SERVICE PRACTICE STATEMENT FOR QUALIFIED TIMESTAMP SERVICE

Statement of NETLOCK Ltd. regarding the detailed requirements of procedure and operation applied in relation to the provision and using of the qualified timestamp service

NETLOCK Informatics and Network Security Services Limited Liability Company

Document name in Hungarian:	Szolgáltatási Szabályzat Minősített Időbélyeg-Szolgáltatásra
Document name in English:	Service Practice Statement for Qualified Timestamp Service
Document short name:	SPS-QT-HU
Version	260721~~18~~
Object identifier (OID):	1.3.6.1.4.1.3555.1.1.11.0.260721~~18~~
Date of approval:	21/07~~19/01~~/2026
Date of publication:	21/07~~19/01~~/2026
Valid from:	21/08~~18/02~~/2026
No. of pages:	73 pages, including cover
Approved by:	~~Koós Sándor Tamás~~Somkuti András Ákos CEO, NETLOCK Ltd.

TABLE OF CONTENT

1 INTRODUCUION

The present document is the statement of NETLOCK Informatics and Network Security Services Limited Liability Company (hereinafter: Service Provider or TSP) regarding the detailed requirements of procedure and operation applied in relation to the provision and using of the qualified trust timestamp service (hereinafter: Practice Statement or Statement).

The requirements specified in the present Practice Statement shall only apply to the qualified timestamps issued according to the certificate policies enlisted in Chapter 1.1 and set out in Chapter 1.2.1.

For the definitions and abbreviations see Chapter 1.6.

1.1 Overview

The qualified timestamp service of the Service Provider regulated by this document is the service specified in Chapter 1.1 of the Service Policy.

Based on the present Statement, the Service Provider issues qualified timestamps.

In addition to describing the detailed procedural and operational rules of the Service Provider, the present Statement also provides recommendations for the Relying Parties to verify the electronic timestamps created using the services.

1.1.1 Standards and requirements

The present Service Practice Statement was created in line with the structure of the NETLOCK *Service Policy for Qualified Timestamp 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 meet the requirements and recommendations of eIDAS, the Digital State and Services Act (hereinafter: Dáptv.) and the Decree of the Ministry of the Interior and makes use of the recommendations of standards ETSI EN 319401, ETSI EN 319421 and ETSI EN 319 422.

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

1.1.2 The Service Provider

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.
Registered site (Customer Service):	H-1143 Budapest, Hungária körút 17.
Company registration number:	01-09-563961
Tax ID:	12201521-2-42
Phone number:	(+36 1) 437 6655 (Application for certificate status change: Press 3)
Website:	netlock.hu
Statements and clauses published:	netlock.hu/aktualis-szabalyzatok (official Hungarian versions) netlock.hu/aktualis-szabalyzatok/#en (English translation)

Customer Service e-mail:	info@netlock.hu
For orders, document copies and agreements:	igenylesek@netlock.hu
NETLOCK Policy Adopting Authority email:	szee@netlock.hu
Customer Service / Business hours	At the place and within the time interval set out on the website of the Service Provider.

The Service Provider was registered on 19 March 2003 by the Trust Services Supervisory Authority (hereinafter: Supervisory Body) as a qualified Service Provider as defined by the Electronic Signatures Act[1]. Registration number: MH-1372-12/2003.

The registry of the services under the Electronic Signature Act maintained by the Trust Services Supervisory Body is available at http://webpub-ext.nmhh.hu/esign/.

This Service Practice Statement contains procedural and operational requirements concerning the rendering of qualified trust timestamp service complying with the provisions of eIDAS and the Dáptv. Service Provider has commenced the rendering of such service simultaneously with the entry into force of the first version of this Service Practice Statement (see 1.2.2), subject to the following terms:

- Prior to launching the qualified trust services hereunder, Service Provider had arranged for an external conformity assessment (see Chapter 8) and, pursuant to the Dáptv., it had reported to the Trust Service Supervisory Body its intention to take up the provision of trust services, providing the data stipulated in the form, i.e. – among other things – the name and registered office of the Service Provider.
- The Service Provider has submitted the Conformity Assessment Report, containing the result of the conformity assessment, to the Trust Service Supervisory Body.
- When reporting the service, the Service Provider submitted the approved public drafts of the Service Policy, the Service Practice Statement and the General Terms and Conditions, as well as the additional documents, instruments and declarations prescribed in Section 2(2) of Government Decree 470/2017 (XII. 28.), to the Trust Service Supervisory Body.
- Service Provider may launch the qualified trust service within the meaning of eIDAS, stipulated hereunder, as a qualified trust service provider after that
  - the Trust Service Supervisory Body has registered the Service Provider and its trust service in its register of qualified trust service providers and qualified trust services, specified in Dáptv., and
  - the "qualified" status of the trust service within the meaning of eIDAS has been added to the trusted lists (EUTSL) specified in Article 22(1) of eIDAS (see below the availability of the lists).

The qualified trust services hereunder have been reported to the Trust Service Supervisory Body simultaneously with the publication of this public draft Practice Statement as its first public draft version (see 1.2.2.). The Supervisory Body conducted an on-site inspection at the Service Provider.

The Service Provider received the resolution of the Trust Service Supervisory Body on the registration on 16 June 2017, according to which the Trust Service Supervisory Body registered the Service Provider under registration number EF/15066/3/2017 as a qualified trust service provider under eIDAS, rendering qualified electronic seal services and

[1] Act XXXV of 2001 on Electronic Signatures (no longer in force)

simultaneously with this added it to the EU trusted list (EU TL).

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

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

The Hungarian Trusted List maintained and published by the Supervisory Body is available at:

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

The list of Trusted Lists maintained and published by the European Commission is available at:

- in a machine processable (xml) format: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
- in a browsable and searchable format: https://webgate.ec.europa.eu/tl-browser

The "qualified" status of the listed services according to the eIDAS is indicated with the "TSA/QTST" value of "ServiceTypeIdentifier" and the "granted" value of "ServiceStatus".

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

Annual voluntary accreditations and other qualifications:

- The certification of the certificate creation service has taken place in accordance with the ETSI 319 401, ETSI 319 421 and ETSI 319 422 standards
- ISO 9001 standard
- ISO 27001 standard

See also Chapter 8.

In furtherance to the compliance with its respective statutory obligations, Service Provider shall pay particular attention to the non-discriminatory serving and equal treatment and shall ensure the equal access to services and information for Clients, the Relying Parties and the persons interested in its services. To this end, no prejudice or discrimination under no circumstances whatsoever, neither on grounds of business or personal relations, shall affect the serving and information of the Clients, Relying Parties and other interested persons contacting the Service Provider. For example, neither Service Provider, nor its employees shall differentiate between Clients, Relying Parties and the persons interested in the services of the Service Provider on grounds of sexual, racial, religious or political orientation or differences in economic size. Service Provider unconditionally requires all of its employees and partners to operate and provide the services in a non-discriminatory manner.

1.2 Document name and identification

For the name of the document and its OID, see the cover sheet (first page with the logo of Service Provider) in the lines of "Document name in Hungarian" and "Document name in English" and also in the "Object identifier (OID)" lines.

On the other pages, the English name of the document is displayed in the header and the OID in

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

the footer.

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 Ltd. – see Chapter 1.1.2 for its details.

1.2.1 Certificate Policies

The Service Provider indicates the OID identifiers specified in Chapter 1.2.1 of the Service Policy as standard Certificate Policy identifiers in the Policy field of timestamp replies.

Commercial name for NetLock timestamp service	Certificate Policy ID[3]	Description
Qualified Timestamp Service	BTSP	Standard eIDAS-compliant qualified timestamp service available under the terms and conditions published on the Service Provider's website.
Qualified Timestamp Service within the framework of NL Sign service	BTSP	Timestamp service available under the terms and conditions published on the website of the service in addition to a certificate requested within the framework of NL Sign service.
Qualified Timestamp Service within the framework of a service package	BTSP	Timestamp service available under the terms and conditions published on the website of the service package in addition to a certificate requested within the framework of a service package according to the GTC.
Qualified Timestamp Service with individual terms	identifier generated by the Service Provider	Timestamp service available under conditions and/or parameters different from those published on the website, based on an individual agreement.

If certain procedures contained in this Statement do not apply uniformly to all types of timestamp service applications, the document separates the different conditions based on the commercial names, also indicating the Certificate Policy identifier in parentheses.

