym selected by the Applicant. The pseudonym is repeated in the commonName field. The pseudonym cannot be misleading and has to be unique at the Service Provider, i.e. the same pseudonym cannot be used for two different users.
id-at-serialNumber 2.5.4.5 Serial number	The globally unique serial number of the natural/legal person indicated in the certificate CN field.
id-at-countryName 2.5.4.6 Country	The country of the Subscriber's seat or home address. The two-letter country code as defined by ISO 3166-1.
L id-at-localityName 2.5.4.7	The city of the Subscriber's seat or home address.
id-at-stateOrProvinceName 2.5.4.8	The county or state of the Subscriber's seat or home address.
id-at-organizationName 2.5.4.10	In the case of business and organisational certificates certificates. The Subscriber organisation's full or short name.

id-at-organizationalUnitName 2.5.4.11	In the case of business and organisational certificates. The name of the organizational unit within the Subscriber organisation The Subscriber has to certify its existence in order to be included in the certificate.
organizationIdentifier 2.5.4.97	In the case of business and organisational certificates The Subscriber's tax identification number as included in the registry, in the semantic format defined by ETSI EN 319 411-1. It can contain, in a bound format, a unique identifier received in an official national or other identification system, as set forth below: 1. If the organisation has a tax number: a VAT prefix followed by the organisation's registered country code, a hyphen, and the organisation's taxpayer identification number, in unchanged format. For Hungarian organisations: the "VATHU-" prefix can be followed by a domestic tax number and the "VATEU-" prefix can be followed by a community tax number, in unchanged format. 2. If the previous point is not applicable, the commercial register code will be used following the prefix "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 will 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. For the identification system of other countries, the Service Provider shall use the country codes defined by ISO 3166.
Id-at-title 2.5.4.12 Title	For business certificates The Applicant's position or title within the Subscriber organisation. Optional.
subject/EMAIL	The contents are the same as that of the SubjectAlternateName:emailaddress field.
SAN field	
SAN SubjectAlternateName:DNSName	For certificates for website authentication Contains one or more domain names If the CN also contains a DNS record, it is included here as well.
SAN SubjectAlternateName:emailaddress	The email address certifiably belonging to the entity defined in the CN, as per the requirements of RFC 822. Not used for certificates for website authentication.
SAN SubjectAlternateName:otherIdentifier	The Service Provider's individual identifier (which is equal to the Service Provider's part of the permanent ID).

See Chapter 7.1 for the different requirements pertaining to filling out the above Subject fields (Subject and SAN) and Issuer fields according to certificate profile.

3.1.1. Types of names

When creating the Subject fields for certificates, the Service Provider has to follow the X.500 distinguished name requirements in accordance with the RFC 5280 standard. The Service Provider distinguishes between the following name types in the case of end-user certificates, and it links the following profiles to them:

Name type (Subject type)	Certificate profile
Natural person	Personal
Legal person	Organisational
DBA / Trademark / Product identifier and legal person together	Organisational
Natural and legal person together	Business
Pseudonym	Pseudonym
Website	DV certificate for website authentication

See Chapter 7 of the present Statement for a description of the certificate profiles.

3.1.2. Need for names to be meaningful

The *Subject* field of encryption or authentication certificates issued to natural persons have to include the following data:

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

The *Subject* field of encryption or authentication certificates issued to legal persons have to include the following data:

- commonName (name);
- countryName (country code);
- organizationIdentifier (organization Identifier).

The *Subject* field of DVCP certificates for website authentication have to include the following data:

- commonName (name);
- countryName (country code).

In case a legal person is specified as the Subject of the, Service Provider shall, in all cases, specify the unique identifier of the organization in the Subject/organizationIdentifier field of the certificate.

In case both a natural and a legal person is specified as the Subject of the certificate (business certificate profile, see Chapter 7.1), the Service Provider shall mandatorily specify the unique identifier of the organization in the Subject/organizationIdentifier of the certificate, unless the applicant of the certificate is an attorney-at-law or a law firm.

The SAN field of the website authentication certificates (DVCP) shall also mandatorily include the domain name set out in the commonName field, as well as the further domain names in the case of a UCC certificate.

Chapter 3.1 contains a detailed description of the Subject field.

The name of the natural and legal person included in the certificate shall be checked by the Service Provider against authentic records or, in absence of such, official identification documents, and shall be included identically to the manner included in those.

If the contents of the *Subject/Serialnumber* field is an official (checked on the basis of a document) national identifier, its obligatory format: <REF>HU-<documentnumber>, where <REF> is replaced by three characters as set forth below:

1. "PAS" for passport numbers (e.g. PASHU-AE123456)
2. “IDC" for ID card and driving licence numbers (e.g. IDCHU-123456AB (ID card) or IDCHU-AB123456 (driving licence))
3. “TIN” for tax identification numbers (e.g. TINHU-1234567890)

In the case of individual identification systems, <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 (e.g. EI:HU-200007292386 or AT:EU-BH16251).

In case the certificate contains more serialnumber values, no formal requirements shall apply to the further serialnumber fields, assuming that those are not filled with the numbers of the above identification documents.

The certificate identifier fields (“Subject” and “Issuer”) meet the requirements of the X.500 name format. Additional rules pertaining to the “*Subject*” and “*Issuer*” fields:

- Data are indicated in the certificates without special and control characters.
- By default, names are indicated in certificates as follows: in the same exact format as the name used for personal identification in the official document, including accented letters in their original form in the CN, SN, and G fields, with the use of UTF-8 encoding. The various name units are separated by spaces.
- Abbreviations can be used in the case of names that exceed the maximum number of characters defined in the applicable standards.

The Subject/organizationIdentifier field shall be filled with a unique identifier given within an official national or other identification system in a mandatory format, which is defined by ETSI EN 319 412-1 5.1.4 (it is set out in the form of *REFCO-organization identifier*, where REF shall consist of three and CO shall consist of two characters, as follows).

Kitöltése:

1. Ha a szervezet rendelkezik adószámmal, az alapján kell kitölteni a mezőt: magyar adószám esetén "VATHU", EU-s adószám esetében “VATEU” értékkel.
2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszámmal "NTRHU" értékkel.
3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.
4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító is alkalmazható.
5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide.

Más országok azonosítórendszerei esetében az ISO 3166 szerinti országkód alkalmazandó a HU országkód helyett.

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 indicate the fact that it is a test with the words “TEST” or “TESZT”, which can be followed by other name data in a clear manner that can be mistaken with any real person.

3.1.3. Pseudonyms

Service Provider shall also issue pseudonym certificates. The Applicant may only apply for pseudonym certificates on its own behalf. The Applicant shall choose the pseudonym, which the Service Provider will not check; the Subscriber is liable for any problems (e.g. copyright, etc.) in relation to the pseudonym.

The Service Provider shall issue pseudonym certificates in accordance with the pseudonym certificate profile, where the “CN=CommonName” and the “Pseudonym” fields contain the pseudonym in the same format; no legal/natural person can be indicated next to the pseudonym.

In case of using a pseudonym, the Service Provider may only hand over the data pertaining to the Client’s true identity to third parties or the authorities if granted the Client’s consent, unless required to do so by a final court ruling. The Service Provider is authorised to deny the issuance of a pseudonym certificate that incurs legal difficulties (or is likely to do so) or revoke such certificate at its own discretion.

Pseudonym certificates for website authentication cannot be applied for. (DVCP)

3.1.4. Rules for interpreting various name forms

The certificates issued by the Service Provider do not aim to function as a digital form of identity for the natural or legal persons indicated as the Subject or for their identities to be established solely on the basis of the data included in the certificate.

The business profile certificate (see Chapter 7.1) itself does not support the right of representation. In case Service Provider issues a certificate purported to support full or partial right of representation, or a legal relationship that may be interpreted as such, then Service Provider shall indicate the above by indicating the position verified on the basis of a public database or on the lack thereof, public instrument. The position shall be indicated by Service Provider in the Subject/Title field of the certificate, and shall indicate the following statement in the certificatePolicies/policyQualifier field of the certificate on the basis of Chapter 7.1.8: “Prior to

the issuance of the certificate Service Provider verified on the basis of credible information the right of the natural person indicated in the Subject/CN field of the Certificate to represent the organization indicated in the Subject/O field.

The contents of the present Statement provide information to Relying Parties for interpreting the identifiers (see especially Chapter 7.1.5.). If the Relying Parties require help with the interpretation of the identifier or any data included in the certificate, they can also contact the Service Provider directly (see Chapter 1.1.2).

The Service Provider will only provide additional information (besides the information that helps in interpreting certificate data) on the data of the Subject(s) on the basis of an authorisation or of relevant legislation.

a. Issuer identifier

The issuer identifier is understood to mean that the Service Provider issued the certificate with the use of a given TSP (intermediate/root) certificate.

The TSP certificate's *Issuer* field contains the country code of the country (*Country*) and city (*Locality*) in which the certificate issuer has its seat, the name of the organisation (*Organisation*), its organisational unit (*Organisation Unit*), and the name of the CA issuing the given certificate (*Common Name*).

b. Subject identifier

The *Subject* field is understood to mean that the certificate belongs to the natural person / legal person / website (domain name) / DBA / product name / pseudonym with the *Common Name* of the *Organisation unit* within the natural or legal person that has the name of the *Organisation*.

The home address of the natural person or the seat or site of the organisation is defined under the fields *Country* (country), *State* (country/county), and *Locality* (settlement). The certificate does not contain any information that is more accurate as regards location.

3.1.5. Uniqueness of names

The Service Provider clearly distinguishes between certificate Subjects (Subject field) in the case of end-user certificates . In the interest of the above, the Service Provider provides all Clients with a unique subject identifier (OID-based Permanent ID), which it includes in the certificate's Subject/Serialnumber field (see Chapter 7.1). This identifier individually identifies the natural or legal person included in the certificate. A Subject may have more than one identifier, but an identifier may never be issued to another Subject.

In addition to the above, the Service Provider can also indicate another individual identifier in another Subject/Serialnumber field (e.g. personal identification card number, official card ID, etc.).

The Permanent identifier is not applicable in the case of certificates for website authentication (DVCP).

3.1.6. Recognition, authentication, and role of trademarks

The Service Provider may also use a trademark in the certificate on the basis of a DBA, trademark, product name, or product identifier owned/possessed by the Client. These data are included in the certificate in the Subject/CN and/or SubjectAltName/dirname fields. See Chapter 3.2.2 for checking these.

The acquisition of a trademark by the Client is not an event that requires the modification of a certificate.

3.2. Initial identity validation

Service Provider shall carry out the client registration prior to the issuance of the end user certificates, including the verifications required by Section 82 of the Electronic Administration Act, with the identity validation and authentication procedures detailed in the subchapters of the present chapter (3.2), provided that Service Provider has not carried out such procedures earlier or the earlier procedures ceased to be valid.

In case of DV website authentication (DVCP) certificates, requirements of present chapter shall be applied, only if the text indicates it separately.

Service Provider shall carry out the following procedures within the framework of the initial identification:

1. identifies the person of the Applicant, by validating the personal data, his right/power to act and his right to use the other data to be recorded in the certificate;
2. identifies the Subscriber if the Subscriber is different from the Applicant, by validating at least the full name and unique identifier of the Subscriber to be recorded in the certificate as well as his right to use the other data to be recorded in the certificate;
3. identifies the person(s) entitled to represent the Subscriber;
4. identifies the person of the attorney in fact of the representative(s) of the Subscriber and validates the power of attorney;
5. validates the Subject-related data to be indicated in the certificate; and
6. validates the possession of the private key counterpart of the public key to be recorded in the certificate, and
7. records the validated data and documents the identification and validation procedures.

For the validations under points 1-5 the Service Provider shall use authentic and valid instruments, documents and/or trusted central registries or databases, which support the veracity and validity of the data submitted by the Applicant and the Subscriber with sufficient confidence, such as:

- the identity of the natural or legal person to be indicated as Subject;
- the right/power of the representative of Applicant and Subscriber to act,
- the right to dispose over the domain (address range) supported by the certificate, or over the IP address to be recorded in the certificate (in the case of website authentication - DVCP - certificate),
- the right to pursuit the regulated profession indicated in the certificate (in the case of the application for a certificate indicating a regulated profession) and
- the authentication of the identifiers and documents used for establishing the identity.

In case there is no official instrument, document or reliable data source is available for the verifications under points 4-5, Service Provider shall verify the above on the basis of a declaration recorded in a private document with full probative value.

The procedures can be deemed successful if the data submitted by the Applicant and Subscriber are precisely identical to the data set out in the instruments, documents and reliable data sources or declarations.

Before the Service Provider starts using any data source as a reliable data source or database, it shall be evaluated as regards reliability, accuracy, and resistance to change and falsification. During the evaluation, the Service Provider takes 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.

In case the registry or database contains public data on grounds of statutory provisions, Service Provider shall not carry out the above evaluation and shall deem such database or registry as reliable data source.

The Applicant and Subscriber of the end-user certificate can be the Service Provider's employee or partner; however, the Service Provider shall proceed in the same manner as in the case of any other Client. Besides the role of Applicant/Subscriber, the Service Provider's employees and partners cannot take any other part in the application and provision of the provided service.

In addition to the recorded data, the Service Provider also records the validity certified by the data source if such is interpreted (e.g. validity of an official document). The validity of the issued certificate can exceed the above validity; however, the data source must be valid at the time of signing the service agreement.

Service Provider shall provide its employees who carry out the identification and validation procedures with a detailed rules of operation regarding the means of the entity identification and data validataion procedures, the practical steps to be performed, furthermore such rules shall provide for a detailed description for the execution of the above.

3.2.1. Method to prove possession of private key

If the Applicant generates the key pair that serves the basis of the certificate, the Service Provider ensures that all technical procedures are applied that allow it to make certain that the Applicant is actually in possession of the private key paired to the public key to be included in the certificate. This can be certified, among others, with the standardised certificate application created by the Client (e.g. PKCS#10 or SPKAC CSR) or with an application based on a self-signed certificate and its submission to the Service Provider.

The certification of principal possession in this manner is valid until a valid certificate is linked to the private key.

3.2.2. Authentication of organization identity

a. Identifying the Subscriber

In the case of non natural person Subscribers, Service Provider shall use a public register or a public document supporting the incorporation and the following data for the validation of the full name and unique identifier of the Subscriber to be indicated in the certificate, and for establishing the person of the legal representative. In the lack of the above, the validation may be based on another reliable data source or legislation.

Service Provider shall use primarily the following public or reliable databases in relation to the identification of the non natural persons:

- in the case of the business associations under the Civil Code, the information provided by online company information service of OPTEN Ltd. or the online company registry provided by the online company information service of the Company Information and Electronic Company Registration Service set out in Section 1 of the Company Registration Act;
- in the case of the organizations under the Act on NGOs, the National Name Register set out in Section 84 of the Act on NGOs;
- in the case of attorneys-at-law under the Act on Attorneys, the online registry available on the website of the Hungarian Bar Association as set out in Section 116 of the Act on Attorneys;
- in the case of a public education institution under the Act on Public Education, the institution search engine that pertains to the public data of the institution master data register of the public education information system set out in the Government Decree no. a 229/2012 Korm. rendeletben, which search engine is available on the website of the Educational Authority;
- in the case of government bodies, public bodies, local governments and other state-listed legal entities under the Public Finances Act , the Master Registry available on the website of the Hungarian State Treasury, as specified in the Public Finances Act.
- in the case of the undertakings under the act on private enterpreneurs and individual companies, the online registry of private enterpreneurs operated by the Deputy State Secretariat of the Ministry of Interior for Management of Registers, as set out in the above referred act.

If the validation options above are not availeble, the Service Provider shall carry out its verification on the basis of other related public or reliable data source, and if such is not available, the public document on the founding or establishing of the organization, or the public document on appointing the respective person, or any other public document supporting the name, unique identifier, as well as the person of the representative of the other non natural person.

Service Provider shall indicate primarily the VAT number as the unique identifier of the non natural persons in the end user certificate; and if the VAT number is not included in the above enlisted registries, Service Provider shall verify the Hungarian VAT number by querying the tax subject in the official registry available on the website of the National Tax and Customs Administration. If there is only EU VAT number, it shall be verified on the website of VIES VAT number validation site of EU. In case the company registration number is used as a unique identifier, it shall be verified by the Service Provider in the above referred company registry.

An attorney-in-fact may also act on behalf of the representative of the non natural person. Service Provider shall verify the power of the attorney-in-act in accordance with Chapter 3.2.3 b.

Service Provider shall verify the other data of the non natural person to be indicated in the certificate on the basis of other reliable data source, other official documents or a power of attorney in the form of a written document. The veracity of the organizational unit of the Subscriber to be indicated in the certificate (Subject/organizationalUnitName) shall be supported by the declaration of the Subscriber regarding the existence of the organizational unit.

Authenticity of the organization unit displayed in the certificate is ensured by the statement of the Subscriber in the Service Agreement – in case the verification options above are not available.

Service Provider may require the Applicant and Subscriber to present original documents or copies (see Chapter 4.1).

b. Retention of Subscriber data:

The Service Provider stores, in its own system, the following data to be indicated as the subject of the Subscriber's certificate and to be stored in the Service Provider's records (see Chapter 9.4):

- The Subscriber's identification data (full and short name, official address, taxpayer identification number, company registration number, name of its organisational unit);
- The data of the documents used to check these (e.g. document type, identification number, validity) and originals/copies OR electronic seal and the data used to check the seal;
- The right of the Subscriber's representative to represent the Subscriber (see Chapter 3.2.3 for other representative data);
- Signed copies of the service agreement and other statements (e.g. authorisations);
- Queries and the provided responses in various records;
- The data required for contact (e.g. telephone number, e-mail address).

c. Checking other, non-personal subject data

If the Applicant requests that a 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), the Service Provider shall ascertain that the Client is in rightful possession of the name and identifier and that these are not misleading. 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 are available.

Except of the DV website authentication certificates (DVCP), because in this case only domain verification is required.

By applying for and accepting a certificate, the Client declares that the names, trademarks, and other data included therein do not violate the rights of third persons.

3.2.3. Authentication of individual identity

a. Checking the Applicant's identity

The Service Provider to check the Applicant's identity inspects the personal identification documents (or their copies) submitted to it to check their validity and authenticity and the veracity of the data provided by the Applicant.

The Service Provider also uses central registries to check the validity and authenticity of the personal identification document, including the data included therein. In the case of Hungarian natives, this shall be done trough the Central Registry of the Ministry of Internal Affairs. If the Service Provider does not know if such records are available – for example person, who is not Hungarian native -, or the price for access and performing the check is disproportionately high, the Service Provider will record this fact and will decide on the basis of the documents available to it on whether to issue the given certificate to the Applicant.

In this case, if TSP will issue the certificate, the way of verification, the documenents and/or datasources used for it must be noticed in protocol and the protocol must be preserve with other verification data.

Personal appearance of Applicant is not required for checking her/his identity.

b. Checking the identity of the Subscriber's representative or agent

If the Subscriber or its representative / agent is different than the Applicant, the service agreement shall also be signed by the Subscriber's representative / agent. A personal appearance is not necessary.

The identity of the Subscriber's representative (or, in case of joint representation, representatives) is established on the basis of the legislation, authentic records, public document certifying registry, instrument of incorporation, or trusted and regularly updated data source defined in Chapter 3.2.2. The Subscriber's agent is determined on the basis of the authorisation signed by the representative(s).

The Service Provider accepts a general authorisation (power of attorney) or an authorization conform with the sample published by the Service Provedier on its website and pertaining to the application and management of certificates, issued in the from of simple private document

The signature of the Subscriber's representative / agent as included on the service agreement and authorisation is verified on the basis of an authentic specimen signature (e.g. specimen signature drawn up in the presence of an attorney or a public notary, or, in the case of an agent, the signature on the letter of authorisation). See also Chapter 3.2.5 for more information on rights and authorisations.

The authentication of the service agreement and authorisation can be performed by other than the Subscriber, in which case it shall be authenticated with an electronic signature (the electronic signature(s) of the representative(s)); the service agreement can also be authenticated with the Agent's electronic signature. The Service Provider shall accept the its representative's or agent's valid electronic signature if their certificates were issued by a service provider included in the EU Trust List in the framework of at least an QCP-n or QCP-n-qscd (or equivalent) certificate policy (see the electronic authentication of the Applicant) and it is recognizable. Non-qualified certificates issued by the TSP are also could be accepted.

c. Checking other subject data

If titles pertaining to a regulated profession or information pertaining to company registration rights are indicated, the Service Provider shall check the pertinent data (if applicable, based on a professional certificate, authentic information described in Chapter 3.2.2, other trusted sdata sources, or documents, the data of a registry kept by a professional chamber, or other official authentic records).

The Service Provider requires that the Applicant send an email to certify the email address to be included in the certificate (or to be in contact, if not included into the certificate) (by returning the Service Provider's email or mailing the Application documents).

d. Identifying the Receiver

If the Applicant did not personally appear at the Service Provider (or receipt does not take place immediately after personal identification) and the Service Provider wishes to hand over to the Client the Client device containing the private key that the Service Provider generated, the Approved Agent shall identify the Receiver at a personal meeting with the use of photographic personal identification documents.

e. Recording Applicant, Subscriber, representative, and agent data

The Service Provider will record the data to be indicated as the certificate's Subject (based on the data sources used during the course of the above checks and records this check

The Service Provider stores, in its own system, the following data and documents pertaining to the Applicant and its representative and agent, as well as to the Receiver (see Chapter 9.4):

- The data required for unequivocally establishing the identities of the Applicant, Subscriber's representative and agent, and the Receiver, based on authentic documents;
- The Applicant's home address, based on authentic documents;
- The Applicant's data required for contact (e.g. postal address, telephone number, e-mail address).
- A signed copy of the service agreement;
- Public key of the requested certificate;
- The data of responses provided to queries in various records;
- The data of the documents used for identification and verification (e.g. document type, identification number, validity)
- The copies of the documents, certifications, and authorisations submitted during the Application, which were either provided by the Applicant or scanned by the Service Provider.

f. Miscellaneous provisions

The Applicant and the Subscriber have to acknowledge the veracity of the data provided during the identification process by signing the Service Agreement.

The Service Provider does not have to indicate an actual 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 subject data is therefore obviously not an expectation.

3.2.4. Non-verified subscriber information

Only such subject data are included in a certificate issued by the Service Provider that the Service Provider has verified (as written in Chapter 3.2), or about the authenticity of which the Applicant or Subscriber has provided a written statement beforehand in full knowledge of their liability under criminal law. If the Service Provider is unable to credibly ascertain the veracity and correctness of the data, it can deny the issuance of the certificate (see Chapter 4.2.2).

3.2.5. Control of eligibilities and delegation

If the Subscriber is a legal person, one natural person(s) may proceed at the Service Provider as Applicant. Such natural persons can be the official representative(s) of the legal person or a third person authorised by such person(s). These persons shall be identified in accordance with Chapters 3.2.3 or 3.3, and the Service Provider shall record the results of the check.

In the case of authorisations granted for specific periods of time, the fact that the expiration day has not yet been reached and (in case of legal persons) that the principal's right of representation is still valid shall be checked for each use.

If a natural person End-User is also named as the Subject of the certificate in addition to the legal person Subscriber, the Subscriber's representative(s) or agents shall grant their consent for the inclusion of the given legal and natural person's name and other data in the certificate.

If the certificate includes a full or partial right of representation (or a right that can be interpreted as such) (hereinafter jointly: right of representation), the Service Provider is obligated to ascertain the validity of the right of representation and its contents as included in the certificate before issuing the certificate, based on legislation, authentic public records, instruments of incorporation or, in absence of the above, an authorisation; the Service Provider is also obligated to record the results of the check.

If the Subject (Subject or SAN field) of the certificate is a domain name, the Service Provider verifies that the Subscriber has the right to use the domain name or has the ability to use it. The Service Provider may check the applied domain names using technical methods. (Se also Chapter 3.2.3. point b.)

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 included in the Service Policy as binding upon themselves.

The Service Provider discloses on its website all cross-certified certificates that it is the Subject or issuer of.

3.3. Identification and authentication for managing certificates

In the case of a process resulting in the issuance of a new certificate (see Chapter 4 Certificate lifecycle requirements, in particular, Subchapters 4.6 Certificate renewal, 4.7. Re-key, and 4.8 Certificate modification), Service Provider shall identify and verify the Client or clients and verify the data set out in the application in accordance with the identification procedure set out in Chapter 3.2.

In case Service Provider has already carried out the followings:

- verification of the identity of the Applicant, verification of his personal data and his right/power to act;
- vertification of the identity of the Subscriber and the verification of his identifiers and his right to use the other data to be specified in the certificate;
- verification of the identity of the person or persons entitled to represent the Subscriber;
- verification of the identity and authorization of the agent of the representative or representatives of the Subscriber;
- verification of the data to be specified as the Subject of the certificate and recorded in the registry of Service Provider; and
- verification of the possession of the private key,

then Service Provider shall repeat these procedures in accordance with the rules of initial identity validation set out in Chapter 3.2 only if the earlier validation is obsolete or not reliable, or if the data of the Applicant, Subscriber or Subject recorded earlier have changed, or if a new key pair is generated for the new certificate.

In such a case Service Provider shall repeat only that parts of the procedures, which are required for verifying the changed data or facts.

In case the application contains a new encryotion, authentication or codesign public key and/or includes the request for a new Client Device, then the provisions under Chapter 3.2.1 shall be complied with in all cases.

In case of applications for the management of website authentication certificates (DVCP), Service Provider shall repeat the verification of the data and the identification at least in every 27 months.

3.3.1. Identification and certification in the case of a valid certificate

In case the data required to be verified for the issuance of the requested certificate are identical to the data verified prior to the issuance of the certificate issued for the Client at an earlier date, and that earlier certificate is still valid at the time of the application of the new certificate, Service Provider does not carry out the verification of such data.

3.3.2. Identification and certification in the case of an invalid certificate

Service Provider shall not accept the service agreement, authorization (power of attorney) or any other document signed or stamped with an invalid certificate.

3.4. Identification and authentication for status change request

The Service Provider provides certificate revocation, suspension, and reactivation services. The Service Provider always identifies the applicant of the status change and ascertains that they have authorisation to perform the given action.

The Applicant's authorisation is checked as per Chapter 4.9.2 and the action is processed as per Chapter 4.9.4. The Service Provider identifies the Applicant of the status change as set forth below for the certificate's Applicant and Subscriber:

CHANNEL	IDENTIFICATION OF THE APPLICANT FOR STATUS CHANGE
Client Menu (Only for suspension requests)	Enter user name and password.
Phone	Of the personal information recorded in the client menu registration, at least three different pieces of information have to be checked. Identification is considered successful if all three pieces of information provided by the applicant are the same as those recorded in the client menu registration.

In case of being contacted by the authorities, identification takes place on the basis of the body's official (electronic or traditional) seal or its electronic signature.

4. Certificate lifecycle requirements

The present Chapter 4 describes the actions that manage the lifecycles of the certificate issued by the Service Provider.

The certificate's lifecycle extends from the application for and the issuance of the certificate until its expiration or revocation. During this time, there is a possibility for suspending, activating, or modifying the certificate (if applicable in the case of the given certificate policy (see Chapter 1.2.1)

or key use (see Chapter 7.1.2)) or replacing the certificate's keys. The Service Provider ensures that the Relying parties can also apply for certificates for testing (see Chapter 7.1). Of the rules set out in the present Chapter 4, only those rules are applicable to test certificates where explicitly indicated by the text of the Statement.

4.1. Certificate enrolment

The conditions and method laid out in the present Statement can only be used to apply for the services defined in Chapter 1.1. to request certificates written in Chapter 1.2.1

The present Chapter 4.1 describes only the procedures pertaining to original certificate applications. The certificate issuance that takes place in the framework of renewal, modification, or re-key applications is described in the appropriate Chapters (4.6-8).

The certificate application submitted previously to the Service Provider's Registration Authority by the Applicant is required for the issuance of all end-user certificates (see Chapter 1.3.2).

The Service Provider provides easy-to-understand information in its regulations and/or on its website (see Chapter 1.1.2) regarding:

- the non-eIDAS nature of the certificates that can be applied for and the legal effects related to their application;
- their use (see Chapter 1.4);
- the business and legal information pertaining to the service (see Chapter 9);
- the conditions for concluding the Service Agreement;
- the rights and obligations of the Parties;
- the parts of the Service Provider's General Terms and Conditions (GTC) that pertain to services related to certificates;
- the security measures necessary in relation to the use of private keys;
- the use of the Client device, if the Applicant acquired such from the Service Provider.

Following the conclusion of the service agreement, the Service Provider will send an email to the Applicant's email address provided in the application (see Chapter 4.1.2) with the relevant version of the Practice Statement, the Service Policy and the Service Agreement; according to relevant legislation, this email address qualifies as a durable medium.

4.1.1. Who can submit a certificate application

The following parties can apply for end-user certificates in accordance with the requested profile:

CERTIFICATE PROFILE (See Chapter 7.1.)	APPLICANT
PERSONAL PROFILE	The natural person indicated as the Subject of the certificate, on behalf of itself.
PSEUDONYM PROFILE	The pseudonym indicated by the natural person as the Subject of the certificate, on behalf of itself.
BUSINESS PROFILE	The natural person indicated as the Subject of the certificate, on behalf of itself, in certification of the fact that the organization also indicated as the subject of the

	certificate granted its consent for the certificate application. OR According to the preliminary agreement between the Service Provider and the Client, the representative or agent of the organization indicated as the Subject of the certificate, naming the natural person whose data it also wishes to indicate as the Subject of the certificate.
ORGANISATIONAL PROFILE	The representative or agent of the legal person indicated as the Subject of the certificate. OR The representative or agent of the legal person holding the trademark indicated as the Subject of the certificate.
DV WEBSITE AUTHENTICATION PROFILE	The natural person who has the control of the domain.

Any natural person can apply for a certificate for testing purposes (see Chapter 7.1) with any profile on behalf of itself, the organisation it represents, or its device.

The Service Provider manages a risk list of the natural and legal 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.

4.1.2. Enrolment process and responsibilities

The certificate enrolment process starts with the application submitted by the Applicant to the Service Provider's Registration Authority and ends with the issuance of the certificate. During the course of this process, the Applicant is liable for the veracity of the data included in the application and the Service Provider is responsible for checking those and correctly displaying the certificate subject data.

a. Client System Registration and Certificate enrolment

The application for the issuance of encryption, authentication or codesign (LCP, NCP, NCP+) certificate may be initiated following the registration (see below) with the Client Menu available on the Website of the Service Provider, by signing in the Client Menu and selecting the certification application function and submitting the data requested by the system (see below). In the case of the service plans set out in the GTC the Application may be initiated by filling and sending the plan order forms available on the website of Service Provider. In this case the registration with the Client Menu (see below) and the recording of the application in the system of Service Provider (see below) takes place on the basis of the data submitted to Service Provider in the order form.

The application for the issuance of DV website authentication (DVCP) certificate may be initiated on onlinessl.netlock.hu available on the Website of the Service Provider.

The Client can initiate its application for a test certificate (see Chapter 7.1) by sending an email to the Service Provider's Registration Authority (see Chapter 1.1.2). The application, after agreed upon with the Client, can be performed if approved by the Service Provider's Legal Department. Following negotiations with the Service Provider's Internal Auditors, any of the Service Provider's employees can request a test certificate for the purposes of internal testing.

The Service Provider can deviate from the above methods of Client menu registration and certification application if agreed upon with the Client (e.g. if certificates are requested en masse).

During the certificate application process, the Service Provider uses the data provided when registering in the client menu and applying for a certificate to prepare, and then send to the Applicant in an electronic format, the service agreement applicable to the issuance of the requested certificate.

Registration in the Client menu and the certificate application process, which are required for certificate enrolment, are partially automated processes but also require human intervention. The steps that the Applicant has to take during these processes are discussed in detail in the guidelines available on the Service Provider's website.

i. Data recorded in the course of the registration with the Client Menu

Service Provider recordes the data required for certificate applications and for contacting the Applicant and the Subscriber.

In the course of the registration of Applicant with the personal Client Menu Service Provider records and retains the following data in its IT system:

- name (mandatory);
- identity card number (mandatory)
- country of home address (mandatory);
- city of home address (mandatory);
- postal code, street and house number of home address (optional);
- phone/fax number (mandatory);
- e-mail address(mandatory);
- login name (mandatory);
- password (mandatory);
- password reminder (optional).

In case a certificate is requested for a legal person (in case of organisational or business profile, see Chapter 7.1), the following data shall also be recorded:

- name (mandatory);
- country of registered address (mandatory);
- city of registered address (mandatory);
- postal code, street and house number of registered address (optional);
- phone/fax number (optional);
- e-mail address (mandatory).

ii. Information required and recorded for certificate enrolment

Certificate enrolment can be initiated by submitting the following data (as part of the application or documents) in accordance with the requested certificate profile. Furthermore, the Subscriber's data required for contract conclusion and invoicing are also required, regardless of the certificate profile and the Applicant's name and password.

CERTIFICATE PROFILE (see Chapter 7.1)	REQUIRED DATA*
PERSONAL PROFILE	The data of the natural person indicated as the Subject of the certificate: ● number of the personal identification document; ● the family and given name(s) included in the personal identification document; ● the home address or residence in the official address certification; ● e-mail address.
PSEUDONYM PROFILE	● The data of the natural person applying for the certificate, as in the case of the personal profile. ● The pseudonym to be used in the certificate.
BUSINESS PROFILE	● The data of the natural person to be indicated as the Subject of the certificate, as in the case of the personal profile (except address). ● The data of the legal person to be indicated as the Subejct of the certificate and the data of its representative agent, as in the case of organisational profile.
ORGANISATIONAL PROFILE	The data of the organizasion indicated as the Subject of the certificate: ● the name indicated in the identification document; ● the registered address indicated in the identification document; ● the name of the organizational unit (optional); ● e-mail address; ● taxpayer identification number; ● the following data of the representative(s) or agent of the organization ○ name ○ e-mail address.
DV WEBSITE AUTHENTICATING PROFILE	The submission of the domain name(s) to be indicated as the Subject of the certificate

When applying for a certificate for testing (see Chapter 7.1), the Applicant has to provide the purpose of the testing and the profile of the certificate to be tested.

iii. Submission of documents

In case a public document or any other official document is needed for the identification of any identity set out in any certificate application under Chapter 3, or for the verification of any right or power, or of any data to be included in the certificate, Applicant shall also present these documents to the Service Provider following the submission of the application. Service Provider shall, after recording the application, provide the Applicant with precise information on the documents to be presented. Applicant may send the copies of the documents in advance to the dedicated e-mail address (see Chapter 1.1.2).

iv. Additional conditions for certificate enrolment

1. In addition to the above, the Applicant also has to indicate
    a. the planned use of the certificate,
    b. the type of Subscriber (private person, company, government, or other),
    c. and also has to submit the service agreement, authenticated as described in Chapter 4.2.1, to the Service Provider.
2. By signing the service agreement, the Client declares the following:
    a. its personal information included in the agreement are true and that it provided those to the Service Provider voluntarily;

b. it has familiarized itself with, understands, and accepts the General Terms and Conditions, the present Practice Statement applicable to the requested certificate, and the Service Provider's Service Policy, which are available on the Service Provider's website;

c. prior to the conclusion of the agreement, it has received the information as required by relevant legislation and has understood the limitations pertaining to the certificate (e.g. key use or the undertaking of liability by the Service Provider);

d. it authorises the Service Provider to issue the certificate indicated in the service agreement.

3. By signing the service agreement, the Client furthermore certifies the following:

a. it grants its consent for the handling of the data provided when registering in the client menu and in its Application;

b. it requests the authentication of the public key set out in the agreement and its registry, storage, and handling in the certificate's public certificate repository (see also Chapter 4.4.2);

c. it is familiar with the rights and obligations of the contracting parties.

4. If an organization is named as the certificate Subject, its representative or agent declares the following in the service agreement or - if such is attached separately to the service agreement - in the annex to the service agreement:

a. the certificate enrolment is taking place with its knowledge and consent;

b. it authorizes the Applicant to apply for the certificate, or

i. with its suspension, revocation, or activation (4.9),
ii. renewal (4.6),
iii. modification (4.8),
iv. to proceed in the re-key process (4.7);

c. it undertakes to pay the service fees incurred in relation to the agreement;

d. it has familiarized itself with, understands, and accepts the GTC, the present Practice Statement applicable to the requested certificate, and the Service Policy, which are available on the Service Provider's website (see Chapter 1.1.2).

b. Responsibilities of Clients

During Application, the Applicant is responsible for exactly providing the data discussed in the present Chapter (4.1.2), for familiarising itself with the information sent by the Service Provider via email, and taking the steps requested by the Service Provider. If the present Statement requires the certification of identity for the issuance of the requested certificate, the Applicant is responsible for such certification as per Chapter 3.

The service agreement has to be signed by the Applicant and the Subscriber, as set out in Chapter 4.2.1. Except the website authentication (DVCP) certificates, where the service agreement is undefined.

4.2. Certificate application processing

The rules of the present Chapter (4.2) apply to applying for new certificates (Chapter 4.1) and to the processing of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7) - also including the identification-authentication procedure that precedes Certificate issuance, the acceptance or rejection of the issued certificate by the Client, and the duration of

processing. The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for processing any requests.

When processing a certificate application, the Registration Authority's trusted employees check the personal and organisational data provided during registration in the Client Menu and certificate enrolment or when filling out the electronic order form; they also identify the Applicant and his right to proceed and - in case of device order - generate the key pair and prepare the service agreement.

During the Application, the Service Provider also checks the trueness of the provided email address by requesting confirmation of certificate enrolment from this address and forwarding instructions and information to this address, the performance by and knowledge of which by the Applicant are essential for conducting the certificate enrolment process.

If, based on the application or the Service Provider's offer, the private key is generated for a Client device provided by the SP, the Service Provider will generate the key during the processing of the application (see Chapter 6.1), after which it compiles a package containing:

- the Client device and, if required for its use, the Client device reader;
- the information required for the first use of the Client device.

The Service Provider will inform the Client on the completion of the package (Client device, reader, and information) by sending an email to the address provided during the Application. The Receiver can then take over the package at the place and with the method provided in the email.

The rules above are not applicable in case of DV website authentication (DVCP) certificates. Therefore the rules in the subchapter below should be applicable only if the given action does not require human intervention.

4.2.1. Performing identification and authentication functions

If the Applicant has provided all information and data during the certificate application process and has also submitted the copies of all documents required for their certification (which are to be handed over or sent to the Service Provider in accordance with the requested certificate profile as per the present Statement (see Chapter 4.1.2)), the Service Provider's Registration Authority performs the identification and authentication tasks that are to be completed before Certificate issuance.

The Service Provider's Registration Authority uses independent sources to check, in accordance with Chapter 3, the data submitted or acquired during the application and the Applicant's identity and right to proceed. Registration Administrators perform the identification and authentication procedure in line with the requirements pertaining to the work processes included in the Registration Authority's internal regulations. These internal regulations may set forth additional requirements (not discussed in this Statement) for identifying certificate applications that the Service Provider considers to be high-risk and for which supplemental control procedures are required.

See Chapters 3.2 and 3.3 regarding the identification of the Applicant and the Subscriber.

c. Certification of the Service Agreement and submitting it to the Service Provider

The Service Agreement has to be authenticated by the Applicant and, if applicable, the Subscriber prior to every certificate issuance, even if the certificate was issued on the basis of a data check performed earlier.

The service agreement includes 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 agreement can be authenticated and submitted in hard copy format with a handwritten signature or electronically with an electronic signature and, if applicable, an electronic seal.

The Applicant has to sign the hard copy of the service agreement in the same manner as the handwritten signature on the personal identification document. If the Subscriber is different than the Applicant, it has to sign the hard copy of the authorisation by way of its representative or agent with the same signature used on the submitted specimen signature (see Chapter 3.2.3).

If the service agreement is authenticated electronically, the personal identification data in the certificate used for the signature have to be the same as the personal data of the Applicant / Subscriber indicated in the service agreement or the unequivocal certificate identification data indicated in the authorisation. The Subscriber can also use a seal for authentication. In this case, the organisation identification data indicated in the seal have to be the same as the Subscriber data included in the service agreement.

If the authorisation does not form a part of the service agreement but is a separate document, the method used to sign the agreement and the authorisation may differ, i.e. one can be hard copy-based and the other can be electronic.

The Applicant cannot authorise others to sign the service agreement; however, an authorised person can also sign the service agreement on behalf of the Subscriber.

The Applicant cannot authorise others to sign the service agreement; however, an authorised person can also sign the service agreement on behalf of the Subscriber.

In the case of website authentication certificates (DVCP), the Service Provider shall carry out CAA verification.

In the course of the CAA verification the Service Provider shall query the CAA record of the domain.

Service Provider deems that the certificate is authorized in the following cases:

- in the case of non wildcard domain, the CAA record issue contains „netlock.hu", „netlock.net" or „netlock.eu";
- in the case of wildcard domain, the CAA record issuewild contains „netlock.hu", „netlock.net" or „netlock.eu".
- the CAA record is unavailable.

In case the CAA record contains issue or issuewild, but it is empty, Service Provider shall refuse the issue of the certificate.

4.2.2. Approval or rejection of certificate applications

The Service Provider certifies receipt of the Application by sending an automatic reply to the email address provided during the Application. The automatic response does not mean that the Service Provider has accepted the Application and merely serves to inform the Client that the Service Provider's Registration Authority has received the Application and it will commence its processing.

The Service Provider's Registration Authority decides on its acceptance or rejection during the processing of the certificate application. The Registration Authority will accept the certificate

application if the identification and authentication steps set out in Chapter 4.2.1 have been successfully completed. i.e.

- the Applicant's person has been successfully identified;
- the data provided as the certificate subject have been checked and found to be true;
- the service agreement has been properly signed (if applicable).

If identification and authentication were successful and the signed service agreement has been accepted, the Registration Administrator performing the check approves the certificate application.

The Service Provider will call upon the Applicant to submit missing information if the identification and authentication steps set out in Chapter 4.2.1 are unsuccessful because

- the Service Provider does not have all the data or documents at its disposal to process the Application (see Chapter 4.1.2), *or*
- the available data are not authentic or their authenticity cannot be determined, *or*
- the Applicant's right to apply for the certificate cannot be established.