1.2.2 Revisions of the Document

OID	Validity	Description of change	Prepared by
1.3.6.1.4.1.3555.1.63.20170301	version not yet in force	First non-public draft version of the uniform Service Practice Statement containing both	János Almási dr. Anett Barabás

[3] See: Service Policy 1.2.1

		qualified and non-qualified services	Viktor Varga Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20170427	version not yet in force	Deletion of provisions relating not to timestamp services from the draft version; clarifications and corrections regarding the timestamp service	Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20170515	version not yet in force	Version clarified and supplemented based on the observations made during the conformity assessment procedure carried out by MÁTRIX Auditing, Evaluating and Certification Ltd	Zoltán Szabó Viktor Varga
1.3.6.1.4.1.3555.1.63.20170615	19.06.2017–31.10.2017	Clarification of the concept of NL SIGN	dr. Anett Barabás
1.3.6.1.4.1.3555.1.63.201708904	version not yet in force	Amendment of the devices used by Service Provider	dr. Anett Barabás
1.3.6.1.4.1.3555.1.63.20171012	01.11.2017–24.05.2018	Supplementation and clarification of the previous version based on the findings of the Supervisory Body: - specifying the location where the EU list of SSCD- and QSCE-qualified devices can be accessed (1.1.2) - specifying the location where the conformity certificate of the applied devices can be accessed (6.2.1) Publication of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) registration number (9.4.1.)	Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20180416	24.05.2018–02.09.2018	*The public draft of the next version of the document includes the following changes:* • Abbreviation of the document title • Amendment of the cover sheet • Updating references to certain laws that have changed recently	Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20180727	version not yet in force	• Clarifications in Chapters 9.4 and 9.12 based on the findings reported by the conformity assessment body (MÁTRIX Ltd.) during the annual review • Clarification of certain definitions (1.6) • Other minor clarifications and corrections	Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20180817	03.09.2018–15.11.2019	Clarification of the previous draft version based on the findings of the Supervisory Body (affected Chapter: 4.1)	Zoltán Szabó
1.3.6.1.4.1.3555.1.63.20191015	16.11.2019–05.01.2020	Addition of rules related to code signing certificate service (4.2)	Zoltán Szabó Viktor Varga
1.3.6.1.4.1.3555.1.63.20191206	from 06/01/2020 until it is withdrawn or until a new version comes into force	Supplementation of the issuers of the qualified timestamp service with the top-level Root CA of the Service Provider (1.3.1)	Éva Varga-Szabó

1.3.6.1.4.1.3555.1.63.20210331	30.04.2021–14.08.2022	Inclusion of the Service Provider's registered site in Chapter 1.1.2 of the Statement	Éva Varga-Szabó
1.3.6.1.4.1.3555.1.1.11.0.220815	15.08.2022–30.06.2024	Updating the Service Provider's list of devices in Chapter 6.2.1 of the Statement 9.12.3: alteration of the document ID (OID)	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.240701	01.07.2024–14.08.2024	9.15: Update of the section on compliance with applicable laws and standards	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.240815	15.08.2024–31.08.2024	5.2.1: Clarification of trusted roles Supplementation of Chapter 8.4 Clarification of the name of the Statement: 5; 5.1; 5.1.6; 5.2.4; 5.3; 5.4.1; 5.5.8; 5.7.1; 6.2.2; 6.2.8; 6.2.9; 6.5; 6.7	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.240829	01.09.2024–12.01.2025	Further updates due to legal changes: 1.1.1; 1.1.2; 1.6.1; 1.6.2; 9.2.1; 9.3.3; 9.15	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.250113	from 13/01/2025 until 16/05/2025	Supplementation of intermediate CAs listed in point 1.3.1 of the Statement	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.250517	from 17/05/2025 until 17/02/2026	Update section 6.2.1	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.260218	from 18/02/2026 until ~~it is withdrawn or until a new version comes into force~~20/08/2026	Delete postal address (1.1.2)	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.11.0.260821	from 21/08/2026 until it is withdrawn or until a new version comes into force	• Addition to section 1.3.1 of the regulations	NETLOCK Compliance

formázott: Betűtípus: 9 pt,

formázott: Listaszerű bekezdés;Listaszerű bekezdés 1, Behúzás: Bal: 0,05 cm, Függő: 0,25 cm, Felsorolás + Szint: 1 + Igazítás: 0,95 cm + Behúzás: 1,58 cm

1.3 PKI participants

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

1.3.1 The Service Provider

The Service Provider provides timestamps for electronic signatures, electronic seals, timestamps within the framework of the trust qualified timestamp service.

CAs of the qualified timestamp service:

CA name	Certificate availability	CRL availability
Arany (Class Gold) Főtanúsítvány	www.netlock.hu/index.cgi?ca=gold	www.netlock.hu/index.cgi?crl=gold
NetLock Minősített Eat. (Class Q) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cqlca	www.netlock.hu/index.cgi?crl=cqlca
NETLOCK Trust Qualified TSA RSA 4096 CA	http://aia.rsa.netlock.hu/index.cgi?ca=qtsarsa4096ca	http://crl.rsa.netlock.hu/index.cgi?crl=qtsarsa4096ca
NETLOCK Trust Qualified TSA ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=tsaeccca	http://crl.ecc.netlock.hu/index.cgi?crl=tsaeccca
NETLOCK Trust Qualified TSA ECC CA 2025	http://aia.rsa.netlock.hu/index.cgi?ca=qtrusttsaeccca2025	http://crl.rsa.netlock.hu/index.cgi?crl= qtrusttsaeccca2025
NETLOCK Trust TSA ECC CA 2025	http://aia.rsa.netlock.hu/index.cgi?ca= trusttsaeccca2025	http://crl.rsa.netlock.hu/index.cgi?crl= trusttsaeccca2025

formázott: Középre zárt

Certificates authenticating timestamp replies issued within the framework of the qualified timestamp service can be downloaded from the Service Provider's public certificate repository.

More information and other CAs can be found on the website of the Service Provider.[4]

1.3.2 Registration Authority

Not applicable.

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.

1.3.4 Relying Parties

The Relying Parties are typically not in contractual relationship with the Service Provider, but the Service Practice Statement for Qualified Timestamp Service may provide them with recommendations.

See Chapter 1.6.1. of the Trust Service Policy.

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

1.3.5 Other participants

Not applicable.

1.4 Certificate usage

A certificate issued for timestamping can only be used for timestamping.

1.5 Statement administration

The issuance and maintenance of the present Trusted Service Practice Statement shall be carried out by the Policy Adopting Authority of the Service Provider.

The permanent members of the Policy Adopting Authority are those employees of the Service Provider, who are designated as such by the Management of the Service Provider. The operation of the Authority is regulated by the internal, non-public rules of operation of the Policy Adopting Authority.

1.5.1 Organisation responsible for the administration of the document

The name of the organizational unit of the Service Provider that is responsible for the policies (terms) is NETLOCK Policy Adopting Authority. The permanent members of the Policy Adopting Authority 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.

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 sheet 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 accordance with the provisions of the unit's regulations.

In the course of processing the query, the Authority or the member shall identify the section(s) of the document affected by the comment, question and then shall respond to the sender in e-mail

upon consulting with other members of the Authority, and with other employees of the Service Provider, if necessary.

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

1.5.3 The organization responsible for the compliance of the present Practice Statement with the Service Policy

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

The Statement 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 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 Service Policy even after the modification, he/she shall approve the 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 and 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.
Activation Data	A code sequence generated by the Service Provider or submitted by the End User, which is known exclusively by the End User (password, PIN code), which makes the private key ready for use. The activation data is not related to certificate issuance.
Signature	See electronic signature.
Signature / Seal Creation Device	A cryptographic device, which is not capable of creating qualified signature / seal (see 1.6.2. Abbreviations, SCD).
Signature Service	The following services under eIDAS: • creation, verification and validation of electronic signatures and electronic seals, • as well as verification and validation of the related certificates.