The Service Provider will reject or delete the certificate application if the identification and authentication steps set out in Chapter 4.2.1 are unsuccessful because

- the data provided in the application are false, *or*
- the Applicant is not authorised to submit the given certificate application, *or*
- the requested missing information is not submitted within 30 calendar day of the request.

Additional circumstances that can lead to the rejection or deletion of the certificate application:

- General, business, and legal conditions:
  - the service fee has not been paid by the deadline set out in the GTC;
  - the Subscriber has overdue amounts for any services under the present Statement;
  - the authorised party does not receive the Client device within 30 days of being notified;
  - final liquidation or settlement proceedings are under way against the organization indicated as the certificate subject;
  - the entity(-ies) indicated as the certificate subject and/or the Applicant's home/registered address are in a country subjected to a technological or economic embargo imposed by Hungary or the European Union.
- Circumstances regarding identification and authentication:
  - the relationship between the entity(-ies) indicated as the certificate subject and the Applicant/Subscriber is not clear;
  - the Applicant's right to apply for the certificate is not clear;
  - doubts arise regarding the originality, trueness, or validity of the data provided in the certificate application;
  - doubts arise regarding the originality, trueness, or validity of the documents submitted in their original or copies thereof to certify the data provided in the certificate application;
  - the Applicant and/or Subscriber do not grant consent for reproducing and/or storing reproductions of the documents presented for the purposes of verifying the data provided in the certificate application;
  - the subject of the certificate application is the issuance of a certificate containing the data of an organisation without legal personality or an association;
  - other conditions violating the Service Provider's regulations.

The Applicant will be notified of rejected applications and of the reason therefor.

The Service Provider will not issue certificates (DVCP) for certain domain endings (which are defined in its internal regulations) and internal domain names; it automatically rejects applications containing such domain names.

4.2.3. Time to process certificate applications

The certificate application will be considered processed once the certificate has been issued or rejected by the Service Provider.

The Service Provider will process the certificate application within 14 days of having sent the automatic email confirming that the certificate application process has been started. The Service Provider will generally issue the certificate within an additional 3-5 workdays if the conditions for issuing the certificate have been met.

In case of a request for missing information, the duration of the request for missing information is not part of the deadline for processing the certificate application.

4.3. Certificate issuance

The rules of the present Chapter (4.3) apply to applying for new certificates (Chapter 4.1) and to the processing of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7) - also including the Service Provider's activities conducted during certificate issuance and informing the End-User on certificate issuance. The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for certificate issuance conducted on the basis of modification, renewal, or re-key requests.

The time of certificate issuance is the time when the Service Provider makes the signed certificate available in the Client Menu; the start of the certificate's validity can differ from this time.

a. The issuance of end-user certificates

A condition for issuing an end-user certificate is the submission by the Applicant of a certificate application (as defined in Chapter 4.1) to the Service Provider. The Service Provider will only issue the certificate if the application has been processed as set out in Chapter 4.2.

A certificate application approved by the Service Provider's Registration Authority is submitted to the Service Provider's Certification Authority, that takes the steps necessary for the issuance of the certificate. The Service Provider can only issue the certificate with the data provided during the application process. Website authentication (DVCP) certificates are issued by automatic system without human interaction, after domain control check and payment.

A DV weboldal-hitelesítő tanúsítványok kiadását automata rendszer végzi, humán beavatkozás nélkül, a domain kontroll ellenőrzése és a díjfizetés sikeressége esetén.

Payment is due before certificate issuance in the manner defined in the GTC. The Service Provider can also agree with the Subscriber differently, in which case the Service Provider can create and issue the certificate before the payment of the service fee and can also set a deadline by which the Subscriber has to pay the service fee.

The End-User can start using the keys after the issuance of the certificate, as set forth below:

CERTIFICATE	KEYS AND THE USE OF THE CERTIFICATE
SOFTWARE-BASED CERTIFICATE	In the case of a software-based certificate, the Applicant generates the key itself on its own computer. Following its issuance, the End-User has to install the certificate on its computer as shown by the instructions available on the Service Provider's website. The keys and the certificate can then be used.
DEVICE-BASED CERTIFICATE	The Service Provider will only hand over the ordered Client device to an authorised Receiver. Following its issuance, the End-User has to upload the certificate to the device as shown by the instructions available on the Service Provider's website. The keys and the certificate can then be used. If the keys included in the certificate were generated by the Service Provider during the course of the application, the certificate can only be issued if the Service Provider has ascertained that the authorised Receiver has received the Client device. However, the Service Provider may, based on a preliminary agreement concluded with the Applicant, issue the certificate and upload it to the device in a suspended state before handing it over. In this case, the End-User shall activate the certificate without delay, but no later than by the deadline set out in Chapter 4.9.13. The keys and the certificate can then be used.
DV SSL	In the case of an SSL certificate, the Applicant generates the key pair itself on the server to be authenticated. The keys and the certificate can then be used after the certificate has been installed on the server.

b. The issuance of TSP certificates

TSP certificates are issued in the manner defined in the Service Provider's Security Regulations and with the control of at least two trusted employees; records shall also be drawn up. The Service Provider publishes TSP certificates in the manner and by the deadline set out in Chapter 2.2.

4.3.1. TSP actions during certificate issuance

a. End-user certificates

Based on the data provided during the application, the Service Provider creates the certificate in its IT system and, after the service agreement has been signed and approved, certifies it with its TSP certificate. The certificate will then be made available to the End-User in the client menu and, the NETLOCK sign system. Unless the Applicant requests otherwise, the certificate will then also be available in the public certificate repository (see Chapter 4.4.2). During these activities (i.e. issuance), the Service Provider ensures that the entire process is secure, thus preventing the certificates from being falsified.

Unless the Service Provider and Subscriber agree beforehand, the certificate can only be issued following the payment of the service fee; the Service Provider will therefore prepare, based on

the invoicing data provided during the application, the hard copy or electronic invoice or the proforma invoice required for payment of the service fee and will mail it to the invoicing/email address provided in the application (see the GTC) before issuing the certificate. In some cases fees are payable online by credit card – in case of DV website authentication certificates it is exclusively.

b. TSP certificates

Simultaneously to making the certificate available, the Service Provider also publishes a brief description of the purpose of the TSP CA certificate. The certificates may be downloaded from the public certificate repository of Service Provider. During these activities (i.e. issuance), the Service Provider ensures that the entire process is secure, thus preventing the certificates from being falsified.

4.3.2. Notification by the TSP of issuance of certificate

The Service Provider notifies the End-User on the issuance of the certificate - no later than the day the certificate becomes valid - by sending an email to the address in the certificate. If the Service Provider issues a certificate that also certifies a right of representation, the Service Provider will inform the Client on the issuance of the certificate without delay.

4.4. Certificate acceptance

The rules of the present Chapter (4.4) apply to applying for new certificates (Chapter 4.1) and to the certificates issued on the basis of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7). The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for certificate issuance conducted on the basis of modification, renewal, or re-key requests.

4.4.1. Conduct constituting certificate acceptance

Before downloading or activating the certificate or starting to use the private key, the Client is obligated to check the veracity of the data in the certificate. The End-User can view the certificate data by logging into the Client Menu. If it discovers any irregularities or deviations, it cannot start using the certificate or private key and is to notify the Service Provider’s Customer Service immediately about its objection; it shall then take the steps necessary for revoking/suspending the certificate (see Chapter 4.9).

The Client has to check whether the private key and the certificate are connected by executing the task for which the key is intended and by verifying the action with a certificate.

In case of device-based certificates, the Service Provider will consider the certificate, the connected public key, and the private key paired to be accepted if the Client does not raise any objections at the Service Provider within 5 workdays of the receipt of the Client device or does not initiate its revocation or suspension. In other cases, the Service Provider will consider the end-user certificate to be accepted by the Client 5 workdays after certificate issuance.

4.4.2. Publication of the certificate by the TSP

Following the issuance of the end-user certificate, the Service Provider will publish it in the public certificate repository unless the certificate’s Applicant has requested otherwise. The Applicant can submit such requests to the Service Provider’s Registration Authority by email during the processing of the certificate application.

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

a. End-user certificates

The Service Provider does not notify any other actors on certificate issuance besides those set out in Chapter 4.3.2.

b. TSP certificates

The Service Provider publishes information on the issuance of TSP certificates on its website (see Chapter 1.1.2).

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The Certificate and the private key paired to the public key included in the Certificate can be used for the purposes defined in the “Key Usage” and “ExtendedKeyUsage” fields, in line with Chapters 7.1 and 1.4.

Other requirements for the use of the certificate:

- If the key was generated for a cryptographic device, the End-User can only activate and use the private key on the device for which it was generated.
- If the key was generated for a cryptographic device, the End-User can only activate and use the private key on the device over which it has control.
- The private key has to be under the sole control of the End-User.
- The use of expired, revoked, or suspended certificates or related keys is not permitted.
- If the End-User makes a copy of the private key, it has to handle the copy with the same level of diligence as the original copy.
- The End-User is obligated to inform 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:
    - 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.
- If the TSP key used to sign the end-user certificate becomes compromised, the End-User is obligated to immediately terminate the use of the private key and the certificate.
- See Chapter 6.2.10 if the certificate expires or is revoked.

4.5.2. Relying party public key and certificate usage

When using the certificate, the Relying Party’s circumspect procedure is a requisite for maintaining the security level guaranteed by the Service Provider: the Relying Party shall proceed in line with the Service Provider’s regulations, with especial regard to the following:

- it is to only accept public keys in case of use that is in line with the Certificate’s “KeyUsage” and “ExtendedKeyUsage” fields (see Chapter 7.1.);
- it is to check certificate validity and status (see Chapter 4.9.6.);
- it is to take into account all restrictions that are included in the certificate or the regulations referred to by the certificate (see Chapters 1.4 and 6.1.7.);
- it shall only use trusted software for using keys and certificates.

If the Relying Party does not proceed in line with the Service Provider's regulations, the Service Provider does not assume liability for the resulting damages.

4.6. Certificate renewal

The Client may request the certificate provided by the SP to be renewed before the expiration of its validity. During the course of renewal, the Service Provider generates a new certificate with the public key in the certificate to be renewed and based on the Subject data.

In case of renewal, the Client cannot request that the Subject data be modified; however, the certificate's other data can change (e.g. certificate serial number and validity, Service Provider data, CRL/OCSP information).

The Service Provider can initiate the renewal of end-user certificates at any time at its own discretion.

End-user certificates can be renewed more than once; the Service Provider is authorised to reject requests for renewal.

4.6.1. Circumstance for certificate renewal

The Client can request that its certificate be renewed if the following conditions are met:

- the certificate is valid;
- the validity of the certificate will expire in no more than 30 days;
- the public key used in the certificate can still be considered to be cryptographically secure and is expected to remain such during the validity of the renewed certificate;
- the private key paired to the public key included in the certificate has not been compromised.

No more than 30 days before the expiration of the certificate, the Service Provider sends an email to the address included in the certificate, in which it informs the Client on the approaching expiration date and the process for certificate renewal / applying for a new certificate.

An application for certificate renewal can be submitted following the instructions available on the Service Provider's website or, based on a previous agreement, by other means in writing.

The Service Provider can initiate the renewal of an end-user certificate at its own discretion if the following conditions are met:

- the certificate is valid;
- the certificate is to be revoked before the expiration of its original validity due to an external circumstance (e.g. a change in legislation or a supervisory decision) and the renewal can ensure that the certificate will meet the new conditions;
- the public key used in the certificate can still be considered to be cryptographically secure and is expected to remain such during the validity of the renewed certificate.

The Service Provider will send a notification to the email address provided in the certificate regarding the end-user certificate renewal it initiates.

The conditions for renewing TSP certificates:

- the certificate is valid;
- the certificate was not issued with the renewal of a previously issued certificate.

4.6.2. Who may request renewal

Renewals of end-user certificates can be requested by the Service Provider or the Applicant or Subscriber of the certificate that is to be renewed.

4.6.3. Processing certificate renewal requests

The Service Provider certifies the receipt of the application for certificate renewal by sending an automatic reply to the email address included in the certificate. The automatic response does not mean that the Service Provider has accepted the Application and merely serves to inform the Applicant that the Service Provider's Registration Authority has received the application and it will commence its processing.

The certificate renewal process is partially an automated process, but it also requires human intervention. During the application for renewal, the Service Provider sends instructions and information to the email address in the certificate, the performance by and knowledge of which by the Applicant are essential for conducting the certificate renewal process. The steps that the Applicant has to take during the renewal process are discussed in detail in the guidelines available on the Service Provider's website.

During the renewal application process, the Applicant has to provide its invoicing data and the data required for preparing the new service agreement. The Service Provider sends the service agreement to the Applicant in an electronic format.

a. Identification and authentication

In case of an application for certificate renewal, the identification of the Applicant and the signing and forwarding to the Service Provider of the service agreement necessary for the issuance of the renewed certificate take place as set out in Chapter 4.2.1.

During renewal, the Applicant declares the following by signing the service agreement (if applicable):

- the data checked when the original certificate was issued has remained unchanged;
- the documents that certified the veracity of its data at the time are still valid;
- it is not aware of the certificate private key having been compromised.

b. Approval or rejection of renewal applications

The Service Provider decides on the acceptance or rejection of a renewal application during its processing. The Service Provider will accept the certificate application if the identification and authentication steps set out in Chapter 4.6.3.1 have been successfully completed.

The renewal application will be considered complete and authentic once the service agreement has been signed. The Service Provider will not sign the service agreement, but will indicate its acceptance by issuing the renewed certificate.

The trusted employee of the Service Provider's Registration Authority will check whether the renewal application is complete and the service agreement is correct and authentic. If the data provided when applying for a renewal are incomplete and/or the service agreement is incorrect, unsuitably authenticated, or its authentication cannot be established, the Service Provider's Registration Authority will call upon the Applicant to submit missing information.

The Service Provider can reject the request for renewal if the following conditions are met:

- the missing information requested by the Service Provider is not provided by the expiration of the certificate that is to be renewed;
- during the course of processing the application, the Service Provider finds out that the data checked when the original certificate was issued have since become invalid, in which case the Service Provider will revoke the certificate to be renewed (see Chapter 4.9);
- during the course of processing the application, the Service Provider finds out that the private key of the certificate to be renewed has become compromised, in which case the Service Provider will immediately implement measures to revoke the certificate;
- any conditions that can result in the rejection of a certificate application and are also applicable to renewal;
- the Client owes overdue payments for an invoice issued for any of the Service Provider's services;
- the certificate to be renewed cannot be unequivocally identified.

The Service Provider can reject the renewal of the certificate with other reasons set out in writing (e.g. supervisory decision).

If the renewal request is rejected, the Client can maintain the continuity of the services by applying for a new certificate.

c. Time to process renewal applications

The Service Provider processes certificate renewal requests with the time set out in Chapter 4.2.3. In case of a request for missing information, the duration of the request for missing information is not part of the deadline for processing the renewal application.

d. Issuance of the renewed certificate

If the applicable conditions are met, the Service Provider will issue the renewed certificate 2-10 workdays before the expiration of the original certificate, unless agreed upon otherwise by the Service Provider and the Client.

The Service Provider does not assume liability if the renewed certificate is not issued before the expiration of the original certificate and the continuity of the service is interrupted if such was caused by the Client's omission or delay.

See also Chapter 4.3.

4.6.4. Notification of new certificate issuance to subscriber

The Service Provider will notify the Client on the issuance of the renewed certificate in the manner set out in Chapter 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the renewed certificate.

4.6.6. Publication of the renewal certificate by the TSP

The provisions of Chapter 4.4.2 are applicable to the publication of the renewed certificate.

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

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.7. Re-key

The Client is provided with the possibility of requesting the replacement of the public key and its private key pair before the expiration of the validity of its certificate provided by the SP. During the course of the re-key, the Client will generate a new key pair on behalf of itself or the Service Provider will generate one for it, after which the Service Provider will create a new certificate (including the new public key) with the use of the subject data included in the certificate on which the re-key is based. The Client has to destroy the private key belonging to the revoked certificate (see Chapter 6.2.10).

In case of a re-key, the Client cannot request that any data besides the key be modified; however, the certificate's other data can change (e.g. serial number, Service Provider data, CRL/OCSP information).

The Client can request the re-key in writing; information on the method for submitting the application is found on the Service Provider's website. In addition to the written request, the Applicant also has to initiate a new certificate application (as set out in Chapter 4.1.2) in order to start the re-key process.

The Service Provider may initiate the re-key of end-user certificates at its own discretion at any time. The Service Provider will inform the Client of re-keys performed at its own discretion by sending an email to the address in the certificate.

Re-keys are possible for both valid and revoked (e.g. due to a compromised key) certificates.

4.7.1. Circumstance for certificate re-key

The Client can initiate the replacement of the key pair belonging to the certificate within the validity of the certificate.

The Service Provider can initiate the replacement of the keys of an end-user certificate if the key pair can no longer be considered to be cryptographically secure or it is forced to do so by an external circumstance (e.g. a change in legislation or a supervisory decision).

The Service Provider will send a notification to the email address provided in the certificate regarding the end-user certificate re-key it initiates.

4.7.2. Who may request certification of a new public key

The provisions of Chapter 4.6.2 are applicable to re-key applications.

4.7.3. Processing certificate re-keying requests

The provisions of Chapter 4.6.3 are applicable to processing requests for certificate modification, with the deviation that the valid status of the certificate and the non-compromised private key is not a prerequisite.

4.7.4. Notification of new certificate issuance to subscriber

The provisions of Chapter 4.3.2 are applicable to notifying the Client.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the certificate.

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

The provisions of Chapter 4.4.2 are applicable to the publication of the certificate.

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

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.8. Certificate modification

The Client has to request the modification of its certificate provided by the SP within its validity if its subject data change within its validity.

During the course of certificate modification, the Service Provider creates a new certificate with the public key in the certificate to be modified and with the subject data modified according to the application. If the certificate on which the modification request is based contains invalid data because of a change in such data, the Service Provider will revoke the certificate during the modification process (see Chapter 4.9).

If the modification request takes place in the 30-day period prior to the expiration of the validity of the certificate for which the application is submitted, the modification is considered to also be a request for renewal (see Chapter 4.6). In this case, Chapter 4.6 is governing regarding the validity period of the new certificate.

In case of a modification, the certificate's other data can also change (e.g. certificate serial number and validity, Service Provider data, CRL/OCSP information) in addition to the requested change in subject data.

The Service Provider may also initiate the modification of end-user certificates at its own discretion at any time. The Service Provider will inform the Client of the above by sending an email to the address in the certificate. In this case, the Service Provider will determine the validity period of the new certificate.

An application for certificate modification can be submitted by the Client following the instructions available on the Service Provider's website or, based on a previous agreement, by other means that take place in writing.

End-user certificates can be modified more than once; the Service Provider is authorised to reject requests for modification.

4.8.1. Circumstance for certificate modification

The provisions of Chapter 4.6.1 are applicable to the circumstances of certificate modification, with the difference that the modification request can be initiated at any time within the certificate's validity period.

4.8.2. Who may request certificate modification

The provisions of Chapter 4.6.2 are applicable to Applicants of certificate modification.

4.8.3. Processing certificate modification requests

The provisions of Chapter 4.6.3 are applicable to processing requests for certificate modification, with the following deviations:

- the Service Provider's Registration Authority will check the changed subject data as defined in Chapter 4.2.1;
- the statement on the fact that the subject data remained unchanged and the validity of the documents presented at the time of the original check does not pertain to the changed data;
- the Service Provider will not reject the application due to the invalidity of the data certified at the time of issuing the original certificate.

4.8.4. Notification of new certificate issuance to subscriber

The Service Provider will notify the Client on the issuance of the modified certificate in the manner set out in Chapter 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the renewed certificate.

4.8.6. Publication of the modified certificate by the TSP

The provisions of Chapter 4.4.2 are applicable to the publication of the modified certificate.

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

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.9. Certificate status change

The Client may request the status of its certification to be changed before the expiration of its validity. The request for status change can include the suspension, activation, or revocation of the certificate (see *Chapter 1.6.1 Definitions* of the *Service Policy*).

In case of a status change request, the Service Provider will change the status of the certificate subject to the request on the basis of the application, as set forth below:

- only active certificates can be suspended;
- only suspended certificates can be activated;
- valid and suspended certificates can be revoked.

A suspension is for a fixed term, within which time the Client is to revoke or reactivate the certificate; otherwise, the Service Provider will revoke the certificate at the end of the period. A suspended certificate will once again become valid after activation, and will then also be considered valid for the term of the suspension. The revocation permanently invalidates a certificate from the moment of its revocation (or its preceding suspension).

The revocation or suspension can pertain to both end-user certificates and TSP certificates.

The subscriber and activation is not applicable in the case of certificates for website authentication certificates (DVCP).