	Within the framework of the present Practice Statement, it means the "cloud-based" provision of the above services, which encompass the storage of end user signature and seal keys by the Service Provider and signing/stamping of the documents uploaded by the Clients via the web-based interface/protocol (including, optionally, the timestamping of the document), as well as their verification.
Signature Partner	A partner of Service Provider, who provides signature service for its own clients, a part of which Signature Partner may participate in the validation of the identity of the End Users (in relation to whom Signature Partner has limited information and administration rights), and who uses the signature service for the provision of service in integration with its proprietary service, and who, as Subscriber, undertakes to pay the fees payable after the end users.
Subject	See the definition in the Dáptv. Within the framework of the present Practice Statement, Subject means the Subject and SAN fields of the certificate, as well as the data set out in the above fields, which may refer to a natural person and/or an entity and/or a trademark/product name and/or the ID/other name of a device/system or a pseudonym. See the Applicant, Subscriber, Client and End User entities.
Status Change	The procedure resulting that the status of the certificate (valid, suspended) changes and acquires a new value (valid, suspended, withdrawn).
Archiving Service	A service for long term storage of electronic documents. An electronic archiving service provided by a qualified trust service provider that meets the requirements set out in Article 45j of eIDAS. Within the framework of this Statement, it refers to a qualified trust service where the Trust Service Provider creates or supplements the entire certificate chain of the electronically signed or sealed documents submitted to it for the purposes of archiving, provides an archiving timestamp to the certificate chain, and then securely stores the document or file so created or completed. If an electronic document bearing an electronic signature or seal is archived by a Qualified Trust Service Provider, the electronic signature, seal or timestamp affixed to the electronic document and the associated certificate shall be presumed to have been valid at the time the signature, seal or timestamp was added, unless proven otherwise.
Recipient	The person receiving any key or device of the end user (e.g. Client Device) and the activation data thereof (in person, or by way of postal or electronic delivery). The Applicant in respect of the subject certificate may act as Recipient.
Seal	See electronic seal.
Trusted List	A list managed by the Trust Services Authority or a software producer, which contains the identifiers (typically certificates) of the trust services considered reliable. A software that manages a trusted list accepts the signatures, seals and timestamps that can be traced back to the services set out in the trusted list. It typically means the EU trusted list, where the services – whether non-qualified or qualified under eIDAS – are enlisted by the supervisory authorities of the Member States. See: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers.
Trust Service Policy	NETLOCK Trust Service Policy for Qualified Certificate Service.
Trust Service Supervisory Body	The authority designated in the Dáptv. for the supervision of trust services. Specifically, it is the National Media and Infocommunications Authority.

Trusted Role	The managerial position that entails general liability for the IT system of the Service Provider. See Chapter 5.2.1 Trusted roles.
Trusted Employee	The person in trusted role at the Service Provider or its Service Provider Partner.
Trust Service	According to Section 16 of Article 3 of eIDAS: "an electronic service normally provided for remuneration which consists of: - the creation, verification and validation of electronic signatures, electronic seals or electronic timestamps, electronic registered delivery services and certificates related to those services; or - the creation, verification and validation of certificates for website authentication; or the retention of electronic signatures, seals or certificates related to those services." Within the framework of the present Statement, trust service means the service of the Service Provider related to electronic signatures, electronic seals and website authentication, that provides the issuance and lifecycle management of the certificates, as well as the timestamp service of the Service Provider.
Security Zone	A (logically or physically) protected area, which safeguards the confidentiality, integrity and accessibility of the systems used by the Service Provider.
CAA Verification	A verification, whereby the Service Provider searches for CAA records under RFC 6844 in the DNS record. If these fields contain a record suggesting that the domain owner liaises with another Service Provider, the certificate shall not be issued.
E-akta (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
EV Certificate Extended Validation Certificate (EVC)	A website validation certificate compliant with the requirements of EVCG.
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (Section 10 of Article 3 of eIDAS). Within the framework of the present Statement: Electronic data created by the natural person with the private key pair of the signature certificate issued by the Service Provider, which is attached to the electronic document (or other electronic data) to be signed, and which can be verified with the certificate and the public key contained therein.
Electronic Seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (eIDAS Article 3, Section 25). Within the framework of the present Statement: The seal certificate issued by the Service Provider with its private key pair are electronic data created by a legal person, which is attached to the electronic document (or other electronic data) to be sealed, and which can be verified with the certificate and the public key stored therein. The counterpart of electronic signature which is created by a legal person.
Subscriber	A contractual partner of Service Provider, who undertakes the payment of the service fees. The rights and obligations of Subscriber are set out separately in the GTC and in the Service Agreement.

	In the case of certification service, in case an organization is also specified as the Subject of the certificate or only a natural person is named, then the Subscriber is typically identical to the Subject. In the case of NLK Sign service, the Subscriber is identical to the Signature Partner or the End User. See also the Client, Applicant and End User entities, as well as Chapter 1.3.3 Subscriber, End User and Applicant.
Relying Party	A natural or legal person, who is not in contractual relationship with the Service Provider but uses any – typically free of charge – certification status service of Service Provider (e.g. verifies electronic signature, seal or timestamp and in relation to this verifies the validity information of specific certificates or the policies of the Service Provider). See Chapter 1.3.4 Relying party.
Valid Certificate	A certificate with a term of validity that includes the actual time and date, and the status of which is not suspended or revoked (see Certificate Status).
Term of Validity	A term between a commencement and end date, in respect of which the certificate has been issued.
Certificate for Device	A certificate with a private key that is issued for a Cryptographic Device.
Chain of Validity	The electronic document or the hash thereof and the series of linkable information (in particular, the certificates, certificate-related information, the data used for the creation of the signature or seal, information pertaining to the actual status, revocation of the certificate, as well as information pertaining to the validity data of the Service Provider, as well as the revocation thereof), which serve for establishing as to whether the advanced or qualified electronic signature, seal or timestamp placed on an electronic document was valid upon the date of its placement on the subject electronic document. In a more general sense, it means the hierarch of certificates certifying each other up to the root certificate.
Advanced Electronic Signature	An electronic signature which meets the requirements set out in Article 26 of eIDAS.
Advanced Electronic Seal	An electronic seal, which meets the requirements set out in Article 36 eIDAS.
Certificate Policy	According to the Dáptv.: a trust service policy, which pertains to certificates issued within the framework of trust service. Within the framework of the policies of the Service Provider, it means a standardized code of procedure, under which the Service Provider issues and manages certificates. The policies of Service Provider include more certificate policies, differentiating the applicable requirements and procedures.
Certification Authority	The organizational unit of Service Provider, which, based on the request of the Registration Authority, carries out the issuance, publishing, revocation, and suspension of certificates, as well as the publishing of the Certificate Revocation List. See Chapter 1.3.1.
Certification Administrator	Within the Certification Authority, the Certification Administrators approve the issuance of certificates.
Accessing Party	A Relying Party having free of charge access to specific functions of the service as regards documents specified by the Subscriber as initiated by the Subscriber of the archiving service.

	See Chapter 1.3.4 Relying party.
Applicant	In the case of certification service, it means the natural person who acts in the certification management and status change procedure, and approves the service agreement on behalf of the Client. The Applicant may be: ● the natural person specified as the Subject of the certificate (the applicant for the alias, in the case of an alias); ● in the lack of the above, the representative or agent of the organization specified as the Subject of the certificate; ● in the lack of the above, the proprietor of the domain name, trademark, or product name specified as the Subject of the certificate, or in case the proprietor is an organization, the Applicant shall mean the representative or agent thereof, or the person having control over the domain name. The Applicant shall be identical to the Subscriber in case a natural person is specified as the Subject of the certificate (and organization type). In the case of NL Sign service, the Applicant shall be identical to the End User. In the case of archiving and timestamp service, the Applicant shall be identical to the Subscriber.
Timestamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Timestamp Server	The technical system of Service Provider that issues timestamps.
Timestamp Service	The service of Service Provider that issues a timestamp on the basis of the hash of the data in electronic format sent to the Timestamp Service.
Timestamp URL	A virtual token that provides access to the timestamp service and contains the unique identifier of the Subscriber, through which the End User may forward timestamp requests to the Service Provider and Service Provider forwards timestamp replies to End User on the basis of the requests.
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 be identical to the Registration Agent.
Public Root Provider (KGyHSz)	Public Administration Root Authentication Service Provider See 1.3.5 and http://www.kgyhsz.gov.hu/
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.
Initial suspension	A special case of certificate suspension when the Service Provider suspends the certificate immediately upon issuance, thus preserving it from the abuse for the period of time that the certificate and the private key pass securely to the Customer.
Right of representation	Fully or partial right of representation or any other right that could be interpreted so (see Dáptv.).
CA	Service Provider's technical system issuing certificate. Service Provider has intermediate CAs issuing the end user and some providers' certificates, as well Service Provider has a top-level rootCA issuing the intermediate CAs. CAs are organized hierarchically.
External Certification	A Certification Authority, that is operated by a sovereign organization or person,