4.9.1. Circumstances for revocation and suspension

The Service Provider will evaluate the request for the revocation/suspension no later than within 24 hours of its receipt by taking into account the following circumstances; based on the evaluation, it will revoke or suspend the end-user certificate or will reject the application for revocation/suspension. The following circumstances may serve as basis of the revocation or

suspension of the end user certificates. In the following cases Service Provider shall revoke or suspend the certificate not later than within 24 hours from the receipt of the Request:

- Compliant request submitted by Client (Status Change request of Client);
- Client notifies Service Provider that the original certificate request was not authorized and does not authorize it subsequently;
- Non-compliance of any obligation of the Client;
- Notification by any third party regarding a lost and found client device;
- any other circumstance set out in the GTC;
- compromising of the private key that belongs to the public key of the certifcate;
- compromising of the service provider private key used for certifying the certificate;
- renewal, modification or key replacement of the certificate;
- unauthorized use of name or data,
- data incorrectly recorded in the certificate, incorrectness, change, misleading nature of the data;
- the Client failed to request the activation of the certificate within the time period of suspension;
- use of the certificate in bad faith;
- a related final, binding and executable resolution of any court or authority;
- the technical properties of the certificate expose any of the parties to a level of risk that exceeds an acceptable level on the basis of the significant professional recommendations (e.g. the key length is shorter than recommended);
- breach or termination of the service agreement;
- the certificate has not been issued in compliance with the applicable policies;
- the Service Provider becomes aware that the Client is not entitled to use any of the names (e.g. FQDN) indicated in the certificate;
- the Service Provider becomes aware of the termination of the right of representation indicated in the certificate;
- the provision of the expiry information services pertaining to the certificate is terminated;
- termination of the service, unless if the Service Provider had early arranged for the continuation of the provision of the CRL and OCSP services related to the certificates issued by the Service Provider;
- required by the law.

Possible grounds for suspension of the certificates:

- initial suspension following the issue of the certificate in order to increase the security of the shipment;
- a strong presumption of any circumstance that serves as ground for the revocation of the certificate.

The Service Provider shall make arrangements within at least seven days for the revocation of the service provider certificates in the following cases:

- the compliant, written request of the Certification Authority (in the case of outsourced issuer);
- the Certification Authority notifies the servie provider that the original issuer certificate request was not certified and does not certify or authorize it subsequently (in the case of outsourced issuer);
- compromising of the private key that belongs to the public key of the certifcate;
- compromising of the service provider private key used for certifying the certificate;
- use of the certificate in bad faith;
- data incorrectly recorded in the certificate, incorrectness, change, misleading nature of the data;

- the provision of the expiry information services pertaining to the certificate is terminated;
- the technical properties of the certificate expose any of the parties to a level of risk that exceeds an acceptable level on the basis of the significant professional recommendations (e.g. the key length is shorter than recommended);
- a related final, binding and executable resolution of any court or authority;
- termination of the service;
- required by the law.

4.9.2. Who can request status change

The Service Provider, courts, the Supervisory Body, other authorities, and, in the case of end-user certificates, Applicants and Subscribers can request the suspension, revocation, or activation of certificates. In case of regulated professions the Chamber of the profession can also request the suspension and revocation of the certificate if Client is no longer authorised to exercise a regulated profession.

In case of notification by a third-party of an abuse of the Service the Service Provider will investigate the circumstances and to decide on the suspension of the certificate.

4.9.3. Procedure for revocation, suspension and activation

a. Procedure for revocation and suspension

The revocation or suspension procedure is a process that starts with the receipt of the status change request for revocation or suspension by the Service Provider or with the Service Provider's decision or instruction and ends with the revocation or suspension of the certificate or, in case of an unsuitable application, with the rejection of the application.

The Service Provider evaluates requests for revocation and suspension without delay and before other requests.

Revocation, suspension, and activation can be requested by the authorised parties (see Chapter 4.9.2) by email or phone. The request for revocation, suspension, or activation has to contain at least the following data:

- the certificate serial number,
- the name of the (natural or legal) person requesting the revocation / suspension,
- the contact information of the person requesting the revocation / suspension,
- the time of the revocation / suspension (if not immediate).

If the key is compromised or lost, the Service Provider conducts a re-key procedure (see Chapter 4.7). The Service Provider can also handle client requests for revocation by issuing a suspension for the time of processing the request.

The certificate suspension can also be requested in the Client Menu. The use of the private key belonging to the suspended certificate shall also be suspended for the term of the suspension. The private key belonging to the revoked certificate has to be destroyed immediately after revocation, if this is possible (see Chapter 6.2.10).

The following rules of liability are applicable to the damages arising from the accepting the certificate as a result of certificate status changes:

- Until the request for revocation or suspension is received by the Service Provider, the Client is liable for any resulting damages.

- Following the receipt of the revocation or suspension request by the Service Provider, the Service Provider is liable for any resulting damages until the time the changed status of the certificate is published.
- If the Service Provider has already published the invalid status of the certificate (revoked or suspended), the Service Provider does not assume any liability for any Relying Parties still considering the certificate to be valid.

See chapters 9.6 and 9.8.

b. Procedure for certificate activation

Those persons can request that the suspended certificate be (re-)activated who are authorised to request the certificate's suspension or revocation. The application can take place in the manner set out in Chapter 4.9.3.1 with the condition that the activation of the certificate cannot be initiated in the Client Menu. If the certificate is not activated during the term of suspension set out under Chapter 4.9.13, the certificate will be automatically revoked after the expiration of the term of suspension.

4.9.4. Revocation request grace period

Before executing status change requests, the Service Provider checks them according to the following:

1. The identification of the Applicant: see the contents of Chapter 3.4
2. The right of the Applicant: see the contents of Chapter 4.9.2
3. The veracity of the application: see the contents of Chapter 4.9.3.1

The executability of the status change request:

- For revocation requests: if the certificate is valid or suspended.
- For suspension requests: if the certificate is valid.
- For activation requests: the certificate is suspended and the circumstances that led to the suspension are no longer applicable.

Once the Service Provider's Registration Authority has ascertained that the Applicant has authorisation and the application if complete and authentic, it will suspend/revoke the certificate without delay.

If the above requirements are not met, the Service Provider rejects the application; otherwise, it has to take measures without delay 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 certificate's Applicant and the Subscriber via email about all executed and rejected applications for suspension, revocation, and certificate activation.

The Service Provider publishes certificate status changes in the framework of its certificate status services (see Chapters 4.9.7-10 and 4.10).

4.9.5. Time within which TSP must process the status change request

The deadlines for processing revocation/suspension/activation requests are as follows depending on the channel used for the application:

CHANNEL	PROCESSING DEADLINE	MAXIMUM PROCESSING DURATION
CLIENT MENU (only suspension)	● Requests are processed continuously, 24/7.	Maximum of 24 hours
PHONE (See Chapter 1.1.2)	Requests are processed continuously, 24/7.	maximum of 24 hours

If the Service Provider is unable to ascertain the legality of the revocation, suspension, or activation request (or the authorisation of the requesting party) within the above time frame, it will consider the request to have been submitted by an unauthorised person until proven otherwise and will close the revocation, suspension, or activation process as having been unsuccessful.

Following the implementation of status change requests, the Service Provider validates the change:

- immediately in the Online Certificate Status Service (OCSP);
- a new revocation list will be issued no later than 1 hour following the change;
- in the public certificate repository no later than 1 hour following the change.

4.9.6. Certificate status checking requirement for relying parties

When accepting and using the information included in the Certificate, the Relying Parties have to proceed with suitable diligence, taking into account the requirements of Chapters 1.4 and 4.5 and the contents of the table in Chapter 7.1 that presents the relationships between certificate profiles, certificate policies, and uses. It is thus especially recommended to check:

- the validity of the end-user certificate;
- the validity period of the intermediate CA's certificate (TSP certificate) used to authenticate the end-user certificate;
- the validity period of the top-level Root CA's certificate (TSP certificate) used to authenticate the intermediate CA's certificate;
- the certificate status of the end-user and TSP certificates by querying the CRL or OCSP-based certificate status information referred to in the certificates.

The certificate can be considered to be valid if the time of the verification is within the certificate's validity period at which time the certificate was in a valid status, and these conditions are also true for all certificates in the certificate chain.

To determine the past validity of expired certificates, the respective revocation list or OCSP response valid at the given point in time is required (e.g. these can be integrated into an electronic signature or seal at the time of authentication).

The validity of website authentication certificates (DVCP) has to be established for the moment the website was authenticated.

The Relying Parties can receive information on the current status of various certificates with the use of certificate status services (see Chapter 4.10). Only the currently valid certificates can be queried in the public certificate repository available on the Service Provider's website - and only if the Applicant of the queried certificate has granted its consent for disclosing the various data in the certificate. Suspended and revoked or expired certificates are not accessible via the public certificate repository.

4.9.7. CRL issuance frequency

Certificate Revocation Lists (CRLs) primarily include those revoked and suspended certificates that were still valid at the time the list was issued; however, the Service Provider may also issue CRLs that include all of the revoked and currently suspended certificates that the Service Provider issued, regardless of the time of their issuance. Suspended certificates will be removed from the list after being reactivated. The Service Provider certifies CRLs with its own electronic signature.

Generally 4, but no more than 24, hours elapse between the issuance of CRLs pertaining to two consecutively issued end-user certificates; CRLs may not be valid for more than 25 hours. New CRLs pertaining to TSP certificates are generally issued every 24 hours, but no less frequently than every 12 months (in case of cross-certified certificates by maximum 31 days); CRLs may not be valid for more than 12 months. A CRL is issued with the above frequency even if no certificate revocations, suspensions, or activations have taken place since the last issuance. CRLs always include the latest time by which the subsequent list has to be issued.

4.9.8. Maximum latency for CRLs

The Service Provider will publish the certificate revocation list (CRL) no later than one hour following the approval of the status change request.

4.9.9. On-line status checking availability

The Service Provider also provides an Online Certificate Status Service (OCSP) for verifying certificate status, as set out in Chapter 4.10.

4.9.10. On-line status checking requirements

The Service Provider supports Online Certificate Status Protocol (OCSP) requests received with the 'GET' and 'POST' parameters defined by RFC 2560 or RFC5019 for querying certificate status information. See: Chapter 4.10.

All Relying Parties are authorised to perform OCSP requests. The Service Provider always serves requests with the proper parameters, by taking into account the provisions laid down in Chapter 6.5. Requests are processed and OCSP replies are sent automatically. The Service Provider authenticates OCSP replies with its own TSP certificate dedicated to this purpose (OCSP responder certificate). The Relying Party that checks the validity of the certificate with the use of the OCSP service also has to check the signature of the OCSP reply.

When the certificate in question is valid, the OCSP reply issued by the Service Provider contains "good" status information if

- the OCSP request pertains to a certificate issued by the Service Provider;

- the OCSP request pertains to the availability of the OCSP indicated in the certificate.

4.9.11. Other forms of revocation advertisements available

The Relying parties can also use the public certificate repository to collect certificate status information: if they do not find a specific certificate issued by the Service Provider here, it is to be considered as not valid.

If the Service Provider terminates the use of its root certificate, it is to publish this fact on its website.

4.9.12. Special requirements re-key compromise

The Service Provider will always notify the Client(s) by sending an email to the address in the end-user certificate if it gains knowledge of a threat of the end-user key(s) becoming compromised or the possibility of any of the circumstances set out in Chapter 4.9.1.

In the case of the assumed or proven key compromise, it will perform the steps of the revocation procedure (Chapter 4.9.1.1). A compromised private key can never be used again; if possible, steps are to be taken to have it destroyed and it is to be provided the same supervision and protection until its destruction as given a valid private key (see Chapter 6.2.10).

The Client is obligated to take all steps to prevent or mitigate damages, including notifying any Relying Parties affected by the private key having been compromised.

If the TSP private key is compromised or threat arises of such, the steps of the revoking the certificate shall be performed (Chapter 4.9.1.2).

4.9.13. Limits on suspension period

A certificate can be suspended until the suspicion of the circumstances that led to its revocation is confirmed or rebuked, but for no more than 30 calendar days. The Service Provider has to provide for the revocation or activation of the certificate as soon as possible. The start of the suspended status is to be calculated from the time the suspension request is approved, i.e. the request defined under Chapter 4.9.3.1, which time is indicated in the CRL. If the suspicion of the circumstances leading to its revocation is not confuted during this period, the Service Provider will automatically revoke the certificate.

Suspension is not applicable in the case of certificates for website authentication certificates (DVCP).

4.10. Certificate status services

The Service Provider provides Relying Parties with the services required for checking the status (valid, suspended, revoked) of certificates issued on the basis of the present Statement.

4.10.1. Operational characteristics

The CRL and Online Certificate Status Service pertaining to the various certificates are available at the URLs indicated in the certificate's crlDistributionPoints and authorityInfoAccess:OCSP certificate extension fields (see Chapter 7.1.2). These records can be used to verify certificates within their periods of validity. Following the time indicated in the certificate's "notAfter" field

- the certificate will not be included in the CRL even if the certificate has been previously revoked/suspended.
- the Service Provider provides the last certificate status within the certificate's validity period as a response to OCSP requests.

After the validity period of certificates the status information can be checked in former CRLs, available (by individual request) at the Service Provider.

During the management of certificate status services, the Service Provider shall proceed according to the following:

- it ensures the continuous, 24/7 online availability of certificate status information (at the URLs indicated in the certificate's applicable fields and on the Service Provider's website);
- the time data indicated in the CRL and OCSP responses will be synchronized at least once a day with the Coordinated Universal Time (UTC);
- it uses a PKI-based signature to ensure the integrity and authenticity of certificate status information;
- it ensures that information on revocation is included amongst the respective certificate status information for at least the certificate's original validity period;
- the revocation information pertaining to expired certificates is accessible amongst the archived CRLs issued during the validity of the certificate;
- it offers a CRL and OCSP for the purposes of verifying certificate status;
- it ensures that the CRL and OCSP services harmonize with each other: the information on a certificate status change has to be available in both of these services and has to be the same;
- it ensures that certificate revocation information is publicly and internationally accessible;
- it ensures that the revoked and suspended certificate statuses are differentiated amongst the certificate status indications;
- it ensures that suspended certificates are removed from the Certificate Revocation List (CRL) after activation;
- in the case of certificate suspension or revocation due to a key being compromised, the Service Provider issues an extraordinary CRL after registering the status change; in case of revocation or suspension for any other reason, the status change will be published no later than in the next planned revocation list.
- In the case of web site authetnitcation certificates (DVCP) the Service Provider will keep the size of the CRL under 7 MB (if possible) in the interest of providing for a fast download.

4.10.2. Service availability

The Service Provider continuously (24/7) provides as part of its certificate services, the availability of requests for revoking and suspending end-user certificates and of CRLs; as set forth below.

In regard to the availability of

- certificate status services;
- the other Terms and Conditions applicable to the use of certificates issued by the Service Provider; and
- services related to status change

and also taking into account the contents of Chapter 4.9, the Service Provider ensures the following:

- 99% availability on an annual level;

- the duration of any single service disruption will not exceed 3 hours.

For thw Web site authentication certificates (DVCP) the response time of CRL and OCSP services will be no more than 10 seconds under normal loads.

Service Provider provides the activation of the end user certificates on business days during the hours of service published on its website (see Chapter 1.1.2).

4.10.3. Optional features

The Service Provider will not apply any more requirements for the certificate status service.

4.11. End of subscription

- Service Provider provides information on the termination of the service agreement in the GTC.

See the relevant Chapter of the GTC.

4.12. Key escrow and recovery

TSP privides key escrow and recovery services for encryption certificates.

In other cases Service Provider shall not store or save the private keys of the end user certificates in any way whatsoever, and therefore Service Provider cannot restore such keys in case these keys are stolen or damaged while in possession of the end user.

4.12.1. Key escrow and recovery policy and practices

The same level of security requirements apply to copies of end-user private keys made by the Client as to the original private key (see Chapter 6.2). The number of copies of a private key should not exceed the amount necessary for maintaining the service.

The Service Provider also saves and stores its own TSP private keys.

4.12.2. Session key encapsulation and recovery policy and practices

The Service Provider does not store or recover symmetric keys.

5. Facility, management, and operational controls

In the interest of decreasing risks, the Service Provider stores the hardware, software, and other devices required for the services it provides in two different locations physically separate from each other: in a primary location and a secondary location. The requirements applicable to the two locations are the same; any deviations are indicated at the applicable points.

The configuration of the Service Provider’s systems is regularly checked in order to filter out any changes that are in violation of the security requirements.

The devices of the Certificate and Registration Authorities are handled exclusively by authorised and suitably trained personnel whose knowledge is checked.

Backups are made of the Authorities’ files (see Chapter 6.5). The Service Provider retains the backups for the time set out in Chapter 5.5.2.

The Service Provider examines the physical, procedural, and personal requirements by regularly assessing risks. The Service Provider keeps an inventory of assets which include the devices (and information assets) that it uses.

The Service Provider's private Security Regulations include the requirements pertaining to information security rules.

The Service Provider reviews the Security Regulations and asset inventory regularly or immediately following any significant changes to ensure they remain continuously applicable, suitable, and effective.

5.1. Physical controls

The aim of physical controls is to prevent unauthorised access, damages, and unlawful entry to the Service Provider's confidential information and physical premises (server rooms). The Service Provider uses a suitable system of authorisations to limit physical access; these authorisations are regularly reviewed.

The Service Provider ensures that the loss of and damages to values are avoided, that values are not compromised, and that operating activities are not disturbed by applying the measures set out in the Service Provider's Security Regulations.

Services that process critical or sensitive information are performed and modules that use cryptographic modules are used and stored in secure locations. The provided protection is proportionate to the risks determined by the Service Provider in the risk assessment.

5.1.1. Site location and construction

The Service Provider performs the services subject to the greatest risks in a secure, protected computer room located on its site. Physical access, the supervision and checking of entry, the power supply, air conditioning, protection against leaks and flooding, fire prevention and fire protection, the storage of data media, the accessibility of the telecommunications network, electromagnetic radiation, etc. are all controlled on the basis of the same factors of protection. Access by unauthorised persons to the computer room is made difficult, but the security personnel can quickly gain access in case of a breach. The security zone does not have any windows; with the exception of the door, the only way access can be gained is by demolishing the reinforced walls. The room is equipped with redundant climate control, automatic fire fighting, and intrusion alarm systems. All equipment is hooked up to a multiply redundant electricity supply.

The Service Provider's secondary location is a server safe in a protected secure computer room, the security level of which is the same as that of the on-site location.

The Service Provider's Central Registration Administrators perform key generation, the preparatory actions pertaining to key storage devices, certificate issuance, and the management of status changes in a separate server room specially designed for this purpose. The protected server room was designed expressly for this purpose.

5.1.2. Physical access

The relevant internal operational documents contain the exact parameters of the security zones and the list of persons who are authorised to enter. Persons other than the employees who fill trusted roles can only enter the security zone with separate authorisation and if accompanied. Access to the computer room takes place with a personalized electronic card; all access is logged both physically and electronically. Within the computer room, the TSP systems are installed in a

separate area where access is only granted after biometric identification. Round-the-clock video surveillance is provided for the room that provides access to the security zone as well as for the computer room itself.

The access system to the secondary location does not use biometric identification; however, security guards provide round the clock protection to protect homogeneity and the security of the secondary location. Access to the server room is granted to authorised employees with their key cards; entry and exit is continuously logged. Round-the-clock video surveillance is provided for the server room.

In the framework of critical services, the Service Provider's risk assessment deals with the regulation of physical access, protection against natural catastrophes, the factors of protection against lightning and fire safety, the faults of support equipment (especially 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 stores TSP certificates separately from its normal operations and access to those is granted only to trusted employees.

5.1.3. Power and air conditioning

The uninterrupted power supply of the Service Provider's protected computers is especially important in order to ensure continuous operation, in the interest of which the Service Provider uses (has used) the following:

- uninterruptible power supply,
- selective short circuit protection,
- protection against electrical anomalies, lightning, and overvoltage.

The system providing the uninterruptible power supply is structured as follows:

- diesel generator,
- local battery-based uninterruptible power supply,
- redundant circuit selector.

The following operational procedure is followed:

- if the network power supply is interrupted or decreased, the system switches to the backup power supply,
- the system meanwhile starts the generator,
- when the network power supply is again usable (for 5 minutes continuously), the system returns to its use.

A selective short circuit protection was used in the computer room to develop several systems that operate independently of each other and thereby support continuous operations. The distribution network was designed to ensure that if any group of equipment is short circuited, power will be cut off from that group while the other equipment groups that are operating flawlessly can remain operational.

In the server room, the computer rooms have an air conditioning system independent of the rest of the building. A suitable filtration system is used to ensure the cleanliness of the air inducted into the protected computer room, which filters out various pollutants and also provides the staff with the air they require. The humidity and temperature of the air is continuously monitored. The air conditioning systems provide for the cooling that the IT systems require. Continuous operation

is also supported by a second (backup) climate control system which will turn on if necessary. The location of the climate control systems ensures that their maintenance does not cause any disturbances to the computer room's operations.

5.1.4. Water exposures

The Service Provider's service locations are protected from leaks and floods. The use of a raised floor increases security in the protected computer room.

5.1.5. Fire prevention and protection

The Service Provider's service locations are operated in line with fire safety requirements. The locations are equipped with fire and smoke detectors as well as manual and automatic fire extinguishers. The location of manual fire extinguishers and escape routes are indicated in high visibility locations.

5.1.6. Media storage

A security zone and a rented bank safe is used to ensure the safe storage of the Service Provider's data media. The Service Provider has several backups of critical data. The Service Provider continuously ensures and takes the necessary steps to prevent the deprecation of its data media.

The Service Provider disposes of data media that contain sensitive data in the manner set forth in the Security Regulations, if such are no longer necessary. The Service Provider permanently deletes the contents of disposed tools or irreparably destroys them.

5.1.7. Waste disposal

The Service Provider shall proceed according to the following regarding physical destruction:

- paper-based documents are shredded,
- floppy disks are shredded (after removal from their housing),
- other magnetic data media are demagnetized and then crushed,
- other data media are crushed.

5.1.8. Off-site backup

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

The Service Provider provides 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 ensures that its systems operate securely, in accordance with applicable rules, and with a minimal risk of error. In the interest of the above, it employs a suitable number of staff with appropriate skills, technical knowledge, and experience.

In the case of non-qualified services, the Service Provider operates 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 independent system controllers also ensure that the system operates suitably.

The Service Provider has a quality assurance and information security management system in place that is continuously monitored by an external, independent system controller.

The Service Provider classifies the managed data created during the provision of non-qualified services into a security class on the basis of the risk assessment defined by relevant legislation and in the Practice Statement; it furthermore ensures 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 (see Chapter 5.2.1 of the Trust Service Policy) at the Service Provider for whom it certifies 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 is filled by a person who has a vocational higher education degree[5] and at least three years of experience in IT security.

The Service Provider employs the person fulfilling a trusted role in the framework of employment; moreover, the person in the trusted role is free of all interests that can negatively affect the reliability or security of the service. The Service Provider ensures that the person dealing with the provision of services has the required and suitably up-to-date skills and experience. The Service Provider ensures that all trusted roles are fulfilled.

The Service Provider keeps a current registry on trusted roles; in case of any changes, it reports the change without delay to the Supervisory Body.

5.2.2. Number of persons required per task

The following activities are performed by the Service Provider in the physical presence of at least two designated trusted employees with direct authorisation, in a physically protected environment:

- generating of TSP key pairs;
- issuing intermediate CA certificates;
- saving and restoring TSP private keys;
- destroying TSP private keys.

5.2.3. Identification and authentication for each role

All of the Service Provider’s employees in trusted roles can only access the secure zone after proper identification and authentication, which in addition to which further identification is also required for access to IT systems. Access to the secure zone and the system is not possible without successful identification and authentication, thus no activities critical to security can be performed without these steps.

[5] 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 Service Provider personally identifies 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 provides 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.

Access to the various applications is restricted. The system can differentiate between the various trusted roles, thus especially access by System Administrators and System Controllers.

Staff is identified and authenticated before they are allowed to use applications critical to services, and they can be held accountable for such activities.

The Service Provider records the permission levels for the various trusted roles in the Human Resources Policy.

5.2.4. Roles requiring separation of duties

In these systems, the Service Provider applies security measures and defines permission levels that minimize unauthorised or unintentional modifications and decrease the possibility of violations.

In the interest of separating roles

- the security officer does not perform the tasks of the independent system controller and the manager generally responsible for the IT system;
- the independent system controller does not perform the tasks of the manager generally responsible for the IT system;
- the security officer does not perform the tasks of the system administrator; and
- the independent system controller does not perform the tasks of the validation specialist and the system administrator.

The Service Provider uses a strict control policy 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. Inspection procedures can be audited.

The Service Provider's Security Regulations contain the detailed rules on conflicts of interest.

5.3. Personnel controls

The purpose of security measures pertaining to personnel is to decrease the risk of human error, theft, fraud, and abuse.

In the interest of the above, the Service Provider deals with personnel security even during the hiring process, and then ensures personnel security with checks performed during the term of employment.

The Service Provider has a detailed and exact Personnel Policy that it continuously maintains as part of its Security Regulations. The Service Provider documents the temporary and permanent roles and responsibilities defined in the Personnel Policy in job descriptions, which include:

- the information management performed by each role and the classification of risks based on their effects on the various authentication processes,

- technical and experience requirements,
- a description of the activities regarding the position and the tasks of the given employee, the scope and extent of responsibilities, and the name of the related positions.

The Service Provider's employees may not fill trusted roles until the time the checks regarding the persons and the required statements have been implemented and until they have participated in the required trainings and gained the necessary experience.

The Service Provider's executives, managers, and employees in trusted roles are independent of all business, financial, and other influences that could influence the trust shown towards the services offered by the Service Provider.

5.3.1. Qualifications, experience, and clearance requirements

The Service Provider employs 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.

All persons designated to fill a trusted role at the Registration Authority undergo an initial check (to verify their reliability and technical suitability). During this basic security check, the inspectors check the data provided in the curriculum vitae (details, references, professional advancement, etc.). During the course of the above:

- the data pertaining to education are compared to the certificates and degrees to be submitted by the candidate,
- the statements made regarding practical experience are verified with personal references, based on publications, and by other means.

Service Provider shall ensure that the Registration Administrators shall have sufficient knowledge for performing their activities in compliance with the practice statement, to this end Service Provider shall provide the Registration Administrators with trainings in the following subject matters:

- basic PKI knowledge;
- principles and procedues of authentication and certification set out in the Certificate Policy and the Practice Statement;
- phishing and other techniques threatening the reliability of the authentication and certification procedure.

Service Provider shall maintain a registry of the trainings.

The Registration Administrators shall not carry out their activities without the knowledge set out above, and therefore Service Provider requires the Registration Administrators to successfully pass the related examination.

The Registration Administratorsare familiar with current official documents and other equivalent documents as well as with their types and characteristics, and they are also capable of verifying the validity of the submitted documents.

All employees who fulfil trusted roles have to undergo periodical security checks in addition to the basic security check.

Persons qualified as a "high security risk" at the basic or any periodical security checks cannot fill a trusted role. Trusted roles may only be filled by 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.

Employees who are employed in trusted roles are succumbed to periodical security checks every year (see Chapter 5.2.1).

Following their appointment, Validation Specialists participate in basic training that provides them with the theoretical and practical knowledge required for their position; they are to take an exam at the end of the training. The main purpose of this form of training is to become familiar with and understand the uniform security policy applicable to the service in the interest of correctly applying the current procedures based on those. The Personnel Policy contains more information.

Employees can fill trusted roles after gaining suitable experience.

5.3.2. Inspection Procedures

During the hiring procedure, the Service Provider checks the identity of the persons during their physical appearance or by checking their photographic personal identification documents. In addition to the above, the Service Provider also takes into consideration the information pertaining to previous employers, relevant education, and professional references.

Employees in trusted roles cannot receive access to the Service Provider's systems before these checks have been performed.

5.3.3. Training requirements

Employees in trusted roles have to have the knowhow required for performing their tasks. In the interest of ensuring this knowhow, employees in trusted roles have to take an exam to certify their knowledge. They cannot access the TSP systems until passing this exam. The exam and the training extend to the following, depending on the type of trusted role:

- 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 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 defines its training and retraining practices in the annual retraining plan.

If any significant changes take place in the trust services, all employees undergo a modular retraining with the necessary structure and level in addition to being provided the required documentation.

5.3.5. Job rotation frequency and sequence

The Service Provider's Personnel Policy defines the applicable rules.

5.3.6. Sanctions for unauthorized actions

The Service Provider regulates the sanctions applied for the unauthorised use of the Service Provider's system and for any errors, omissions, or damages caused during the provision of the service in the employment contracts of the persons filling trusted roles.

5.3.7. Independent contractor requirements

The same security rules apply to any contractors used by the Service Provider in other than employment relationships as to its employees.

5.3.8. Documentation supplied to personnel

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

5.4. Audit logging procedures

In the interest of retaining the actions involving certificates and the preparation of Client devices and the data used during these processes, the Service Provider's authentication system performs a wide array of logging activities that meet the requirements of legislation and applicable standards and requirements. The log file includes the exact time of the record, the calendar date of the logged event, the type of event, the data required for traceability and reconstructing the event, the name of the user or other person that caused the event, and whether the action was successful or not. The Service Provider synchronizes the time indicated in its logs with a frequency that ensures that the difference between its own time and the current time does not exceed 1 second. Any deviations that exceed this amount will also be logged.

The Service Provider's other system also perform logging. The characteristics of these logs depend on the given application. The log elements are created separately in the various modules. Since the system consists of several components, the log files are not created in one location; however, they are processed in one central location.

The Service Provider protects all records in the log file from changes and unauthorised access. The log is 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. The Service Provider regularly backs up the log file and ensures that log data are continuously evaluated and controlled.

The Service Provider documents the method of accessing logged information and the time for which it must be stored.

At an operative level, the operational descriptions of the various systems regulate the handling of log data.

5.4.1. Types of events recorded

The system used by the Service Provider logs all the events and errors required by relevant legislation that are critical from the aspect of services. Log files are recorded automatically or manually. In addition to the log files, the Service Provider also uses records to record various events.

The Service Provider sets forth in detail in the Security Regulations the exact data/events that it records in relation to each event.

Logged events are recorded in the log file as dated entries. The Service Provider protects all log entries from modification, unauthorised access, destruction, deletion, or any changes to the order of entries by using electronic signatures, saving, and backups.

Searches for event type and/or user can be performed in the log files. The log entries are in text format.

5.4.2. Frequency of processing log

The Service Provider's log entries are reviewed on a daily basis by Independent System Controllers who have the required expertise and authorisation. Evaluation takes place both manually and with the use of software tools.

During the course of the evaluation, the evaluator analyses the error messages generated by the systems, the significant changes to the traffic data, the trends that differ from the usual, and suspicious activities. The evaluator or the software tool records the fact and results of the evaluation as well as any necessary measures.

The Service Provider's network protection systems are also equipped with an automatic alarm function, which goes off if any unauthorised access is detected. In the case of such alarms, the log entries are immediately reviewed. The Service Provider may also review the log data if any irregularities are found, if complaints are received, or if otherwise contacted.

5.4.3. Retention period for audit log

Log files are stored at the place of their creation and are also archived (see Chapter 5.5.2); the related certificates are stored for a period of 10 years after their expiration (one year in the case of other services) or until the final closing of any legal disputes that are incurred and reported in relation to those. Log files are accessible to Independent System Controllers.

5.4.4. Protection of audit log

The log entries of the Service Provider's authentication system are stored with the Service Provider's electronic signature and in a manner that excludes the possibility of undetected deletion or insertion.

Backups protect log files from accidental and intentional damages. In the case of log entries containing personal information, the Service Provider ensures that the data storage is confidential. Only those persons are authorised to access the log files who require access for their roles (generally the Independent System Controllers). The Service Provider checks access in a secure manner.

5.4.5. Audit log backup procedures

Log files are regularly saved in the manner defined in Chapters 5.1.6 and 5.1.8. If the log entry is created in only one location, the Service Provider ensures that a backup will be created within 24 (twenty four) hours.

5.4.6. Audit collection system

The applications automatically collect and store log entries in the log files. The Service Provider collects the saved media on a daily basis. The Service Provider's own employees transport the media to the place of storage.

5.4.7. Notification to event-causing subject

The persons, units, and applications that cause a log entry are not notified by the Service Provider; however, it may include them in inspecting the event. If the parties that caused the event are in a contractual relationship with the Service Provider or if otherwise required by relevant legislation, they are obligated to cooperate with the Service Provider.

5.4.8. Vulnerability assessments

During the course of processing log entries, the Service Provider performs assessments regarding vulnerability. In addition to the processing performed on a daily basis, the Service Provider's experts also review extraordinary events every month, on the basis of which they assess vulnerabilities. Based on these assessments, the Service Provider takes steps to improve the security of the system.

Every year, the Service Provider performs a risk assessment, with the help of which it identifies, evaluates, and classifies into risk classes the foreseeable external and internal threats that could lead to the unauthorised access, disclosure, modification, destruction, or other abuse of the certificate management processes. The risk assessment also extends to expected damages if such threat were to become real. In addition to the above, the risk assessment also includes a description of the processes and security measures that the Service Provider takes to prevent these threats.

5.5. Records archival

The Service Provider retains the data pertaining to the service in the manner and for the time defined in this Chapter. Together with the retention, the Service Provider also provides a tool with which the contents of the issued certificate can be determined.

The Service Provider protects all entries in archived data files from unauthorised modification, deletion, destruction, and access. Archived data files stored electronically are affixed with at least advanced electronic signatures or seals and with timestamps. The Service Providers ensures 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 retain the data related to the certificates it issues - thus especially related to their creation and issuance and including personal information. In accordance with the above, the following are archived:

- the data provided by the Applicant and the Subscriber during certificate enrolment (see Chapter 4.1.2.1);
- the electronic or hard-copy documents, or copies thereof, that came into the possession of the Service Provider during the course of the identification and authentication processes (see Chapter 4.2.1);
- the ID of the Registration Administrator who accepted the application (see Chapter 4.2.2);
- the name of the Registration Authority that performed identification and authentication;
- the information disclosed during the certificate status change procedure (see Chapter 4.9.3);
- the information logged in accordance with the present Statement (see Chapter 5.4).

The Service Provider archives electronic data in an electronic format. The Service Provider archives documents available in hard copy format either in the form of an electronic copy or in their original hard copy format.

5.5.2. Retention period for archive

The Service Provider archives the electronic and hard copy information and personal data pertaining to certificates for at least ten years following the expiration of the certificate as defined by the certificate, or until the legal dispute regarding the certificate, regarding the public key in the certificate is closed in a final ruling. For the same periods as set forth above, the Service Provider also ensures that tools are available that can be used to determine the contents of the issued certificates.

5.5.3. Protection of archive

To protect electronic documents and data, the Service Provider applies the requirements set out in Chapter 5.4.4 regarding both documents received in electronic format and the electronic copies that the Service Provider itself makes.

The Service Provider stores the documents available in hard copy format within the security zone defined in Chapter 5.1, thus ensuring that only Registration Administrators, Certification Administrators, and Validation Specialists can access those.

5.5.4. Archive backup procedures

The provisions pertaining to saving log files set out in Chapter 5.4.5 are applicable to archive backups.

5.5.5. Requirements for timestamping of records

The Service Provider affixes the data to be archived with timestamps or time data in the manner defined in Chapter 5.4.1.

5.5.6. Archive collection system

No rule.

5.5.7. Procedures to obtain and verify archive information

Access to the archive can be requested by submitting a request to the Service Provider’s customer service. Access is provided for Clients to the data that pertain to them; other persons are provided access as laid out in Chapter 2.4.1. The Service Provider always checks authorisation and logs access.

5.5.8. Miscellaneous archiving provisions

The Security Regulations contain the detailed provisions applicable to archiving.

5.6. Key changeover

The Service Provider replaces its own key that it uses if the TSP certificate expires or the keys that it uses become deprecated. In addition to the above, the Service Provider can also decide to replace keys at its own discretion.

In the case of a new certificate generated with a new key, the Service Provider aligns its profile and data with current regulations and best practices.

5.7. Compromise and disaster recovery

In order to identify the threats that affect the services and to manage any possible risks, the Service Provider uses a risk management assessment and also has a Business Continuity Disaster Recovery Plan (ÜFKT), which applies to the management of extraordinary situations, the prevention as soon as possible of emergencies, and to the provision of continuous operations.

5.7.1. Incident and compromise handling procedures

In accordance with the contents of applicable regulations, the Service Provider continuously monitors the system activities pertaining to logging on to IT systems, to IT system users, and to requests for the provision of services. The Security Regulations contain the exact factors for these checks.

If the Service Provider detects a critical vulnerability in its IT systems, it will perform one of the following measures within 48 hours of detecting such vulnerability.

1. Repairs the critical security hole.
2. If a critical security hole cannot be repaired within 48 hours, the Service Provider will prepare and implement an action plan to mitigate the vulnerability, the primary task of which is the following:
    a. repairs the most critical security holes in accordance with the CVSS[6] (starting with the highest score);
    b. repairs the security holes of the systems that do not have supplemental protection mechanisms and which are subjected to the threat of unauthorised access and to becoming compromised if the vulnerability is not decreased.
3. The Service Provider documents the facts because of which the vulnerability does not have to be repaired, which can include the following:
    a. The Service Provider disagrees with the vulnerability scoring defined by the CVSS;
    b. the vulnerability was misidentified;
    c. the vulnerability cannot be exploited due to the subscriber protection mechanism; *or*

The ÜFKT applied by the Service Provider also includes the disaster recovery plan. The ÜFKT contains procedures that describe the fastest method for restoring reliable services as soon as possible. The Service Provider regularly performs checks (at least annually) to test whether the security regulations are executed correctly regarding the technical and personnel aspects.

The Service Provider uses backups to ensure that it can restore the entirety of its IT system if necessary. The Service Provider protects the backups from modification and access by unauthorised persons.

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

The Service Provider has equipment and systems with advanced security to minimize the chance of hardware and software errors or data corruption. The ability to restore the Service Provider's

[6] Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss/specification-document)

services is guaranteed by its background agreements and its own reserve equipment, which are capable of substituting any of the critical equipment within the time undertaken in Chapter 5.7.4. The Service Provider's regular backups (see Chapter 5.5) and transaction logging (see Chapter 5.4) ensure that data can be restored if any data storage equipment becomes faulty. In the worst case scenario, this system is capable of restoring the data of the previous day.

The ÜFKT contains event reporting requirements for the cases in which any of its equipment become faulty and for irregular operations (some are automated and some are the responsibility of the managing personnel). The reports are evaluated by a professional staff, who minimize any damages and service downtime by executing response procedures.

The ÜFKT contains the detailed rules pertaining to faults experienced by critical system components.

The system elements that provide certificate status information shall have priority in the course of the restore.

5.7.3. Entity private key compromise procedures

a. End-user key compromise

See the contents of Chapter 4.9.12 for the end-user key becoming compromised.

b. TSP key compromise

If the TSP key is compromised, the Service Provider informs its Clients, contractual partners and the Relying Parties. It indicates that the certificates issued with the affected Service Provider keys and the certificate status information are no longer valid. The Service Provider will revoke the certificate that contains the private key that has become compromised.

The ÜFKT contains the additional requirements applicable if the TSP private key is compromised and the procedure to be followed. In case of a disaster, the Service Provider will take the necessary steps in order to avoid the reoccurrence of the disaster.

c. Change in algorithm

If any of the algorithms used by the Service Provider or any related parameters do not meet the requirements applicable during any period of the planned term of use (regarding both end-user and TSP certificates), the Service Provider informs its Clients, contractual partners and the Relying Parties, and also takes the steps necessary to revoke the affected certificates.

5.7.4. Business continuity capabilities after a disaster

The Service Provider has a business continuity plan in place that it puts into effect in case of a catastrophe. In case of a catastrophe (including if any of the TSP private keys or other authenticating data are compromised or if any critical elements of the TSP systems become faulty), the Service Provider's normal operations will be reinstated, and it will also be ensured that the errors do not happen again.

The aim of the Service Provider is to restart all services as soon as possible after averting the error and restoring integrity. The recovery of the reliable operation of certificate status services receives priority over the recovery of all other services and activities.

After a natural or other disaster or if the Service Provider's equipment becomes faulty, the Service Provider undertakes to start the provision of the following services within 24 hours:

- status change services,
- OCSP services.

The Service Provider undertakes to start all other services within 5 workdays.

5.8. CA or RA termination

If the Service Provider terminates its activities in a planned manner or for an extended period of time, it will perform the following before cessation of its activities:

- Service Provider shall use all reasonable efforts in order that a suitable service provider takes over its registries and its obligations of service provision until the termination of the provision of the service at the latest.

- Service Provider shall, at least 60 days prior to the termination of the provision of the service, publish a notification on its website and send e-mail notification for its clients having an e-mail address of the above termination.

- Service Provider shall destroy its own private keys and shall revoke the certificates related thereto, and shall publish the related information on its website.

- Then Service Provider shall continue to provide the revocation information, if possible.

After the revocation of the certificates, Service Provider shall continue to meet its obligation of publication until the termination of its activities.

- The Service Provider revokes the as-yet unrevoked certificates it issued at least 20 days before the termination of its activity.
- The Service Provider will revoke all management rights and authorisations derived from agreements concluded with any companies in a contractual relationship with the Service Provider and participating in certificate issuance or with the Registration Authority; the Service Provider will also call upon all Registration Authorities to hand over the data they store.
- In the interest of retaining the registration information and event log archives, the Service Provider will create a full backup including a timestamp. The backup includes the data of previous changes related to certificates, to their status or possible suspension, and to revocation, the Practice Statement pertaining to the issuance of the certificates, public key, and the registry of revoked certificates. The Service Provider protects the saved data files from unauthorised modification and ensures that unauthorised access is excluded; it furthermore provides for the accessibility and interpretability of the data by authorised persons for the retention period.
- The Service Provider will not issue new certificates after announcing its termination.

6. Technical security controls

The Service Provider uses an IT system that consists of reliable and checked products that have been evaluated as regards security technology.

The key management provisions differentiate between the following keys:

TSP private keys:

- private key used to sign end-user certificates and CRL and OCSP responses,
- private key used to sign other certificates and CRL and OCSP responses,
- infrastructure and control keys,

- authorisation response signature key.

TSP public keys:

- the public key pairs to TSP private keys.

End-user private keys:

- the private key of an end-user that it created itself,
- the private key of an end-user created on its behalf by the Service Provider.