Authority	independent of the Service Provider (as a service partner) according to the regulation of Service Provider.
External Registration Authority	A Registration Authority, that is operated by a sovereign organization or person, independent of the Service Provider (as a service partner) according to the regulation of Service Provider.
Terms (and Conditions)	Documents of the Service Provider which describe the manner in which the services are provided and what the expectations are and what the other parties are responsible for. This includes collectively the Provider's following documents: Extract of the Service Practice Statement, Certificate Policy, Service Practice Statement, GTC, Service Agreement and other agreements concluded between them.
Chryptographic device	Secure hardware device, which stores the private key of end user, saves that against compromising, makes cryptographic operations (ex. encryption, signing) for the user. It may be SCD or QSCD, HSM or any other non-signature device. It may be handled both by the Service Provider or Client. In the latter case, it is referred to as "Client Device".
Critical Services	Service Provider's services which are related to certificate issuance, key generation, providing devices and certificate status service.
Re-key	The process when Service Provider issues a new certificate and private key for a former registered Client (or itself) based on the Client's (or it's own) former existing certificate. In the new certificate, end user's public key also changes. See Chapter 4.7.
Key escrow service	A service which protects end-user's private key and make it available for end user (in the case of losing, destroying or becoming for any other reason useless of the private key).
Private key	One of the keys of the key pair, generated by the Service Provider or Client, that is managed by the End User. See also Public key. If the public key is placed in a signature or seal certificate, the private key conforms to the definition of electronic signature/seal creation data of eIDAS.
Qualified Signature / Seal Creation Device	A cryptographic device, which is capable of creating qualified signature or seal (see also 1.6.2 Abbreviations, QSCD).
Qualified Certificate	A certificate issued by a qualified trust service provider that conforms to Annex I, II or IV of eIDAS or to directive 1999/93/EC, depending on which was in force when the certificate was issued.
Qualified website authenticating certificate	In accordance with eIDAS Article 3., point (39): "a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV". A qualified certificate that with the authentication of the included websites assures the visitors of this sites that behind the sites there is an existing and legitim organization.
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.

NL Sign service	Secure centralized key storage (managed SCD) and key management service, which enables electronic signature or seal (and timestamp) of documents uploaded through web interface. The certificates usable in the frame of NETLOCK Sign service and the required registration, as well as using the certificate after issuance, are available on the own web interfaces of NETLOCK Sign service.
Public key	One of the keys of the key pair, generated by the Service Provider or Client, that is placed in the certificate created by the Service Provider. See Private key.
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, followed by 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. If used, it is entered in the certificate's Subject/SerialNumber field.
Registration	Initial registration process that is performed by the Service Provider to identify Applicant and Subscriber, as well as to establish their procedural right and record their data.
Registration Authority	Service Provider's organizational unit which performs processing the service application, registration of Applicant and Subscriber, as well as in case of certification service verification of the data indicated in certificate. It may operate both within (as inner organizational unit) or outside of the Service Provider's organization (as External Registration Authority).
Registration Officer	Trusted Role. See Chapter 5.2.1 Trusted Roles.
Registration Agent	A partner of the Service Provider (or its employee) who, on behalf of the Service Provider, performs personal identification tasks related to certificate issuance at the Applicant's location.
Registration (and Revocation) Administrator	These employees within the Registration Authority are responsible for managing certificate applications and verifying the veracity of the data provided in the certificate application (see Chapter 4.2.1), as well as managing and executing revocation requests (see Chapter 4.9).
SSL certificate	Certificate for website authentication.
Statements	The present Practice Statement and the relevant Service Policy collectively.
Organization	Regarding the Subject or Subscriber of certificate: legal person, self-employed or private lawyer.
Software certificate	A certificate where the private key is not issued on a cryptographic device.
Service	In the frame of present Statement, the Service Provider's trust services (see Chapter 1.1).
Service Practice Statement, Statement	The statement of the trust service provider about the requirements and conditions of the detailed procedural or other operational requirements (see Dáptv.) which

	includes the detailed procedural and other operational rules related to the Service Provider's activities.
Service Agreement	An agreement concluded between the Service Provider and the Client, which contains the terms and conditions for the provision and use of the service. Its conclusion is a prerequisite for the use of the service.
Service Provider	NETLOCK Ltd. that provides trust services according to the present Statement.
Service Provider's Regulations	Trust Service Policy, Trust Service Practice Statement, GTC, Service Agreement, Extract of the Service Practice Statement. Furthermore, other non-public regulating documents.
Service Partner	Natural or legal person, independent of the Service Provider, who participates in providing services under the agreement with the Service Provider.
Service Provider's systems	All systems of the Service Provider together that are providing the services.
Service Provider Certificate	Service Provider's certificates, used for provision of services (e.g. certificates of CAs and timestamp servers).
Certificate	An authentic verification, issued by the Service Provider, that links the public key to the Subject and verifies the authentication of data published in certificate.
Certificate Activation	Status change procedure that restores validity of a suspended certificate. After activation the certificate will be valid again retrospectively, so also for the interval of suspension as if suspension would not have happened.
Certificate status	The valid, revoked or suspended status of certificates that is registered by the Service Provider during the validity period of certificate. Service Provider informs the Clients and Relying Parties about the status of certificates via the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP).
Online Certificate Status Protocol (OCSP)	A service that provides real time information about a given certificate's status to the Relying Parties. See also: Certificate Revocation List.
Certificate suspension	Status change procedure during which the Service Provider temporarily makes a valid certificate invalid before the expiry of the original validity period. The certificate suspension is a temporary status, during the original validity period the suspended certificate can be revoked or made valid again. After cancellation of suspension the certificate will be valid again retrospectively as if suspension would not have happened.
Certificate application	A process when Applicant requests a certificate, i.e. submits and proves data needed for creating a certificate, then finally verifies his/her claim for the given certificate by signing the Service Agreement (and making also the Subscriber sign it, if not identical to the Applicant) and thus authorizes the Service Provider to issue the certificate requested.
Certificate Management Process	A process that results issuing a new certificate based on an existing certificate and a former client registration (see Chapters 3.3. Identification and authentication for managing certificates and 4. Certificate lifecycle requirements).
Certificate Service	Service within the framework of which the Service Provider creates a new certificate. The issuance may take place based on an already existing certificate (subsequent issuance through Certificate Management Process) or also without such antecedent

	(original issuance).
Certificate Renewal	A process when the Service Provider issues a new certificate with unchanged Subject data for an already existing public for a new validity period. See Chapter 4.6.
Certificate Modification	A process when the Service Provider issues a new certificate for an already registered Applicant based on his/her former certificate for the same public key but with changed Subject or Service Provider data. See Chapter 4.8.
Certificate Repository	The Service Provider's register that includes issued certificates. Public certificates and Certificate Revocation Lists issued by the Service Provider are queryable from this repository.
Certificate Type	Distinguishing the various certificates issued by the service provider according to some characteristics, mainly based on the purpose of use. See Practice Statement, Chapter 1.2.1.
Certificate Revocation	Status change procedure during which the Service Provider makes a valid certificate invalid before the expiry of the original validity period. The certificate revocation is an irreversible and definitive status change, the revoked certificate becomes invalid immediately in the moment of revocation and it will never be valid again.
Certificate Revocation List (CRL)	An authentic list of permanently and temporarily invalid certificates, published in the Certificate Repository by the Service Provider periodically or due to status changes. Acceptance and use of certificates listed in the CRL is not recommended. It is a kind of the revocation registry defined by Section 17 of the Decree of the Ministry of the Interior (24/2016).
Test certificate	Certificate issued by the Service Provider for testing. The content of a test certificate is the same as that of a real authentic certificate, but the Certificate Policy field and the name of the Subject indicate the test character of usage. Such certificates must not be used for commitment and do not have legal effect. They may be accepted exclusively for testing purpose. The Service Provider does not assume responsibility for the included data and usage of test certificates and for the availability level of services related the certificate.
UCC Certificate for Website Authentication	A certificate for website authentication that includes several 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 username and password (following registration in the Client Menu). Registration and login in the qualified Client Menu are 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 username and password.
Client	Party who contracts with the Service Provider. In the case of certificate service, it is the Applicant and Subscriber of the certificate (where appropriate, these actors are the same). In the case of NL Sign service, it is the Signature Partner and the End User.