End-user public keys:

- the public key pair to end-user private keys.

6.1. Key pair generation and installation

In the case of according to secondary certificate policy displayed in the certificate refers to SCD keystorage (see at Service Policy chapter 1.2.1 Cerificate Policy) key is generated in a chriptographic device listed in chapter 6.2.1.

6.1.1. Key pair generation

Regardless of who generated the key pair, the Service Provider checks whether the public key had been previously issued to another Client.

a. TSP key generation

The Service Provider generates TSP key pairs in a physically protected server room in the presence of at least two trusted employees and with the exclusion of the presence of any other persons; a report is drawn up of the process. The list of persons who fill trusted roles and are authorised to generate keys is included in the Service Provider's Security Policy.

The Service Provider uses the cryptographic hardware modules detailed in Chapter 6.2.1 of this Statement for the generation and storage of TSP keys. The Service Provider generates all of the TSP key pairs. With the exception of the saving described in Chapter 6.2.4, the generated private keys remain on the cryptographic hardware modules for their entire lifecycles and are not transferred anywhere before being destroyed. If it becomes necessary to destroy the TSP private key for any reason, such destruction takes place under the control of two persons as required by the device's certificate.

Prior to the expiration of TSP keys, the Service Provider will generate the new CA keys and issue the new TSP certificates in a manner that ensures that the transition is as smooth as possible for the Client and the replacement of the certificate does not cause any disturbances for the Clients and the Relying Parties.

A qualified auditor also observes the generation by the Service Provider of Root CA keys in order to check compliance with the above requirements and the integrity and confidentiality of the key pair. The auditor issues 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.

The key generation scenario contains the details rules pertaining to the generation of TSP keys.

b. End-user key generation by TSP

The Service Provider uses algorithms for the generation of end-user keys for authentication and encryption purpose that meet the requirements of the standards applicable at the time of issuance and the Supervisory Body's decision. The Service Provider rejects all requests for certificate issuance that do not meet these requirements.

End-user keys are generated only by persons who fill trusted roles and either in an automated manner or in the Service Provider's protected server room. If the key pair is used on a Client device, the Service Provider will create it directly on the device and will not store or save it by any other means, with the exception of the cases outlined in Chapter 4.12 Key escrow and recovery.

The Service Provider ensures that its end-user private key and the activating data are inaccessible to others.

See Chapter 6.1.2 Private key delivery to subscriber.

The Service Provider does not generates private keys for web authentication certificates (DVCP).

c. End-user key generation by itself

For the end-user may also generate the end-user key pair. When using a Client device or, it must notify the Service Provider.

See also Chapter 6.1.3 Public key delivery to certificate issuer.

6.1.2. Private key delivery to subscriber

If the Service Provider generated the end-user key pair, it will deliver it together with the carrier Client device to the End-User in a secure manner, by way of the Receiver.

Menedzselt SCD esetén a szolgáltató nem juttat el kulcsot a felhasználóhoz, a felhasználó értesítést kap arról, hogy kulcsát a korábban megadott aktiváló adattal igénybe veheti.

6.1.3. Public key delivery to certificate issuer

If the key is generated by the End-User, the successfully registered Applicant delivers the public key to the Registration Authority, which first checks whether the Applicant truly has the private key that is paired to the public key sent by the Applicant and then forwards it to the CA, again using a secure channel.

If the Service Provider generates the key pair for the end-user certificate, there is no need to deliver the public key.

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.

6.1.4. TSP public key delivery to relying parties

The Service Provider's TSP certificates are available on the Service Provider's website (Chapter 1.1.2). The availability of TSP certificates is also indicated in the AIA:CAIssuer field of end-user certificates as standard.

The Service Provider's public keys (including timestamp keys) are accessible as part of its TSP certificates.

6.1.5. Key sizes

The key pairs used by the Service Provider (for both TSO and end-user certificates) meet the requirements of the applicable standards and the Supervisory Body's decision. The algorithms used by the Service Provider:

Hash algorithm IDs:

- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-256 (1) }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-512(3)}

IDs and key sizes of cryptographic algorithms:

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) PKCS-1 (1) RSA Encryption (1) } – Minimum 2048 bit key length
- DSA OID ::= { iso(1) member-body(2) us(840) X9-57 (10040) x9algorithm (4) id-dsa (1) }

The Service Provider may not use the algorithms defined herein past the time indicated in the Supervisory Body's Algorithm Decision.

6.1.6. Public key parameters generation and quality checking

The system used by the Service Provider checks two different aspects of the compliance of key generation parameters:

- the compliance of random number generation used for the parameters (whether the generation is statistically random enough),
- the fulfilment of the conditions and relationships pertaining to parameters.

The basis for checking the compliance of random number generation is whether all cryptographic hardware modules used in the system are capable of statistically testing the consistency and independence of the bit sequence it generates. The modules enable the calling of the tests by way of a standard interface.

Besides the testing instruction that can be called with the use of the external interface, the hardware modules also continuously test their own random number generation and stop if they find any faults.

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

a. Root CA key

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

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

b. Intermediate CA key

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

- Signing end-user certificates
- Signing internal TSP certificates (e.g. OCSP, CRL)
- For testing, if the signature of the Intermediate CA is required for live use

c. End-user certificate keys

The various types of end-user certificates can be used for the following purposes:

- Encryption (encryption certificate)
- User authentication (authentication certificate)
- Signing program code (codesign certificate)
- Website authentication and creating encrypted communication (website authentication certificate)

in accordance with the integrated X509v3 bits.

See Chapter 7.1.2 Certificate extensions for the corresponding values of the key usage fields.

6.2. Private key protection and cryptographic module engineering controls

The Service Provider implements physical and logical protection that prohibits unauthorised certificate issuance.

The Service Provider stores its private keys in a secure manner that prevents access and use by unauthorised persons. The Service Provider stores the TSP private keys used for the creation of certificates, for the authentication of certificate status services, and for other purposes in a physically protected environment and uses those only for the purposes defined for the given key.

6.2.1. Cryptographic module standards and controls

The Service Provider proceeds as set forth below in regard to the creation, saving, storage and destruction of TSP keys:

- keys are created, stored, saved, restored, and destroyed in a physically secure environment under the control of two persons (the joint presence of two employees filling trusted roles) (see Chapter 6.1.1.1),
- in accordance with applicable standards, CA keys are generated, stored, and used on ISO/IEC 19790 or FIP PUB 140-2 level 3 equivalent hardware cryptographic devices with at least EAL4 certificates with the ISO/IEC 15408 or equivalent security

requirements (see Chapter 6.1.1.2 and Chapter 6.2.7 Private key storage on cryptographic module),
- keys can only be used by the authorised persons for functions in line with the purpose of their creation,
- before using their own TSP keys, the Service Provider's systems make sure that the certificates belonging to these keys are valid,
- the Service Provider's certificate, CRL and OCSP signing keys are different from the keys used for all other functions,
- the Service Provider's keys are updated with an out-of-band technique,
- when exporting a key stored in a secure cryptographic module from a module, the Service Provider ensures that the key is protected,
- the systems that process information sensitive from the aspect of cryptography (private or secret keys) outside of a cryptographic device are protected by the Service Provider from becoming compromised by electromagnetic radiation (see Chapter 5.1.3).

The Service Provider handles and operates the cryptographic devices used to provide qualified services separately from those used for non-qualified services and other activities, which latter devices can thereby not influence the reliable operation of the products that are used to provide the qualified service.

The Service Provider keeps a record of its products that are directly used to provide trust services, in which they are classified according to security.

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

The key storage, key generation and signature creation devices used and provided by the Service Provider could be the followings:

Devices	Hardware and firmware specifications	The specification of the software used directly for key management
TSP key device	● ProtectServer Gold (hardware version: B4, firmware version: 2.07.00, 2.08.00 and 3.00.03; Hardware version B2 and B3, firmware version 2.08.00; Hardware version C / PSG-01-0101, firmware version 2.08.00)) ● Luna® PCI 3000 V3.0 Hardware version: VBD-03-0100, firmware: 4.7.1(3000) ● Luna® PCI 7000 V3.0 Hardware version: VBD-03-0100, firmware: 4.7.1(7000) ● Luna® PCI-e 3000 V3.0 Hardware: VBD-04-0100, firmware: 4.7.1(3000) ● Luna® PCI-e 7000 V3.0 Hardware: VBD-04-0100, firmware: 4.7.1(7000)	● ProtectServer Gold (hardware version: B4, firmware version: 2.07.00, 2.08.00 and 3.00.03 Hardware versions B2 and B3, firmware version 2.08.00; Hardware version C / PSG-01-0101, firmware version 2.08.00)) driver, ● Luna cryptographic module drivers ● ProtectServer Internal Express 2 (PSI-E2) drivers

	● Luna® PCI-e 3000 SFF V3.0 Hardware: VBD-04-0102, firmware: 4.7.1(3000) ● Luna® PCI-e 7000 SFF V3.0 Hardware: VBD-04-0102, firmware: 4.7.1(7000) ● Luna® PCI-e cryptographic module Hardware version: VBD-05-0100, VBD 05-0101 and VBD-05-0103, firmware version: 6.2.1 ● ProtectServer Internal Express 2 (PSI-E2) Hardware version VBD-05, firmware version: 5.00.02)	
QSCD Client device (can be used as SCD device too)	● ID-One Cosmo v7.0.1 with IAS ECC 1.0.1 card application (applet version 1121) and NXP P5CC081 V1A (Standard) component ● Gemalto MultiApp ID Citizen 72k intelligent card: S3CC91C microchip, MultiApp v1.1 Java Card platform and IAS Classic v.3.0 electronic signature application (also known as: Gemalto TCP IM CC) ● SafeNet eToken (Smartcard or USB token), Version 9.1, Athena IDProtect/OS755 Java Card card, Atmel AT90SC25672RCT-USB Microcontroller, with integrated IDSign applet ● IAS Classic v3 application Java Card platform with P5CC081V1A chip, MultiApp ID V2.1 according to open standard, MPH117 v2.2 with filter (also known as: Gemalto ID 340)	● Drivers for Oberthur tools ● Drivers for Gemalto tools ● Drivers for SafeNet tools
SCD Client device	● ProtectServer Orange (previously known as CSA 8000 Adapter), hardware version: G version, Cprov firmware version: 1.10 ● IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4, applet IDOneClassIC v1.0 embedded, P5CT072VOP-en, ● IDOneClassIC Card (ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1 platforms: P5CT072VOP, P5CC072VOP and P5CD072VOP) secure signature creation tool ● NLSIGN system ● ProtectServer Internal Express 2 (PSI-E2) Hardware version VBD-05, firmware version: 5.00.02)	● ProtectServer Orange (its early name CSA 8000 Adapter), hardware version: G version, Cprov firmware version: 1.10 ● Oberthur device drivers ● NLSIGN system ● ProtectServer Internal Express 2 (PSI-E2) drivers

The Service Provider continuously monitors the validity of the certificates for the devices it has reported and any newer restrictions pertaining to their application. In the interest of the above, it has taken internal administrative measures to keep records of the validity of the certificates and to track the changes in validity of certification performed within the European Union; in addition, the Service Provider also communicates with the manufacturers and distributors of the devices affected by the certificate to ensure that it learns of changes in certificates as soon as possible.

Service Provider can employ other key handling and cryptographic devices for its own use and as Client devices also, if they possess the certification required for the intended usage.

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

The Service Provider's Security Regulations contain the detailed rules on the multi-person control of private keys.

6.2.3. Private key escrow

See Chapter 4.12.

6.2.4. Private key backup

Saving takes place in a ciphered format. When saving, the private key is copied from the cryptographic hardware module that generated the private key (in accordance with the type of the cryptographic hardware module) to smart cards in several parts (see Chapter 6.2.2) and in a protected manner; otherwise, it ends up in the backup HSM module. The saved copies are provided the same type and strength of protection as the original copy of the hardware module that generated the key. An algorithm and key size is used for encryption that ensures protection for its entire remaining validity. The copies of the TSP private key not being used are protected with a level of security equal to the productive key.

The Service Provider saves the following TSP private keys:

- the Root CA's authenticator private key,
- the Intermediate CA's authenticator private keys.

See Chapter 4.12.1 regarding the saving of end-user private keys.

6.2.5. Private key archival

The Service Provider archives neither TSP private keys nor end-user private keys.

6.2.6. Private key transfer into or from a cryptographic module

The transfer into a cryptographic module of TSP private keys is implemented by the Service Provider in a physically protected environment with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons.

See the contents of Chapter 6.2.4.

6.2.7. Private key storage on cryptographic module

In the case of the TSP private keys stored on cryptographic devices, the Service Provider ensures that the keys cannot be accessible outside the device (with the exception of the saving set out in Chapter 6.2.4). In the case of cryptographic devices, the Service Provider provides protection against forgery even during transport and storage.

See the contents of Chapter 6.2.1.

6.2.8. Method of activating private key

The activation of TSP private keys is implemented by the Service Provider in a physically protected environment with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons. The Service Provider's Security Regulations sets forth the details of the method for activating TSP keys.

The end-user private keys generated by the Service Provider and the Client devices can only be activated with the use of activation data.

In the case of NLSign service the end-user private key is to be activated for every individual or batch signature/seal action.

6.2.9. Method of deactivating private key

The Service Provider's Security Regulations set forth the details of the method for deactivating TSP keys.

6.2.10. Method of destroying private key

The Service Provider destroys the TSP keys in a manner that ensures that the signing keys cannot be restored. During the course of destruction, the Service Provider uses secure deletion processes that actually overwrite all instances of the key on all storage devices on which copies of the key could have occurred.

If a TSP device is destroyed, the Service Provider ensures that the private keys stored on it are also destroyed.

The end-user 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.

6.2.11. Cryptographic Module Rating

See the contents of Chapter 6.2.1.

6.3. Other aspects of key pair management

The Service Provider uses the TSP keys in the manner and for the validity period indicated in the certificate.

6.3.1. Public key archival

The Registration Authority archives all certificates created by the Service Provider for the following period:

- TSP certificates: for 10 years starting from the end of their term of validity,
- end-user certificates: for the time following their expiration as required by relevant legislation (see Chapter 5.5.2).

6.3.2. Certificate operational periods and key pair usage periods

Type	Certificate lifetime	Key pair usage period
Non-eIDAS end-user certificates	maximum of 2 years	The Service Provider does not set a limit for the lifetime of the key but can require the generation of a new key at any time.
TSP certificate	maximum of 20 years	Equal to the validity of the certificate.
Test Certificate	maximum of 1 years	The Service Provider does not set a limit for the lifetime of the key but can require the generation of a new key at any time

The certificate's validity is indicated in the certificate. The validity of the certificate commences at the time of its issuance or thereafter.

6.4. Activation data

The issues related to the activation data are set out in the following chapters.

The installation and restoration of the service key pair on the cryptographic device shall only be carried out under the dual (or higher) control of employees employed in trust position.

The Service Provider shall provide the change of the activation data of the Client Device (SCD or QSCD, managed SCD) in possession of the current activation data. Service Provider shall, under no circumstances, store the end user activation data.

6.4.1. Activation data generation and installation

The Applicant provides the activation data as part of the key generation or, if a Client device provided by the Service Provider is being used, it is generated by the Service Provider.

The Service Provider generates the activation data belonging to the Client device in a secure manner and independently of the device. The Service Provider provides the Receiver with the activation data in a sealed envelope. The End-User can activate its Certificate (see Chapter 4.9.3.2 if the Service Provider has uploaded it to the Client device in a suspended state) or upload it to the Client device (see Chapter 4.3 if the Service Provider only generated the private key for the Client device and is making the certificate available in the Client Menu) after receiving the device and the envelope. It is recommended that the activation data be changed when the Client device is first used.

The activation data can be changed in possession of the current activation data.

6.4.2. Activation data protection

The Service Provider only records the activation data for the Client devices so it can hand it over to the person utilising the service; the Service Provider does not retain a copy.

6.4.3. Other aspects of activation data

The End-User has to ensure that the private keys it is provided are activated and deactivated in a secure manner.

6.5. Computer security controls

Only authorised persons can access the Service Provider's systems. The Service Provider protects the boundaries of internal zones with firewalls and takes the steps necessary to ensure that sensitive data cannot be recovered when data media are reused.

The Security Policies applied by the Service Provider ensure that data can only be added and the measures related to changing certificate status (suspension, revocation, activation) can only be accessed by authorised persons.

The Service Provider uses monitoring and alarm equipment to filter out unauthorised access.

6.5.1. Specific computer security technical requirements

The Service Provider uses multi-factor authentication for all users authorised to issue Certificates in the manner set out in the Security Regulations.

6.5.2. Computer security rating

The Service Provider's Risk Management Regulations for internal use contain the applicable provisions.

6.6. Life cycle technical controls

6.6.1. System development controls

In the case of the systems developed by the Service Provider, the risks are assessed and analysed from a security aspect.

In the case of the software that it developed, the Service Provider applies a change management procedure for issuance, modification, and urgent software repairs. If possible, the change management procedure is completed before placing into operation. Urgent repairs can be an exception to the above, in the case of which the documentation can also be prepared afterwards if placing the software repair into operation at a later time would threaten the Service Provider's operations or would result in serious financial or moral damages.

The Service Provider's Software Development and IT Change Management Regulations for internal use contain part of the applicable provisions.

6.6.2. Security management controls

The Service Provider uses 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 devotes special attention to security even during purchases: the suppliers of its systems of key importance are suppliers evaluated in accordance with the Purchasing Regulations and the purchased equipment are also evaluated equipment. The manufacturers of the equipment are organisations with numerous references and a reliable background. These rules ensure that if necessary, the Service Provider receives the necessary support for its equipment and that any warranty and guarantee claims can be validated against the supplier if any faults occur. The majority of used and integrated equipment are readily available through commercial distribution, meaning they can be replaced with relative ease from several different sources.

The Service Provider protects its IT systems and information from viruses, malware, and unauthorised software. The Service Provider applies procedures that ensure that security fixes can be applied within a reasonable amount of time (6 months). The Service Provider will not apply security fixes if they contain additional security holes or cause instability.

Only authorised persons can make entries and changes to the Service Provider's data. The authenticity of the data can be verified. The data pertaining to Clients are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained.

6.6.3. Life cycle technical controls

The Service Provider continuously monitors capacity utilisation and prepares forecasts in the interest of ensuring that enough storage space and processing capacities will be available in the future as well.

6.7. Network security

The Service Provider classifies the systems it uses for the provision of services into various security zones. Following the above classification, the Service Provider ensures that the communication between the various zones is secure. During the provision of its services, the Service Provider removes or blocks all connections and ports that are not required by the service.

The Service Provider provides a separate network for service systems. The productive systems are separated from development, test, and other systems. The Service Provider developed redundant network connections for all cases that require high availability external access.

In the interest of continuously maintaining security, the Service Provider regularly (every quarter or as soon as possible if any significant network changes take place) performs vulnerability testing.

In addition to the vulnerability testing, the Service Provider annually (or as soon as possible in case of any significant changes in infrastructure) also performs intrusion tests.

Further provisions regarding network security are part of the Service Policy.

6.8. Timestamping

Within the framework of provision qualified certificate issue service, Service Provider shall use timestamps issued by qualified trust provider if timestamping is needed.

Service Provider shall, at least once a day, synchronize the time source of its systems to UTC time source.

7. Certificate, CRL, OCSP profiles

The Service Provider primarily uses certificate profiles to regulate certificate contents and functions. The Subject(s) of the certificate determine the subject data to be included in the certificates; the purpose of use determines the use of the certificate by way of the X509 extensions.

7.1. Certificate profile

The Service Provider uses different certificate profiles in accordance with the certificate's Subject and use. The various certificate profiles have the data that meet MELASZ eIDAS profile recommendations[7], which is to be interpreted as follows.

End-user certificates contain the following data (irrespective of profile):

Name	Contents
Version	3 (0x2)
Serial Number	contains at least a 20 bit random number
CA signature algorithm (SignatureAlgorithm)	sha256withRSA
Issuer	The Issuer data of the certificate's issuer, corresponding to the Subject data in the CA certificate
Validity	The validity of the certificate (from - to)
The certificate signature	The result of the signature performed with the certificate issuer's CA key
Certificate Policy	The identifier(s) of the policy(-ies) applicable to the given end-user certificate Primarily standard and, if applicable, secondary identifiers

Personal certificate profile Subject fields:

Personal certificates are issued to natural person End-Users; thus only a natural person is indicated as the certificate subject, who is identified in the certificate with the use of his/her actual name. The following profile applies to encryption, authentication and codesign certificates.

Field name	Definition
Subject fields	
commonName (CN)	The End-User's full name as registered in authentic records or, if such is unavailable, the name on the certificate used as identification.
surname (SN)	The surname part of the name indicated in the commonName field, in the breakdown provided by the MELASZ profile recommendation.

[7] http://www.melasz.hu/lang-en/a-melasz-hirei/1291-melasz-ready-ajanlas-eidas-kompatibilis-tanusitvany-profilokra

givenName (G)	The first name part of the name indicated in the commonName field, in the breakdown provided by the MELASZ profile recommendation.
emailAddress (E)	The End-User's own e-mail address.
serialNumber (CNSN) (1.)	The permanent identifier created by the Service Provider (the Service Provider's + the client's identifier).
serialNumber (2.) Optional	A unique identifier with the contents required by the client or a group of clients.
countryName (C)	The End-User's country of residence[8]; the two-letter country code as defined by ISO 3166-1.
localityName (L)	The locality of the End-User's residence.
Subject Alternative Name fields	
email	The same as field E.
othername	NetLock's OID based service ID: 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5

Conditions:

- With the exception of the serialNumber field, there can be only be one of each field.

Fields not included above:

- Pseudonym
- An organisation cannot be used as the Subject of a personal certificate, and the appropriate fields are therefore not included (CN/organizationName, CN/organizationalUnitName, CN/ organizationIdentifier, and CN/title).

Pseudonym certificate profile Subject fields:

Personal certificates are issued to natural person End-Users who are identified by a selected name in the certificate. The person's true name (which the Service Provider knows) and the connected organisation are not included in the certificate. The following profile applies to encryption and authentication certificates.

Field name	Definition
Subject fields	
commonName (CN)	The pseudonym selected by the Applicant (unique at the Service Provider)

[8] based on an address card or, in lack of such, other official document

pseudonym (P)	The pseudonym selected by the Applicant. Equivalent to the contents of the commonName field.
serialNumber (CNSN)	The permanent identifier created by the Service Provider (the Service Provider's + the client's pseudonym identifier – see Chapter 1.6.1). 1.3.6.1.4.1.3555.5.x.*ClientPseudID* The value of this field is unique as regards the PSEUDONYM and cannot be the same as the identifier of the pseudonym certificate.
countryName (C)	The Applicant's country of residence; the two-letter country code as defined by ISO 3166-1.
Subject Alternative Name fields	
othername	NetLock's OID based service ID 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5

Conditions:

- There can be only be one of each field.

Fields not included above:

- title, organizationName, organizationalUnitName, organizationIdentifier, localityName, surname, givenName, emailAddress, SAN/Email

Business certificate profile Subject fields:

Business certificates are issued to natural person End-Users, in addition to whom an organisation can also be named as the subject of the certificate (who will be the certificate's Subscriber). The natural person applies for the certificate with the consent of the organisation, and the certificate can then be used in its representation (which in this case does not necessarily mean legal representation). The relationship between the organisation and the person can be of any type (e.g. employee, member, contractual)[9], which is not examined at the time of issuing the certificate; however, the organisation does have to certify the fact of belonging to it (and, if the Title is provided, its contents). The following profile applies to encryption and authentication certificates.

Field name	Definition
Subject fields	
commonName (CN)	Same as the personal profile.
surname (SN)	Same as the personal profile.

[9] As defined by the Electronic Administration Act: "natural person certificate subject: the natural person included in the certificate, regardless of whether the right to represent a non-natural person or a relationship thereto is also certified in the certificate;"

givenName (G)	Same as the personal profile.
serialNumber (1.) (CNSN)	Same as the personal profile.
serialNumber (2.) Optional	Same as the personal profile.
emailAddress (E)	Same as the personal profile.
organizationName (O)	Same as the organisational profile.
organizationalUnitName (OU) Optional	Same as the organisational profile.
organizationIdentifier Optional	Same as the organisational profile.
title (T) Optional	The role or position of the certificate subject in the organisation. This field can contain only verified data. Certain titles can only be used in exceptional cases: (e.g. “Attorney” can only be used for persons authorised for attorney certificates and “CEO” and “Managing Director” can only be used for the persons verified by the business association’s registration documents).
countryName (C)	Same as the organisational profile.
localityName (L)	Same as the organisational profile.
Subject Alternative Name fields	
email	Same as the personal profile.
othername	Same as the personal profile.
dirname Optional	In special cases, the End-User name with a different manner of writing than that indicated in the CommonName field.

Conditions:

- With the exception of the serialNumber field, there can be only be one of each field.

Fields not included above:

- Pseudonym

Organisational certificate profile Subject fields:

Organisational certificates are issued to legal person Subscribers; thus only this legal person can be indicated as the certificate subject. The profile applies to encryption, authentication and codesign certificates.

Field name	Definition
Subject fields	
commonName (CN)	The Subscriber's full or short name, OR A certified DBA name / Trademark / Product name and the related identifier, which is both unique and used exclusively by the legal person.
organizationName (O)	The Subscriber's full or short name
organizationalUnitName (OU) Optional	The name of the Subscriber's organizational unit within the organisation identified in the organizationName field.
countryName (C)	The country of the Subscriber's official seat (the two-letter country code as defined by ISO 3166-1).
localityName (L)	The name of the locality of the Subscriber
serialNumber (CNSN) (1.)	The permanent identifier created by the Service Provider (the Service Provider's + the client's identifier). 1.3.6.1.4.1.3555.5.1.*ClientID*
organizationIdentifier	The Subscriber's registered identifier (see Chapter 3.1 Naming).
emailAddress (E)	Subscriber's e-mail address.
Subject Alternative Name fields	
email	The same as field E.
othername	NetLock's OID based service ID: 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5
dirname Optional	The following, as used by the organisation and certified by a statement: ● DBA name ● or Trademark ● or Product name and related identifier.

Conditions:

- With the exception of the serialNumber field, there can be only be one of each field.
- Pseudonyms cannot be used in organizational certificates.

Fields not included above:

- Title, Pseudonym, organizationIdentifier, surname, givenName

The interpretation of the data contents included in the certificate:

- The certificate belongs to the organisation called O, as indicated in the certificate (within which, if indicated, the OU organizational unit).

DV website authentication certificate profile Subject fields:

The DV SSL certificate is a website authentication certificate that has a Subject of one domain name.

Field name	Definition
Subject fields	
commonName (CN) Optional	If the field is present, it can contain one domain name from among those included in the SAN/dNSName. Only an existing domain name rightfully used by the Applicant can be used. Pseudonyms are not allowed. The indicated domain name can be a wildcard.
Subject Alternative Name fields	
DNSname	The domain names of the websites authenticated by the certificate. Only existing domains name rightfully used by the Applicant can be used. They can contain wildcards.

Conditions: -

Fields not included above:

- givenname, surname, organization, country, locality, title, pseudonym, organizationalUnitName, organizationIdentifier

TSP Root CA certificate profile:

Field name	Contents
Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 20 bits of entropy)
public key	see minimum algorithms table
Validity	The validity of the certificate (from - to)
subject:commonName (CN)	Root CA name
subject:countryName (C)	HU
subject:localityName (L)	Budapest
subject:organizationalUnitName	Certificate CAs (Certification Services)
subject:organizationName (O)	NetLock Kft.

Signature	the Root CA's own signature	
Extensions		Critical
basicConstraints	CA:TRUE	Yes
keyusage	keyCertSign, cRLSign	Yes
Subject Key identifier	subject key hash	No

Requirements: the self-signed subject and issuer parts of the root authenticator certificate are the same

Fields not included above: certificatePolicy, extendedKeyusage

TSP Intermediate CA certificate profile

Field name	Contents	
Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 20 bits of entropy)	
public key	see minimum algorithms table	
Validity	The validity of the certificate (from - to)	
subject:commonName (CN)	Intermediate CA name	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
subject:organizationalUnitName	Certificate CAs (Certification Services) or not included	
subject:organizationName (O)	NetLock Kft. or NetLock Ltd.	
Signature	Root CA signature	
Extensions		Critical
basicConstraints	CA:TRUE	Yes
keyusage	keyCertSign, cRLSign	Yes
Subject Key identifier	subject key hash	No

AIA:Ca issuers	The availability of the certificate of the root CA that issued the certificate, in an http URL format	No
AIA:OCSP	The availability of the OCSP service of the root CA that issued the certificate, in an http URL format	No
CDP	The availability of the CRL service of the root CA that issued the certificate, in an http URL format	No
Authority Key Identifier	The hash of the Root CA's issuing key	No

Conditions: -

Fields not included above: certificatePolicy, extendedKeyusage

The connection of the various certificate profiles with certificate policies and certificate types:

The table defines the profiles and certificate policies that the various certificate types are available with.

Profile	Certificate policies	Certificate types
Personal	LCP	Encryption, authentication
Pseudonym	LCP	Encryption, authentication
Business	LCP	Encryption, authentication
Organisational	LCP	Encryption, authentication
Website authentication	DVCP	Website authentication
Service Provider	-	Service Provider

The Service Provider can create additional special profiles within the certificate profiles listed above (e.g. business profiles that meet the requirements of certain professions).

7.1.1. Version number(s)

The Service Provider issues certificates in accordance with the X.509v3 specifications.

7.1.2. Certificate extensions

The Service Provider uses the certificate extensions defined in the X.509v3 specifications by indicating the critical fields. All end-user certificates include the following certificate extensions:

Extension	Critical	Contents
basicConstraints	yes	CA:FALSE
subjectKeyIdentifier	no	The Subject's own key ID
Subject Alternative Name	no	Other names of the Subject. See the Subject fields of the various certificate profiles for how this is to be filled out.
authorityKeyIdentifier	no	The certificate issuing CA's key ID
crlDistributionPoints	no	The availability of the CRL
Authority Information Access:CAIssuers	no	The availability of the TSP certificate
authorityInfoAccess:OCSP	no	The availability of the OCSP
Certificate Policies	no	The identifier of the Certificate policies that was used for issuing of the certificate (see the Chapter Certificate policies). If more than one HRs are identified, the field is included more than once. No policy constraints are used. Of the policy qualifiers, only the User Notice field is filled out, the contents of which is a brief textual description, indication, or supplementation with restricting information of the policy valid for the certificate, in a format that is legible for humans.
Keyusage	yes	The permitted possibilities for using the private key paired to the public key included in the certificate (see below for filling out).
extendedKey Usage	no	The use possibilities of the private key extending keyusage (see below for filling out).
QcStatements/QcType	no	The certificate type with the following possible values: ● id-etsi-qct-esign - for signature certificates ● id-etsi-qct-eseal - for seal certificates ● Id-etsi-qct-web – for website authentication certificates The types are indicated with OID values.

Filling out end-user key use extensions, according to certificate types:

Cert type / Key use	Encryption certificates	Authentication certificates	DV Certificate for Website Authentication
Keyusage	KeyEncipherment	digitalSignature	keyAgreement, KeyEncipherment, KeyExchange
extendedKey Usage	emailProtection	clientAuth	serverAuth

The End-User can use the private key only for the purposes indicated here (the parentheses include the certificate's applicable use):

- nonRepudiation: ensuring non-repudiation (Verification of user)
- digitalSignature: Electronic signature (Verification of integrity and authenticity)
- KeyExchange: Key replacement
- keyAgreement: Key agreement
- KeyEncipherment: Key encryption (Key decryption)
- clientAuth: Client identification (Client authentication)
- serverAuth: Server identification (Server authentication)

7.1.3. Algorithm object identifiers

The Service Provider indicates in the certificate the name and parameters of the algorithm used for the authentication of the certificate. Refer to Chapter 6.1.5 for the possible values.

7.1.4. Name forms

The provisions of Chapter 3.1 are governing as regards Subject names forms.

The value in the certificate's CA ("Issuer") field is the same as the "Subject" value in the issuing CA certificate.

7.1.5. Name constraints

The Service Provider indicates any name constraints in the "nameConstraints" field.

7.1.6. Certificate Policy object identifier

In the certificates issued on the basis of the Certificate Policy, the Service Provider indicates the Certificate Policy OID.

7.1.7. Usage of Policy Constraints extension

The Service Provider sets no requirements.

7.1.8. Policy qualifiers syntax and semantics

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

7.1.9. Processing semantics for the critical Certificate Policy extension

The Service Provider sets no specific requirements.

7.2. CRL profile

7.2.1. Version number(s)

The Service Provider issues CRLs in line with the x509 and RFC5280 standards with the frequency and contents defined in the Policy.

7.2.2. CRL extensions

The CRL does not contain any fields marked as critical. The Service Provider provides CRLs with serial numbering increasing at a rate of one.

The certificate's CRL profile:

Field	Contents
Version	V2
Issuer	The Issuer data of the certificate issuer that issued the CRL
Last update	Date of last update
Next update	Date of next update
Signature	Electronic signature of the issuer
CRL entry	The serial number of the invalidated certificate, the date, time, and reason of invalidity in a format in line with RFC 5280.
CRL entry extension	

7.3. OCSP profile

7.3.1. Version number(s)

During the course of the OCSP service, the Service Provider supports the certificate status questions and responses created on the basis of version V1 of the RFC 6960 standard.

7.3.2. OCSP extensions

The OCSP responder certificate includes the NoCheck extension, meaning the OCSP responders do not have to be checked by the client.

The certificate profile of the OCSP responder:

Field name	Contents	Critical
basicConstraints	CA:FALSE	Yes

Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 20 bits of entropy)	No
extendedKeyusage	OCSPSigning	No
keyusage	digital signature	Yes
private and public key	see minimum algorithms table	No
Validity	The validity of the certificate (from - to)	No
Subject Key identifier	subject key hash	No
Authority Key identifier	CA key hash	No
OCSPNocheck	empty	No

Conditions: -

Fields not included above: certificatePolicy

8. Compliance audit

TSP shall provide its services compliance with:

- applicable regulation og EU and Hungary,
- rules of present Practice Statement
- standard ETSI 319411-1

Before commencing the provision of its services, the Service Provider had an external, independent conformity assessment body evaluate those on the basis of applicable standards and legislation.

8.1. Frequency or circumstances of assessment

Once a year, the Service Provider conducts an internal self-audit, with the help of which it regularly reviews compliance with the Service Policy and the present Statement, as well as previous audits and evaluations; if any derogations are uncovered, it takes the necessary measures to correct those.

In the course of the annual self-revisions, the Service Provider audits at least 3% of the website authentication certificates (DVCP) selected with random sampling, it has issued since the previous self-audit.

8.2. Identity/qualifications of assessor

Internal audits are performed by an experienced professional who has the suitable legal and technical know-how, a higher education degree, and at least 5 years of experience in regulation, IT system audits, or trust services.

External conformity assessments are performed by a legal person that has suitable authorisation granted by a national accreditation organisation of an EU Member State.

During the course of external conformity assessments, the Service Provider cooperates with a natural or legal person, or a group of natural persons, who or that

- is/are capable of performing an audit as regards the standards set forth in Chapter 8;
- meet the requirements set out in Chapter 8.3;
- has/have suitable experience regarding PKIs, IT, IT security solutions, technologies, and audits,
- in the case of audits/evaluations 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*
    - accreditation to perform an ISO 27001 assessment with the ISO 27006 methodology provided by the National Accreditation Authority in accordance with ISO 17021;
- 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 assessor's activities.]

8.3. Assessor's relationship to assessed entity

The trust employees filling the role of Independent System Controller who perform internal conformity assessment at the Service Provider are independent of the Service Provider's organizational units responsible for services.

The auditors who perform external conformity assessment are independent from:

- the owners, managers, and operations of the audited Service Provider;
- the audited organisation, i.e. neither the auditor nor any direct relation is in an employment relationship with the Service Provider;
- the results of the activities performed during the assessment, which do not affect their relationship.

8.4. Topics covered by assessment/audit

The following topics are covered by assessments/audits:

- compliance with applicable law;
- compliance with technical standards;
- compliance with the Service Policy(-ies) and Practice Statement(s);
- compliance of applied processes;
- compliance of physical security;
- compliance of staff;
- compliance of IT security;
- adherence to data protection privacy policy.

8.5. Actions taken as a result of deficiency

The Service Provider summarizes the results of external and internal conformity assessments in a report that includes the system components and processes that were audited. The document includes the evidence used during the audit and the assessor's findings. The report furthermore

contains the deficiencies and derogations uncovered by the audit and the deadlines set for their repair. The uncovered deficiencies are classified into the following categories in accordance with their severity:

- “Slight” deviation, for which the documents certifying the corrective measures have to be presented during the subsequent assessment.
- “Severe” deviation, for which the documents certifying the implemented corrective measure have to be presented during the current assessment.

The Service Provider is obligated to provide a written response to the deviations recorded by the independent assessor and to present as of the next assessment the measures taken to correct those.

8.6. Communication of results

The Service Provider will not disclose the detailed assessment report drawn up on the assessment or audit. However, it will disclose the issued certificate within three months of the assessment.

9. Other business and legal matters

9.1. Fees

The Subscriber is obligated to pay in advance the value of the periodic services and the other services made use of in addition or during applying for those (e.g. optional services), as well as other fees determined by the Service Provider (e.g. administration fee), in the manner set out in the GTC and according to the price list made available on the Service Provider website or in the individual client offer.

In the price list published on its website and in its offers, the Service Provider determines especially, but not exclusively, the following fees for the services set out in the present Statement and the related optional service fees.

Periodic Services:

- Certificate service (see Chapter 9.1.1 fejezet);
- Service pack(see Chapter 9.1.4.2);
- services not detailed in the present practice statement (see Chapter 9.1.4.2);

Optional services related to certificate issuance:

- Mobile registration service;
- Delivery of Client device with an approved agent;
- Identification via a Registration Agent;
- Post payment);
- Management of Client requests for amendments to the Service Agreement;
- Unlocking a blocked Client device;
- Replacing a Client device;
- Other administrative fees.

The Service Provider publishes on its website the exact definitions and conditions of the various optional services. The Service Provider may suspend the provision of optional services and can also introduce other optional services in addition to those listed above, about which it will publish information on its website.

The fees for applying for services and for the optional services provided with those are payable to the Subscriber together with the fee of the given service.

The Service Provider can also sell the services as part of service packages, in which case the service fee is included in the service package fee. The conditions of packages and the other rules pertaining to the Service Provider are laid out in the GTC.

9.1.1. Certificate issuance or renewal fees

The Certificate creation service fee includes the issuance of the certificate (as part of an initial, renewal, modification, or re-key process), its publication during the entire term of validity (in the certificate repository or in the CRL), the provision of related services (e.g. certificate status), and storage during the entire retaining period.

9.1.2. Certificate access fees

The Service Provider does not charge for queries from the certificate repository if they take place in accordance with the applicable rules of Chapter 2.4, if the interface maintained by the Service Provider for the purpose on its website is used, and if certificates are queried one at a time with the manual entry of the data required for viewing certificates.

The Service Provider only provides for other uses of the certificate repository (e.g. large number of automated queries) on the basis of a separate agreement and with the conditions and for the service fee set forth therein.

9.1.3. Status changes or status information access fees

The Service Provider does not charge for certificate status changes (see Chapter 9.1.3).

The Service Provider only provides for uses of the certificate status service other than that set out in Chapter 2.4 (e.g. frequent or a large number of OCSP queries) on the basis of a separate agreement and with the conditions and for the service fee set forth therein.

9.1.4. Fees for other services

a. Fees for service packs

The fees of the service packs under the GTC include the fees of the timestamps that can be used during the term, and the fees of the client devices.

b. Fees for other services not detailed in this Statement

The Service Provider may also charge a fee for the services not detailed in this Statement if those are published on its website in accordance with the GTC or it concludes an agreement with the Subscriber for the provision of such service.

9.1.5. Refund policy

If the service agreement is terminated for a proven serious breach of contract on behalf of the Service Provider as defined in the GTC or due to an amendment of the GTC, or the Service Provider terminates the given service during the term of the agreement (and it is not taken over by another service provider), the Service Provider will pay a fee commensurate to the provided services to the Client as compensation. If the service agreement is terminated or rescinded within 14 days of its conclusion, the Service Provider will refund the entire service fee.

In other cases, e.g. the service agreement is terminated (before its expiration), or the service was not used, the Client device was not taken over, or the service packages pertaining to the contractual term are not used up, the Service Provider will not refund any part of the paid service fees to the Subscriber. The fees of these services were set with the express assumption that a certain proportion of Clients would only make use of a part of the quotas.

9.2. Financial responsibility

The Service Provider restricts its financial liability as set forth below:

In respect of the various services and certificate types, it sets different values for assumptions of liability in the Price list which can be validated per insurance event (which took place as a result of one or more reasons but are linked in time). If more than one Client or several different agreements and the related certificates, timestamps, or files are affected in a given insurance event, the rate of compensation is determined for the individual Clients and agreements (certificates) in a manner that ensures that the highest value of assumption of liability is not exceeded by the total amount of compensation and the value of such assumption for the given service or certificate type is limited in all cases.

The Service Provider provides information on the value of assumed liability on its website.

These amounts were defined for the full price amounts included in the Services price list. If the Client receives the services at a discounted rate, the amount of compensation will be defined commensurately to the provided discounts and will be proportionate to those.

Service Provider can define transaction limits for the certificates that is shown in the certificates at the Price list. The Service Provider is not liable if the certificate is used in transaction with higher value than this limit.

9.2.1. Insurance coverage

Service Provider has liability insurance in order to cover the costs for indemnifying Clients and Relying Parties and any other incurred costs. The liability insurance covers the Service Provider's indemnification liabilities incurred during the provisions of all services set out in this Statement. See Chapter 9.6.

The liability insurance shall, in addition, cover the followings:

- the damages caused to trust service clients in connection with the breach of the trust service agreement,
- the non-contractual damages caused to trust service clients and third parties,

The insurance coverage set out in the insurance agreement shall not be lower than HUF 3,000,000 (three million Hungarian forints) per damage.

In the case of DVCP web authentication certificates, the upper limit of compensation paid by liability insurance is the forint value of USD five million, at the bank exchange rate at the time of paying indemnification.