	See also Chapter 1.3.3 Subscriber, End User and Applicant.
Client Device	See Chryptographic device.
Client Registration	Identification of natural or legal persons, validation and recording their data, before signing the Service Agreement and issuing a certificate. See Chapter 3.2 Initial identity validation.
End User	Natural person who disposes of the private key counterpart of certificate's public key (uses it exclusively or is responsible for it). In the case of NL Sign service, it is the person who performs signing or sealing operation within the framework of signature service by activating his/her private key. See also the Client and Subscriber entities, as well as Chapter 1.3.3 Subscriber, End User and Applicant.
End User Certificate, End User Key	It represents the Subscriber's certificate and key, distinguished from the Service Provider's own certificates and keys.
Certificate for Website Authentication	Certificate as defined in Article 3 point 38 of eIDAS regulation.
Wildcard Certificate for Website Authentication	Certificate for website authentication issued by the Service Provider for certifying several subdomains (domain name is displayed in the form of *.domain.com, so it includes all subdomains of domain.com).

1.6.2 Abbreviations

Abbreviations of the laws and regulations referred to herein

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.
Dáptv.	Act CIII of 2023 on the digital state and certain rules for the provision of digital services.
Nytv.	Act LXVI of 1992 on keeping records on the personal data and address of citizens.
Szmtv.	Act I of 2007 on the entry and residence of persons with the right of free movement and residence.
Harmtv.	Act II of 2007 on the entry and residence of third-country nationals.
Infotv.	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

24/2016 BM	Decree of the Ministry of Interior 24/2016 of 30 June on the detailed requirements concerning trust services and their providers

Abbreviations for technical terms

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority Issuer
CAA	Certification Authority Authorization Trust Service Provider Authorization
IP	Internet Protocol
IT	Information Technology
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy
CPS	Certification 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 (not certified)
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider
QSCD formerly SSCD	Qualified Signature / Seal Creation Device
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

See also Chapter 9.15.

2 PUBLICATION

2.1 Repositories

Service Provider shall publish its terms and conditions and policies in PDF format on his website. Here, in addition to the current versions of the documents, their previously valid versions and public drafts of future versions can also be found.

2.2 Publication of certification information

The Service Provider is obliged to publish the Service Provider's certificates used for the provision of the timestamp service in accordance with the provisions of the Terms and Conditions, as well as to create and keep the Certificate Repository up to date.

The Terms and Conditions must be published with the content and structure according to RFC 3647.

2.3 Time and frequency of publication

New versions of this Statement will be published in accordance with the procedures described in Chapter 9.12. For the publication of new versions of the Trust Service Policy, see Chapter 9.12.

Other policies and contractual terms of the Service Provider, as well as their new versions will be issued as necessary.

The Service Provider will publish extraordinary information – when necessary – in accordance with legal requirements, or without delay in the absence thereof.

The certificates of the Timestamp Issuers will be published at the latest upon the start of the service.

2.4 Access controls on repositories

Not applicable.

3 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

In the case of timestamp service, the Service Provider requires the Client to register and uses various registers to verify subscriber and contract data.

Registered Clients are identified based on username and password, or by means of a unique customer identifier (timestamp URL).

4 LIFE CYCLE REQUIREMENTS

This Chapter 4 and its sections contain a description of the procedures related to the provision of the timestamp service provided by the Service Provider, the application for the service, the conclusion of the Service Agreement, as well as the Service Provider activities to be performed during the term of the contract and the operations that can be performed by the Client.

4.1 Application for the service

Timestamp service can be applied for as follows:

- by filling out the order form that can be downloaded from the Service Provider's website and sending it to the Service Provider's email address;
- within the framework of a service package, by filling out the service package's web order form and sending it to the Service Provider;
- within the framework of NL Sign service, by submitting an application in the system of the service (timestamp option is integrated in the NL Sign service).

Before concluding the Service Agreement, the Service Provider shall fully inform the Applicant about the qualified nature of the service, the exact contractual terms and conditions for the use of the service, including any restrictions on use, the terms and conditions related to the use of timestamps, as well as the related laws.
The Service Provider shall publish its policies and other information documents on its website in non-editable PDF format and shall also provide information directly through the content displayed on the website.
No later than after concluding the agreement, the Service Provider shall make the Service Agreement, the Service Policy and the Service Practice Statement available to the Customer via link(s) inserted in an electronic mail.

4.2 Provision of the service

After concluding the Service Agreement, the Service Provider must provide the End User with unique access to the Timestamp Server.
After concluding the agreement, the Service Provider must also provide the Client with the Service Practice Statement and the Service Agreement, prepared on the basis of the Service Policy, on a durable data medium.
When receiving timestamp requests, the Service Provider must identify the sender of the timestamp request in accordance with the provisions of the Service Practice Statement. During the life cycle of the Service Agreement, the Service Provider has the right – in the cases specified in the Terms and Conditions, in particular in the case of breach of contract – to restrict or suspend the service.

The Service Provider provides the timestamp service continuously (24/7) as follows:

- ensures 99.9% availability on an annual level;
- guarantees that the duration of service outages will not exceed 3 hours per occasion.

The timestamp service is available to the Clients without restrictions; however, in case of excessive use, requests may be limited for service protection reasons if a certain limit is exceeded. The terms of the restrictions are published on the Service Provider's website.

End Users shall send the timestamp requests to their own unique URL.

Restrictions on timestamp service related to code signing

In the case of timestamp service provided in addition to code signing certificates, the Service Provider ensures compliance with the relevant CSBR regulations (see Service Policy Statement for Non eIDAS Certificate Services). Therefore, in the case of timestamp service provided in addition to code signing certificates, the Service Provider uses exclusively timestamp certificates with a maximum validity period of 135 months and replaces these timestamp certificates with a new certificate with a new key at least every 15 months.

4.3 Termination of the Service Agreement

Before the termination of the Service Agreement, the Service Provider shall warn the Subscriber of the consequences of the termination and then suspend the use of the unique URL of the timestamp.

4.4 Timestamp status checking requirement for Relying Parties

A timestamp may be checked by checking the signature of the timestamp, then by checking the timestamp certificate in accordance with Chapter *4.9.6 Certificate status checking requirement for Relying Parties* of *Service Practice Statement for Qualified Certificate Services*.

5 PHYSICAL, PROCEDURAL AND PERSONAL SAFETY 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 non-public Information Security Regulations include the requirements pertaining to information security rules.

The Service Provider reviews the Information 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 room). 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 Information 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 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 uniformly in the computer room. It is difficult for unauthorized persons to access the computer room; however, security guards can quickly approach it in the event of an alarm. The security perimeter has no windows, and apart from the entrance door, the only way to enter is by breaking down the particularly strong wall. 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 can be found in the server vault of a protected computer room, the security level of which is the same as that of the site.

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. In addition to physical and electronic logging of the entries, access to the computer room takes place with a personalized electronic card. Within the computer room, the Service Provider's systems have been installed in a separate area that can be accessed after biometric identification. Round-the clock video surveillance system is also set up for both the entrance area of the security zone and the computer room itself.

The access control system of the secondary location does not have biometric identification, but to maintain consistency, the secondary location is also secured by permanent manned security. Authorized employees can enter the server room after card identification; entry and exit are continuously logged. Round-the clock video surveillance system is also set up 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.

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 (makes it use) 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 Risk of water exposures and flooding

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 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 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 following shall be regarded as trusted roles:

- Manager generally responsible for IT system;
- Security Officer: person generally responsible for the security of the service;
- System Administrator: person in charge of installing, configuring, maintaining the Service Provider's IT system;
- System Operator: person responsible for the continuous operation, saving and restoration of the Service Provider's IT system;
- Independent System Auditor: person responsible for auditing the Service Provider's logged and archived data files, monitoring compliance with the control measures implemented by the Service Provider in order to ensure proper functioning, continuous auditing and monitoring of existing procedures;
- Registration Officer: person responsible for approving the production, issue, revocation and suspension of certificates.

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

[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

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 with the exclusion of the presence of any other persons:

- generating of Service Provider's key pairs;
- saving and restoring Service Provider's private keys;
- destroying Service Provider's 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.

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 Operators.

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's Information 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 Information 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.

Employees working in the area of customer registration are 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, Registration Officers 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 know-how required for performing their tasks. In the interest of ensuring this know-how, 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 systems 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.

In the case of the timestamp service, the Service Provider logs the events specified in the Trust Service Policy.

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.

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 Information 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 to the timestamp service, disclosure, modification, destruction of data stored in connection with the provision of the service or other abuse. 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 timestamps 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 timestamps it issues – including personal information. In accordance with the above, the following are archived:

- data provided by the Applicant and the Subscriber during application for the service (see Chapter 4.1);
- 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 3), as well as data retrieved from registers;
- 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 timestamps for at least ten years following the expiration date of the certificate authenticating the timestamp as defined by the certificate, or until the legal dispute regarding the verification of the timestamp 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 timestamps.

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 Registration Officers 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

The requirements for log file collection specified in Chapter 5.4.6 apply to archive collection.

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 Information Security Regulations contain the detailed provisions applicable to archiving.

5.6 Key changeover

The Service Provider will replace the timestamp keys at the required time, preferably out of service, in an appropriate manner (by renewal or issuing a certificate for a new key).

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.

The Service Provider informs the Supervisory Body, the other involved bodies (if applicable), and the Clients of the service that are negatively affected, immediately, but no later than within 24 (twenty-four) hours, of any violations of the security of the Service Provider's systems or if the integrity of the data becomes compromised, if such has a significant effect on the services or the stored personal data (incident).

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 Information 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 so-called 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 subject 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. Service Provider disagrees with the vulnerability scoring defined by the CVSS;
    b. the vulnerability was misidentified;
    c. the vulnerability could not 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

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

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 enhanced security to minimize the chance of hardware and software errors or data corruption. The ability to restore the Service Provider's 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.

5.7.3 Entity private key compromise procedures

If the Service Provider's key is compromised, the Service Provider shall at least:

- inform its Clients, Service Partners, the Relying Parties, and the Supervisory Body;
- indicate that the operations performed with the affected Service Provider key are no longer valid; and
- revoke the affected Service Provider certificate.

If any of the algorithms (or any related parameters) used by the Service Provider do not meet the requirements for the entire period of the planned term of use, the Service Provider is obliged to:

- inform its Clients, Service Partners, the Relying Parties, and the Supervisory Body; and
- revoke the affected Service Provider certificate.

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 Service Provider's private keys or other authenticating data are compromised or if any critical elements of the Service Provider 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. If the duration of the extraordinary operating event exceeds the period of time set forth in Articles 36 and 45 of the Decree of the Ministry of the Interior, the qualified service provider informs the Supervisory Body without delay, including the provision of the following information pertaining to the event:

- the start of the extraordinary operating event, a description of the event, and, if different, the time it was discovered;
- the effects of the extraordinary operating event (which include, in the case of a security

event, a description of the effected services, IT components, and personal data, as well as the number of effected trust service clients);
- the expected duration of the extraordinary operating event;
- the measures taken and planned in the interest of preventing the extraordinary operating event in the future; and
- the end of the extraordinary operating event.

The Disaster Recovery Plan of the Service Provider addresses the case of compromise of the timestamp private key and loss of clock synchronization, which may also affect already issued timestamps.

In the event of such and other cases of compromise or suspicion thereof, the Service Provider

- informs all Subscribers and Affected Parties;
- suspends the issuance of timestamps until normal operations are restored;
- identifies the timestamps affected by the compromise and discloses the information necessary for their identification to Subscribers and Affected Parties, taking into account data protection considerations.

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 service within 5 workdays.

5.8 Termination of the service

If the Service Provider terminates or suspends for an extended period all or part of its activity in a planned manner, prior to ceasing the activity it shall execute at least the following procedures:

- 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, and shall inform the Supervisory Body of the above termination. In the notification the Service Provider shall indicate the organization – with classification identical to those of the Service Provider – which will take over the services, as well as the obligations to maintain the registration information and event log archives until the termination of the provision of the service at the latest for the term prescribed for, or undertaken by, the Service Provider.
- Service Provider shall destroy its own private keys and revoke the corresponding certificates and shall publish information to this effect on its website.
- In case only trust service is terminated, then Service Provider shall continue to provide the related 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.

- 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, signature verification data, 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.

If liquidation or winding up proceedings have been initiated against the Service Provider on the basis of a final court decision, the Service Provider will immediately inform the Supervisory Body of this fact and will name the body conducting the proceedings.

With a view to transferring its data to another service provider, Service Provider shall copy those data on a media and in a format acceptable for the recipient service provider or ensure that the recipient service provider can process the data in their original format, for the purpose of which it shall transfer the appropriate devices, documentations and knowledge.

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.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Service Provider generates its own timestamp key pairs in a physically protected server room in the joint presence of at least two trusted employees; a report is drawn up of the process.

When generating and storing its own timestamp keys, the Service Provider shall proceed in accordance with Chapter 6.2.1. The Service Provider shall generate all of its own key pairs itself and shall verify whether the public key has not previously been allocated to another entity.

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 Service Provider's 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 Service Provider's keys, the Service Provider will generate the new CA keys and issue the new Service Provider's 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.

If the same timestamp key is used in more than one cryptographic module, the Service Provider shall attach the same certificate to it.

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

6.1.2 Private key delivery to End User

The private key is generated in a cryptographic device, this point of RFC 3467 is not applicable in the case of timestamp service.

6.1.3 Public key delivery to certificate issuer

After generating the key pair for the archiving system, a certificate request is created. This request contains the public key. The request is submitted to the qualified certificate issuing system and the certificate is issued based on this.

6.1.4 Publication of timestamp public key

The Service Provider's own timestamp certificates are available on the Service Provider's website (Chapter 1.1.2) in accordance with Chapter 2. The availability of issuers of certificates authenticating timestamps is also indicated in the AIA:CAIssuer field of the certificate as standard.

The public keys of the Service Provider's certificates authenticating timestamps are accessible as part of the certificates.

The Timestamp Server does not issue timestamps before its certificate has been loaded into the cryptographic unit and the certificate has been fully verified.

6.1.5 Key sizes

The key pairs used by the Service Provider (for both Service Provider's 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) } – at least 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)

The timestamp key can only be used to sign timestamp replies.

6.2 Private key protection and cryptographic module engineering controls

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

The Service Provider stores the timestamp private keys in a secure manner that prevents access

and use by unauthorised persons. The Service Provider stores its own private keys used for the creation of certificates, the authentication of timestamp replies and 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 its own keys (also including timestamp 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 qualified trust services, in which they are classified according to security.
Before the qualified service provider uses its products that implement trust services used to provide a qualified service for any other purposes besides its own provision of services, it ascertains that the product does not contain any data linked to a trust service and that such data cannot be recovered. The qualified Service Provider logs this examination and the measures taken on its basis.
The list of key storage, key generation and signature creation devices used and provided by the Service Provider as well as the certificates of conformity of the devices, can be downloaded from the following link:
https://netlock.hu/en/documents/

The Service Provider continuously monitors the validity of the certificates for the devices it has

applied and any newer restrictions pertaining to their application. In the interest of the above, it has implemented internal administrative policies to keep records of the validity of the certificates and to track the changes in the validity of certifications performed within the European Union. Furthermore, the Service Provider also communicates with the manufacturers and distributors of the devices affected by the certification to be informed as soon as possible about the changes of the certifications.

Service Provider can employ other key handling and signature creation 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 internal Information Security Policy must contain a detailed description of the multi-person private key management method. If this Practice Statement requires multi-person management of a private key, trusted employees authorized to perform the given operation must act in accordance with this requirement.

6.2.3 Private key escrow

The Service Provider does not apply escrow of its own signing private keys used in the provision of the timestamp service.

6.2.4 Private key backup

The Service Provider shall perform the backup (copy), storage and restoration of its own timestamp private keys in a documented manner, in a physically protected environment in the joint presence of at least two trusted employees, with the exclusion of the presence of any other persons. The number of employees authorized for these operations shall be kept to a minimum.

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 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 are used for encryption that ensures protection for its entire remaining validity. The copies of the Service Provider's private key not being used are protected with a level of security equal to the productive key.

6.2.5 Private key archival

The Service Provider doesn't archive its own timestamp private keys.

6.2.6 Private key transfer into or from a cryptographic module

The transfer into a cryptographic module of Service Provider's private keys – thus also including timestamp 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 Service Provider's timestamp 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 Information Security Regulations sets forth the details of the method for activating its own keys.

6.2.9 Method of deactivating private key

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

6.2.10 Method of destroying private key

The Service Provider destroys its own 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 Service Provider's device is destroyed, the Service Provider ensures that the private keys stored on it are also destroyed.

6.2.11 Cryptographic module rating

See the contents of Chapter 6.2.1.