9.2.2. Other assets:

The Service Provider has cover for the costs related to the performance of the requirements for terminating the service. A HUF 25,000,000 bank guarantee is in place for the fulfilment of the obligations.

9.2.3. Insurance or warranty coverage for relying parties

The Service Provider is liable for the damages caused to third parties that it does not have a contractual relationship with in accordance with the general rules of the Civil Code.

9.3. Handling of business information

The Service Provider stores and handles the confidential information that comes into its possession by taking into account the provisions of relevant legislation and in accordance with Chapter 5 and the Service Provider's private Data Management Regulations.

When the obligation of storage expires, the Service Provider irrevocably deletes the confidential information, unless provided otherwise by the Client.

9.3.1. Scope of confidential information

The Service Provider considers all data pertaining to any Clients and not included in Chapter 9.3.2 to be confidential information. The following are especially confidential information:

- the Client personal information that is not included in the certificate;
- registration data (e.g. audio and video recordings, document copies);
- the audio recordings recorded at customer service;
- private keys and their activation data;
- certificate enrolment data;
- service agreements;
- private regulations;
- the log data created in connection with the services;
- all data that would threaten the security of services if disclosed;
- all data that, if disclosed, could lead to third parties learning of the above data.

The Service Provider handles confidential information in the manner set out in Chapter 9.3.3.

9.3.2. Information not within the scope of confidential information

The Service Provider does not consider the following information to be confidential:

- the certificate data required for certificate status services;
- all data included in the certificate (see Chapter 7.1), unless provided otherwise by the Applicant during the application;
- other anonymized data that can no longer be linked to the owner of the information or to any persons about which conclusions can be drawn on the basis of the information.

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

9.3.3. Protection of confidential information

In addition to the requirements set forth by law and the present Practice Statement, the Service Provider takes all measures, including the method defined in the Data Management Regulations, for the secure handling of the confidential information as defined in Chapter 9.3.1.

The Service Provider stores in an electronic format any data that it was provided in an electronic format; any information provided to it in hard copy format can be stored and managed in both hard copy form and/or electronic format.

The Service Provider retains personal information, protects their security, and prevents data loss, damages, and the incorrect or unauthorised use in the manner laid out in Chapter 5.5 and by taking into account the IT security requirements of Chapter 6.5.

The Service Provider grants access to the confidential information that comes into its possession only to those of the employees defined in Chapter 5.2.1 for whom the information is required (e.g. Registration Administrators).

Service Provider shall disclose confidential information only in the following cases and means:

- In case Service Provider terminates of all of its trust services, the Service Provider shall, following the termination of the activities related to service provision, provide the statutorily specified recipient service provider with access to the registries related to the services, and shall hand over all data related to the revoked certificates (including personal data).
- Service Provider shall, without any delay, provide the investigative authority and/or national security services with the requested data upon request, for the purpose of detection or prevention of criminal offenses that may be linked to the trust services of Service Provider or in the interest of national security, upon the fulfilment of the criteria set out in separate legislation, including the handover of personal and other information verified and recorded in the course of the authentication-certification procedures (see Chapter 3). Service Provider shall draw up minutes of the fact of disclosure, but Service Provider shall not notify the affected Client or Clients of the disclosure, pursuant to the applicable legislation.
- In the case of civil litigious or non-litiguous proceedings that affect the validity of the certificate issued by Service Provider, Service Provider is entitled to disclose, upon request, the personal and other data verified and recorded in the course of the authentication-certification procedures prior to the issue of the certificate (see Chapter 3) to the counterparty to the proceedings or to the representative therof, or may disclose such data to the court that contacted the Service Provider with such request.

Service Provider shall have no right to refuse the disclosure of data in the above statutority regulated cases. In the course of the disclosure, Service Provider shall maintain the confidentiality of the data, as well as their complete, true and correct form. The actual management of the Service Provider shall appoint the employee responsible for the performance of the mandatory disclosures and for recording the minutes.

9.4. Privacy of personal information

With the exceptions set out in Chapter 9.3.2, the Service Provider considers Client personal information to be confidential information as defined by Chapter 9.3.1 and handles those in line with the provisions of Chapter 9.4.1 and by providing them suitable protection (Chapter 9.3.3).

9.4.1. Data management

The Service Provider handles Client personal data in line with the provisions of:

- this Statement and the Service Policy,
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information,
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and
- the Service Provider’s Data Management Regulations.

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 to Clients on its website.

The Service Provider is registered by the Nemzeti Adatvédelmi és Információszabadság Hatóság [The Hungarian National Authority for Data Protection and Freedom of Information] (NAIH) as a data controller.

9.4.2. Private information

The Service Provider considers all data in its possession to be private information

- on the basis of which the natural person can be identified, with especial regard to the name of the person or his/her identifier registered by the authorities, and
- which can be linked to a natural person, or
- from which conclusions can be drawn regarding the natural person,

and which is not listed under Chapter 9.4.3.

The Service Provider requests the Client to provide only the personal information that is required for the provision of the requested service. This does not exclude the possibility of the Service Provider also requesting data that allow it to perform its activity more effectively. The provision of these data is not obligatory.

9.4.3. Information not deemed private

The Service Provider does not consider the data referred to in Chapter 9.3.2 to be personal.

9.4.4. Protection of personal data

The provisions of Chapter 9.3.3 are applicable to the protection of personal data.

9.4.5. Usage of private information

The personal data related to the issuance of certificates and not included in the certificate are securely stored and protected by the Service Provider and are used only according to the provisions of the act on informational self-determination.

9.4.6. Data management

If granted the consent of the Client, the Service Provider stores and handles the personal information that comes into its possession by taking into account the legislative provisions listed on Chapter 9.4.1 and in accordance with the provisions of Chapter 5; the Service Provider can only hand those over to the third parties defined by law in the cases referred to in Chapter 9.3.3.

Clients grant their consent for the management of their personal information by requesting/ordering services.

9.4.7. Other information disclosure circumstances

In the interest of uncovering and preventing crimes with the use of the 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 is recorded by the Service Provider; however, it does not inform the Relying parties of the data provision.

9.5. Intellectual property rights

All of the

- names,
- products,
- software and hardware components

used during the course of the service activity are owned by the Service Provider, or the Service Provider uses those lawfully.

Furthermore, the

- regulations,
- contractual conditions,
- other documents and information prepared by it,
- certificates,
- certificate status service data,
- and individual identifiers disclosed/issued/created by the Service Provider are also owned by the Service Provider.

The Subscriber is the owner of the public and private keys issued by the Service Provider.

The End-User is the user with full rights of the end-user certificate, the public key included therein, and the permanent identifier.

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 (see Chapter 4).

During its operations, the Service Provider takes care not to infringe upon the intellectual property rights of third parties.

9.6. Representations and warranties

The Service Provider is liable for damage caused intentionally or through negligence to any natural or legal person due to a failure to comply with undertaken obligations.

In the case of services, the party applying for compensation has to prove that the Service Provider acted intentionally or negligently.

In the case of qualified services, the Service Provider's intentional / negligent actions are assumed until the Service Provider proves otherwise.

The Service Provider is not responsible for damages that exceed beyond the restrictions applicable to the use of services (see this Statement, the Service Policy, the GTC, and the service agreement for the restrictions).

The Service Provider is liable for the service activities performed in the framework of its regulations and for the operations of its Registration and Certification Authority even if any functions are performed by TSP Partners.

9.6.1. The Certification Authority's responsibilities

See Chapter 9.6.1 of the Service Policy.

9.6.2. The RA’s responsibilities

See Chapter 9.6.2 of the Service Policy.

9.6.3. Client representations and warranties

See Chapter 9.6.3 of the Service Policy.

The Applicant is responsible for:

- providing and verifying the data required for processing applications (see Chapter 4)
- the veracity, accuracy, and validity of the data provided during registration and application;
- cooperating with the check outlined in Chapter 3 pertaining to identity and the data provided during application, and for taking all steps that can be expected of it to ensure that the process can be completed as quickly as possible;
- checking the data in the certificate after its issuance and for notifying the Service Provider if it uncovers any deviations;
- reporting without delay any changes to data and requesting the suspension or revocation of the Service Provider and for the suspension of the use of the keys;
- becoming familiar with the contents of the Service Policy, this Service Policy, the GTC, and the service agreement before making use of the services.

The End-User is responsible for:

- using its Client device, key, and certificate in accordance with the regulations;
- the secure handling of its Client device, key, and activation data,
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the certificate or its use before using legal means to settle the dispute;
- using the services in the manner required by law and this Statement;
- using certificates for the purposes and with the restrictions indicated therein;
- the use of private keys belonging to test certificates without actual commitment and for testing purposes;
- if the End-User’s private key, Client device, or activation data ends up in unauthorised hands or suspicion of such arises, the End-User is obligated to inform the Service Provider without delay and to initiate the suspension or revocation of the certificate(s), and the use of the certificate must be terminated.

The Subscriber is responsible for:

- familiarizing itself with the Service Provider’s regulations before making use of the service;
- the veracity, accuracy, and validity of the data provided during application;
- cooperating with the check outlined in Chapter 3 pertaining to the data provided during application, and for taking all steps that can be expected of it to ensure that the process can be completed as quickly as possible;
- initiating the modification, re-key, or revocation of the certificate as per Chapters 9.6.3 and 4.9.1 of the Service Policy and Chapters 4.7 and 4.8 of this Statement;
- adhering to the End-User’s obligations to the degree it effects those;
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the certificate or its use;

- ensuring that unauthorised persons cannot access the data and devices required for making use of the services;
- assuming liability for adhering to the End-User's obligations to the degree it effects those;
- meeting its fee payment obligations.

9.6.4. Relying party representations and warranties

See Chapter 9.6.4 of the Service Policy.

In the interest of the circumspect procedure required for maintaining the security level guaranteed by the Service Provider, it is recommended that Relying Parties:

- adhere to the requirements and rules set out in the Service Provider's Service Policy and this Statement;
- use reliable IT environments and applications;
- check certificate statuses with the current CRL or OCSP response (see Chapter 4.9.6);
- take into consideration all restrictions (indicated in the policies and the certificate) applicable to certificate usage.

Relying Parties are authorised to decide at their own discretion and/or on the basis of their own policies on whether to accept certificates and on the method for doing so.

9.6.5. Representations and warranties of other participants

No requirements.

9.7. Disclaimers of warranties

The Service Provider will reject claims for warranty, guarantee, or compensation against the Service Provider for its services if

- the event on which it is based can be traced back to the Client's omission, failure to meet an obligation or responsibility, or an external, unforeseeable event;
- the regulations applied by Relying Parties do not meet the requirements of the present 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 limits its liability as set forth in Chapter 9.16.5 and below.

The Service Provider is not liable for damages resulting from a circumstance subject to the exclusion of the Service Provider's warranty as defined in Chapter 9.7, or if the Client or Relying Party did not proceed with proper diligence, proceeded contrary to the Service Provider's Conditions, or proceeded unlawfully.

The Service Provider is only liable against third persons for contractual and non-contractual damages related to its services to the extent that they were caused by its own fault, from a breach of its obligations, or for a reason attributable to it, and if the damages can be proven.

The Service Provider does not assume liability for using test certificates for other purposes than testing.

See also the contents of Chapter 9.2 and 9.6 for liability and its limitations.

9.9. Indemnities

The Service Provider has liability insurance to cover its indemnification obligations (see Chapter 9.2).

The Client is obligated to indemnify the Service Provider for any proven losses or damages that are incurred by the Service Provider as a result of the Client failing to meet obligations or adhere to recommendations either intentionally or through negligence.

The general provisions of the Civil Code are applicable to compensation and indemnification proceedings; the Service Provider provides details on the procedure in its GTC.

As regards proving liability, see Chapter 9.6 and the contents of 9.7 and 9.8 for warranty, guarantee, and compensation and indemnification claims.

9.10. Term and termination

9.10.1. Term

The term of this Statement starts on the day this version becomes effective as indicated on the cover (effective date).

The personal scope of this Statement extends to the Service Provider’s trusted employees, the Service Provider’s partners, to Clients, and to all Relying Parties.

The scope of this Statement includes the provision and usage of services as defined in Chapter 1.1 of this Practice Statement.

9.10.2. Termination

The Statement remains valid until the service is terminated, the Statement is revoked, or until a new version enters into effect. As regards the validity of the certificates issued during the term of this Statement, Chapter 9 of the Statement shall be applied even after the validity of the Statement itself, regardless of the manner for the termination of its validity.

9.10.3. Effect of termination

If the present Statement 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 Practice Statement is revoked.

9.11. Individual notices and communications with participants

In the interest of communicating with its Clients, the Service Provider operates a customer service office and telephone service, which is available at the contacts provided in Chapter 1.1.2 (also see Chapter 1.3.2).

During the administration of service usage and other tasks related to end-user certificates, Customer Service primarily communicates with Clients via emails. Customer service can also be contacted both by phone, fax and in person.

The Service Provider provides a unique identifier to all Customer Service emails sent to Clients, based on which the given data or topic can be easily identified if contacted by the Client. If a Client responds to such an email, the subject of the email should be kept the same in order to facilitate the process.

If the Client sends an email other than a response to a Customer Service email, it should take all steps necessary to ensure that the email can be identified as easily as possible, e.g. by providing an electronic signature/seal to the email and/or sending it from the email address in the certificate in question.

In the course of contact by email, it is also necessary for the service or certificate in question to be unequivocally identifiable.

If the Client contacts the Service Provider by email or fax, the Registration Administrator is responsible for deciding what steps can be taken on the basis of the fax or email. If the Service Provider requires more information, it provides information in its response. If doubt arises regarding the identifiability of the Client, the Service Provider will attempt to contact the Client by phone to conciliate personal information.

In addition to communication by email, the following channels of communication are also open to Clients.

Phone

A customer service representative is only available at the customer service number during the indicated times; otherwise, a message can be left (except for certificate revocation, see Chapter 4.9.4).

Personally in the customer service office

The Service Provider only provides personal service at its customer service office (see Chapter 1.1.2) with appointments.

9.12. Modifications

If any changes occur in normative regulations, security requirements, the market environment, or other circumstances, the Service Provider will amend its Practice Statement. Compliance of regulations with each other, relevant legislation, and applicable standards is examined at least annually. The regulations are to be reviewed and amended whenever justified by changes in relevant legislation and/or the environment of technical standards. Based on the experience it has gained during its operations, the Service Provider continuously reviews its Practice Statement.

See also Chapter 1.5 and 2.1.

9.12.1. Amendments

The Service Provider will examine requests for amendments as regards their compliance with the content requirements defined in the Service Policy, the law, and standards. If no objections are raised regarding either, it accepts the request for amendment and commences its processing.

The person who approved the Statement approves the amendments, prior to which the above requirements regarding content and form are again checked. Clients and Relying Parties are then notified. The Service Provider has final liability and responsibility for approving the Policy.

The Service Provider accepts comments regarding the published draft Policy for 14 days after its entry into effect; comments are to be submitted by email. In case of any comments affecting the merits, the Service Provider makes the necessary modifications to the draft and finalizes and published the version changed on the basis of the comments 7 days before its entry into effect.

9.12.2. Notification mechanism and period

There are no requirements to notice supervisory body in case of non-eIDAS services.

9.12.3. Circumstances under which OID must be changed

New versions of the Practice Statement are published with new version numbers.

9.13. Dispute resolution

The Service Provider (including service provider partners) receives questions, objections, and complaints pertaining to its activities by email, phone, or in person at the Service Provider's customer service offices (see Chapter 1.1.2).

If any disputes or complaints occur, Clients are obligated and Relying Parties and other third parties are recommended to notify the Service Provider immediately before taking legal steps and to inform the Service Provider of all aspects of the case. The Parties will always attempt to settle disputes by amicable means through negotiations.

9.13.1. Dispute resolution provisions

The Service Provider will examine complaints within 30 calendar days of their having been reported and will inform the complainant by email of the results of the inspection, unless agreed on otherwise by the parties. If the examination of the complaint is expected to take more than 30 calendar days due to the nature of the complaint, the Service Provider will inform the Client that submitted the complaint.

In case of complaints filed in person or by phone, the Service Provider will draw up records on the receipt of the complaint.

After examining the complaint, the Service Provider will fix (if applicable) the error within the time technically justified and will inform the reporting party about this activity in writing.

If the reporting Client does not accept the response, it can initiate negotiations with the Service Provider. If the Service Provider rejects an application for negotiations or if the negotiations do not lead to results within 20 workdays of their commencement, the dispute can be settled according to Chapter 9.13.2.

9.13.2. Amicable dispute resolution through negotiations

If the negotiations between the Client and the Service Provider do not lead to results, the Client is recommended to turn to the Budapesti Békéltető Testület [Budapest Conciliatory Body] before initiating court proceedings.

The contact information of the competent bodies as of the entry into effect of this Statement:

Budapesti Békéltető Testület [Budapest Conciliatory Body]:

- Address: 1016 Budapest, Krisztina krt. 99. III. em. 310.
- Mailing address: 1253 Budapest, Pf.: 10.
- Email address: bekelteto.testulet@bkik.hu
- Website: www.bekeltet.hu

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály [Budapest Government Office, Consumer Protection Department]:

- Address: 1056 Budapest, Váci utca 62-64.
- Phone: +36-1 328 5862
- Mailing address: 1364 Bp., Pf.: 234
- Email: budapest@bfkh.gov.hu

9.13.3. Litigious dispute resolution

If the dispute cannot be settled with any of the negotiation methods outlined in Chapter 9.13, the Parties will take the case to court. In this case, the Parties subject themselves to the sole competence of the Court of Budapest Districts II and III.

9.14. Governing law

The Service Provider shall perform its activity in accordance with 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 (see chapter 9.15).

9.15. Compliance with applicable law and standards

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.

TSP is not obligated services according to present Service Policy to compliance to the following laws and regulations, however these services typically compliance the requirements of these regulations to maintain uniform conditions.

- **eIDAS:** 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
- **Electronic Administration Act:** Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services
- **BM Decree:** Decree 24/2016 of 30 June of the Minister for the Interior on the detailed requirements pertaining to trust services and their providers
- Decree 26/2016 of the Minister for the Interior about the content of the records led by the supervisory body and the notifications regarding the provision of trust services
- **Public Administration Decree:** Government Decree 137/2016 of 13 June on the requirements for the use of electronic signatures and seals related to the provision of electronic administration services
- **Commission Implementing Decision (EU) 2015/1506** of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of 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

- **Government Decree 137/2016** of 13 June on the requirements for the use of electronic signatures and seals related to the provision of electronic administration services;
- **Consumer Protection Act:** Act CLV of 1997 on Consumer Protection
- **Records Act:** Act LXVI of 1992 on the Records of Civilian Private Information and Addresses
- **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
- **Public Administration Act:** Act CXL of 2004 on the General Rules for Official Public Administration Procedures and Services, and its implementing regulations
- **Civil Code:** Act V of 2013 on the Civil Code
- Government Decree 45/2014 of 26 February on the detailed rules on agreements between consumers and companies
- **Information Act:** Act CXII of 2011 on Informational Self-Determination and Freedom of Information
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and
- Közigazgatási Gyökér Hitelesítés-Szolgáltató [Public Administrative Root Authentication Service Provider] Authentication Regulations,
- ISO 3166 English Country Names and Code Elements,
- FIPS PUB 140-2 (May 2001): “Security Requirements for Cryptographic Modules”
- RFC 5280 (previously RFC 3280) and RFC 6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3647 (previously RFC 2527) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - As regards regulation structure
- International Telecommunication Union X.509 “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”
- RFC 6960 Online Certificate Status Protocol (OCSP)
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust services providers issuing EU qualified certificates
- ETSI EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4 Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations
- ETSI EN 319 412-5 Certificate Profiles; Part 5: QCStatements
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles
- LCP: Lightweight Certificate Policy, OID: 0.4.0.2042.1.3
- NCP: Normalized Certificate Policy, OID: 0.4.0.2042.1.1
- NCP+ Extended Normalized Certificate Policy (Requiring the use of a cryptographic device), OID: 0.4.2042.1.2

- EVCP: Extended Validation Certificate Policy: Certificate Policy pertaining to the certificates for website authentication subject to extended validation, 0.4.0.2042.1.4
- IVCP: Individual Validation Certificate Policy for the website authentication certificates of natural persons, OID: 2.23.140.1.2.3
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record
- RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1
- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates

9.16. Miscellaneous provisions

9.16.1. Entire agreement

The Service Provider provides no merger clause.

9.16.2. Transferral

Any service providers included in the provision of services may only assign their rights and delegate their obligations to third parties if granted the Service Provider's preliminary written consent.

9.16.3. Partial invalidity

If any provisions of the present Statement 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 caused by partners or clients, the Service Provider may claim compensation and the reimbursement of attorneys' fees. 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 Practice Statement 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 Statement if the fault or delay was caused by an unforeseen circumstance outside its scope of inspection.

9.17. Miscellaneous provisions

The Service Provider's Registration and Certification Authorities perform their activities regarding the service subject to the present Statement and regulated by Chapters 3 and 4 independently and in their own competence.

The executive employee(s) of the Registration and Certification Authorities are independent of any business, financial, and other influences that can have a negative influence on trust in the services.