6.3 Other aspects of key pair management

The conditions regulating the use of timestamp keys are as follow:

- The Service Provider shall specify the validity period of its own timestamp certificates in a way that the end of validity does not exceed the time until which the applied cryptographic algorithms can be safely used.
- The Service Provider shall issue the timestamps securely and include the exact time, which can be traced back to a UTC time. The time shall be synchronized with UTC in a way that it shall not deviate from the 1-second accuracy. If the Service Provider's clock deviates from this accuracy, the Service Provider shall not issue timestamps. The Service Provider shall protect the Timestamp Server's clock from any threats that would degrade the accuracy of the time in an undetectable manner. It shall manage the time and its synchronization in the event of a leap second and shall log the exact time of the procedure.
- Timestamps are signed with a key that is not used for any other purposes. The system refuses to issue timestamps after the timestamp key expires.

- The Service Provider issues only qualified timestamps through a qualified timestamp access point. Qualified timestamps are signed with a private key that is verified by a qualified certificate.

6.4 Activation data

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.

6.4.1 Activation data generation and installation

The activation data of the Service Provider's key pair is created when the key pair is generated.

6.4.2 Activation data protection

The activation data of the Service Provider's key is securely stored.

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 Information Security Regulations 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

Not applicable.

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 Information Security Regulations.

7 TIMESTAMP PROFILES

For the profiles of the certificates authenticating the issued timestamps see Chapter 7.4 of NETLOCK Service Practice Statement for Qualified Certificate Services.

For the timestamp, timestamp request and timestamp reply protocol profiles see Chapter 7 of NETLOCK Service Practice Statement for Qualified Timestamp Service.

7.1 Timestamp request profile

The Timestamp Server only supports the timestamp requests according to the ETF RFC 3161, Chapter 2.4.1[7] (supported fields: reqPolicy, nonce, certReq) and those hash algorithms that comply with the resolution of the National Media and Infocommunications Authority on permitted algorithms and minimum key sizes. Accordingly, the Service Provider may only accept timestamp requests from clients containing a hash fingerprint generated with sha256 or sha512 algorithm.

7.2 Timestamping profiles

The timestamp issued by the Service Provider complies with the ETSI 319 422 timestamp profile. Supported fields: Policy, genTime, accuracy.

The ordering field may not be included in the timestamp or may only be set to “false”, and none of the extensions may be marked as critical.

The timestamp reply contains only the Service Provider’s timestamp signature. The signerInfo attribute of the SigningCertificate or SigningCertificateV2 field of the SignedData must contain the timestamp certificate identifier (ESSCertID or ESSCertIDv2).[8]

The Timestamp Server supports and the applications processing the timestamps must support the timestamp replies according to the ETF RFC 3161, Chapter 2.4.2[9] (fields to be supported are: accuracy, nonce) and those signature algorithms and key lengths that comply with the resolution of the National Media and Infocommunications Authority on permitted algorithms and minimum key sizes.

If the nonce field was present in the timestamp request, the reply shall contain the nonce field with the same value.

The qualified timestamp may also include the qcStatements extension in the form according to the IETF RFC 3739 standard with the esi4-qtstStatement-1 value, marked as a non-critical extension.

7.3 Timestamp transport protocol profile

The Timestamp Server supports and the applications processing the timestamps must support the timestamp transport protocol over HTTP and HTTPS protocols[10]. The use of HTTPS protocol is preferred.

The Service Provider issues only qualified timestamps via the access URL provided to the

[7] See https://www.ietf.org/rfc/rfc3161.txt

[8] IETF RFC 3161 IETF RFC 5816

[9] See https://www.ietf.org/rfc/rfc3161.txt

[10] See IETF RFC 7230–7235 and IETF RFC 2818 standards and IETF RFC 3161, Chapter 3.4

Subscriber.

8 COMPLIANCE AUDIT

In line with European Union and Hungarian regulations and the requirements laid out in the Trust Service Policy, the Service Provider performs its service activities according to the following standards (see Chapter 9.15 for legal compliance).

Standard identifier	Short English name
ETSI EN 319 421	ESI; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI EN 319 422	ESI; Time-stamping protocol and time-stamp token profiles

The Service Provider performs (and makes others perform) compliance inspections and checks in the interest of ensuring that the processes, staff, devices, and environment related to its Services always meet relevant legislative and professional requirements.

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, adhering to the following:

- evaluation takes place on the basis of the pieces of legislation and standards laid out in this Chapter;
- the evaluation takes into account all of the unique features of the Service Provider's trust services to be audited;
- the evaluation covers all service activities related to its subject.

8.1 Frequency or circumstances of assessment

In line with EU law, the Supervisory Body supervises the Service Provider's activities. At least every year, the Supervisory Body holds an on-site inspection at the Service Provider's registered address or site.

The results of the audits and the documents drawn up in the course of such audits are confidential, with access provided only to persons with suitable authorisation.

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

The Service Provider has an independent accredited conformity assessment body perform a conformity assessment audit at least every year.

The Service Provider's compliance with the ISO 9001 and ISO 27001 standards (as detailed in Chapter 1.1.2 of this Statement) is evaluated and continuously monitored by an external auditing organisation, with a frequency of at least once a year.

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 trusted 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 of his/her direct relatives can be in an employment relationship with the Service Provider;
- the results of the activities performed during the assessment, which do not affect their fee.

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 Trust 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;
- occasional configuration monitoring of the Trust Services according to IT security requirements.

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.

The Service Provider will send the results of the compliance assessment to the Supervisory Body within 3 working days.

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 fees for the timestamp service set out in the present Statement.

The Service Provider can also sell the services as part of service packages, in which case the timestamp service fee is included in the service package fee.

The fee for the timestamp service used within the framework of the NL Sign service is included in the fee for the NL Sign service.

The conditions and the other rules pertaining to the Service Provider's fees are laid out in the GTC.

9.1.1 Timestamp service fees

The timestamp service fee covers the costs of the identification and authentication process required to conclude the Service Agreement, the generation of the timestamp URL and the provision of the contractually agreed amount of timestamps for the contractually agreed period.

9.1.2 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 (possibly 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 (e.g. a certain number of timestamps) 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, 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 timestamps are affected in a given insurance event, the rate of compensation is

determined for the individual Clients and agreements 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 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.

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 costs payable to the Supervisory Body under the Dáptv. due to the non-performance of the obligations prescribed by the Dáptv.; and
- the costs of the procedures of the compliance assessment organs involved by the Supervisory Body under the applicable provisions of eIDAS, provided that such costs are claimed by the Supervisory Body as procedural costs.

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

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:

- registration data;
- documents submitted by the Client;
- the audio recordings recorded at Customer Service;
- unique identifier in the timestamp URL provided to the Client;
- data provided by the Client when requesting the service;
- 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: 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 may transfer the Client data to the degree necessary and for the purpose of performing the respective tasks to its sub-contractors and agents in the following cases:

- creating the devices necessary for the use of the service;
- invoicing;
- enforcement of claims against the Client.

Service Provider shall disclose confidential information only in the following cases:

- Mandatory data provision for the Supervisory Body in accordance with the relevant

provisions of Dáptv. The Service Provider ensures the confidentiality, authenticity and completeness of the data during data provision.

- For the purpose of detection or prevention of criminal offenses or in the interest of national security, upon the fulfilment of the criteria set out in separate legislation, upon request of the investigative authority and/or national security services in accordance with the relevant provisions of Dáptv. Service Provider shall record the fact of disclosure, but shall not notify the affected Client of the disclosure, pursuant to the applicable legislation.
- Provision of information in the context of civil or criminal proceedings in accordance with the relevant provisions of Dáptv.
- In the event of termination of the trust service, the transfer of data specified in the law related to the service to be terminated to the receiving Service Provider in accordance with the relevant provisions of Dáptv.

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 personal data of the Clients in line with the provisions of

- this Statement and the Service Policy;
- Act CXII of 2011 on the Right of Informational Self-Determination and on 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.

Service Provider shall prevent the unauthorized access to any data it has been provided with.

Service Provider shall have a data processing policy in place, which shall be comprised of detailed provisions on the processing of confidential information and personal data. Service Provider shall, on its website (see Chapter 1.1.2) inform its Clients in a Privacy Notice on the data processing practice laid down by the data processing policy.

The Service Provider is registered by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) as a data controller. Data processing registration number of the Service Provider: NAIH-50145/2017.

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; or
- 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 indispensable and 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, and the processing thereof shall be based on the consent of the data subject.

9.4.3 Information not deemed private

The Service Provider does not consider the data outside the scope of data specified in Chapter 9.4.2 to be personal.

9.4.4 Protection of personal data

The Service Provider shall store the personal information in its possession in a secure manner and shall protect it, in compliance with the applicable requirements (see Chapter 9.4.1). Suitable measures shall be implemented to protect the data from unauthorized access and modifications, especially when forwarding those between the Client and the Service Provider's various units. They shall furthermore be protected against data loss, damage, and unauthorized processing. See also: Chapters 5.3.1, 5.5.1, 5.7.1, 5.7.4, and 9.3.3.

9.4.5 Usage of private information

With regard to the requirements set out in the Privacy Act of Hungary, the Services Provider may only use the personal data in a manner and to the extent that is required for the actions related to the service.

9.4.6 Data management

The ground for processing data by Service Provider is the lawful interest of the Service Provider and the data subject, as well as the prior, informed and specific consent of the data subject.

Service Provider shall store and process the personal data in the light of the provisions enlisted in Chapter 9.4.1 and in accordance with the applicable procedural rules set out in Chapter 5, and the personal data may be disclosed by Service Provider to statutorily specified third parties only in the cases enlisted in Chapter 9.3.3 and in the cases set out in the applicable legislation.

9.4.7 Other information disclosure circumstances

In the interest of uncovering and preventing crimes with the use of the trust services that it provides, as well as for reasons of national security, the Service Provider shall forward data free of charge to investigating authorities and national security services if the conditions for data requests set forth in separate legislation are met; the above extends to data certifying the personal identity of the involved parties and other data. The fact of the data provision is recorded by the Service Provider; however, it does not inform the Relying parties of the data provision (see 9.3.3).

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 the Service Provider,
- timestamp URL provided to the End User

disclosed/issued/created by the Service Provider are also owned by the Service Provider.

End User is a full user of the timestamp URL provided to him/her.

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 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 Service Partners.

9.6.1 The Certification Authority's responsibilities

See Chapter 9.6.1 of the Service Policy.

9.6.2 The Registration Authority's responsibilities

See Chapter 9.6.2 of the Service Policy.

9.6.3 Representations and warranties of the Client

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;
- reporting without delay any changes to data;
- becoming familiar with the contents of the Trust Service Policy, this Practice Statement,

as well as the GTC and the Service Agreement before making use of the services.

The End-User is responsible for:

- the secure handling of the timestamp URL;
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the issued timestamps, certificates or their use before using legal means to settle the dispute;
- using the services in the manner required by law and this Statement.

The Subscriber is responsible for:

- being familiar 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;
- adhering to the End User's obligations to the degree it affects those;
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the issued timestamps, certificates or their use;
- ensuring that unauthorised persons cannot access the timestamp URLs required for making use of the services;
- meeting its fee payment obligations.

9.6.4 Representations and warranties of the Relying Party

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:

- check the acceptance and qualified nature of the Service on the trusted list;
- adhere to the requirements and rules set out in the Service Provider's Trust Service Policy and this Statement;
- use reliable IT environments and applications;
- check the status of the certificate authenticating the timestamp with the current CRL or OCSP response.

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

See Chapter 9.6.5 of the Service Policy.

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.

See also the contents of Chapters 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 timestamps 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 administrative tasks and processes related to the use of services and the use of timestamps, 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 submitted during the registration process.

In the course of contact by email, it is also necessary for the service in question to be unequivocally identifiable.

If the Client contacts the Service Provider by email, 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.

The amended Statement may enter into effect on the 30th day from the publication thereof and the notification of the Supervisory Body, at the earliest, but in extraordinary cases, such amendments may even enter into effect immediately.

The Service Provider shall notify the Supervisory Body if there is a change in its operation or in the provision of trust services – for example, in the Service Policy or the Statement – compared to the data registered based on previous notifications.

See also Chapters 1.5 and 2.1.

9.12.1 Amendments

The Service Provider collects requests for changes (see 1.5), performs the amendments, fulfils internal and external information provision obligations, and has the changes enter into effect.

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.

By collecting the modifications, the Policy Adopting Authority shall create internal, non-public drafts of the regulations, which shall be subject to an internal review before the publication. Service Provider shall, if possible, batch the changes into a new version of the regulation, in order to reduce the number of issues of the regulations.

The person who approved the given regulation (see 1.5) approves the amendments, prior to which the above requirements regarding content and form are again checked. The Supervisory Body, Clients and Relying Parties are then notified (see 9.12.2). The Service Provider has final liability and responsibility for approving the regulation; after its notification, the Supervisory Body registers the Statement.

Service Provider shall have the ultimate power and responsibility for the adoption of the Practice Statement.

The versions of the amended statements – including the public drafts – shall always be published with new version numbers.

The Service Provider accepts comments regarding the published draft Policy or Practice Statement for 14 days after its entry into effect; comments are to be submitted by email (see 1.5). 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 before its entry into effect.

9.12.2 Notification mechanism and period

The Service Provider shall inform the Supervisory Body of any planned changes to its Policy and Practice Statement as compared to the former regulations reported to and registered by the Supervisory Body. Simultaneously with the notification the Service Provider shall send to the Supervisory Body the new version of the regulation with the amendments approved, and – for informing the Clients and the Relying Parties – shall publish it on its website (see 2.1.2).

In case Service Provider plans to launch a new service as a result of, and simultaneously with

the change, it shall notify the Supervisory Body at least 30 days prior to the planned launch of the new service.

The notice shall be made by filling the form published by the Supervisory Body, in accordance with Decree No. 470/2017 of the Government. The Service Provider shall attach the followings to the form

- the amended and approved new version of the Certificate Policy;
- the amended and approved new version of the Practice Statement;
- the amended and approved new version of the extract of the Practice Statement;
- the other instruments and documents set out in Decree No. 470/2017 of the Government.

9.12.3 Circumstances under which OID must be changed

New public versions of the Practice Statement – also the drafts – are published with new version numbers, i.e. two documents with different contents shall not have an identical OID.

The identifier of the document shall be comprised of the following elements – the elements are separated by dots: Service Provider OID (1.3.6.1.4.1.3555), marking of public documents (1), marking of Practice Statements (1), the unique serial number of this document among the public Practice Statements (11), an indication that the document is not an annex (0), version (which is the effective date in short date format), i.e. in the case of the present Service Practice Statement: 1.3.6.1.4.1.3555.1.1.11.0.YYMMDD.

Please note, that the new Practice Statement will only be applicable to certificates issued after its effective date. Any certificate issued prior to the release of the Statement will not be subject to the new guidelines.

9.13 Dispute resolution

The Service Provider (including service 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 being 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: H-1016 Budapest, Krisztina krt. 99., III. em. 310.
- Mailing address: H-1253 Budapest, Pf. 10.
- Email: bekelteto.testulet@bkik.hu
- Website: www.bekeltet.hu

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály (Budapest Government Office, Consumer Protection Department):

- Address: H-1056 Budapest, Váci utca 62–64.
- Phone: +36-1 328 5862
- Mailing address: H-1364 Budapest, 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 conducts its activity in line with applicable law and standards. The registration of both the Service Provider and the trust services at the Supervisory Body certifies that operations meet the requirements of relevant legislation.

The Service Provider conducts its activities in accordance with the applicable provisions of the following pieces of legislation, standards, and requirements:

- **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 (eIDAS)
- **Dáptv.**: Act CIII of 2023 on the digital state and certain rules for the provision of digital services
- **BM Decree**: Decree of the Ministry of Interior 24/2016 of 30 June on the detailed

requirements concerning trust services and their providers
- Decree 470/2017 of 28 December of the Government 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
- **Fgytv.**: Act CLV of 1997 on Consumer Protection (Consumer Protection Act)
- **Nytv.**: Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens (Records Act)
- **Szmtv.**: Act I of 2007 on the Entry and Residence of Persons with the Right of Free Movement and Residence (Free Movement Act)
- **Harmtv.**: Act II of 2007 on the Entry and Residence of Third Country Nationals (Third-Country Nationals Act)
- **Ket**: Act CXL of 2004 on the general rules of administrative procedure and services and its implementing regulations (Act on Administrative Procedures)
- **Ptk.**: Act V of 2013 on the Civil Code (Civil Code)
- Government Decree 45/2014 of 26 February on the detailed rules on agreements between consumers and companies
- **Infotv.**: Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Information Act)
- **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Public Administration 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
- EVCP: Extended Validation Certificate Policy: Certificate Policy pertaining to the certificates for website authentication subject to extended validation, 0.4.0.2042.1.4
- 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 Partners 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.