PKI DISCLOSURE STATEMENT

Extract of the practice statements of NETLOCK's certificate and timestamp services

NETLOCK Informatics and Network Security Services Limited Liability Company

Document name in Hungarian:	PKI Szabályozási Nyilatkozat
Document name in English:	PKI Disclosure Statement
Document short name:	PDS-EN
Version:	26021850414
Object identifier (OID):	1.3.6.1.4.1.3555.1.6.202602185041 4
Date approved:	19/01/2026 14/04/2025
Valid from:	18/02/2026 14/04/2025
No. of pages:	28 pages including cover
Prepared by	NETLOCK Compliance
Accepted by:	**dr. Vey Dorottya** **Head of Compliance**

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

The present document is a translation of the original Hungarian language Service Policy with the same title.
It is published with the same OID as the original Hungarian document (see Hungarian and English title and OID on the cover).

The present English version is not the official document.
The official Service Policies registered by the Supervisory Body are the Hungarian versions.

In case of any difference between the Hungarian and the English version, the Hungarian version shall be applied.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

Tartalom

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

1 Introduction

This document is a single summary (hereinafter referred to as the extract) of NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Kft. (hereinafter referred to as Service Provider or Trust Provider) for the following trust services:

- Qualified website authentication certificate service, qualified signature and seal certificate service with software and smart card key storage as well as within the framework of the "NETLOCK" cloud service, furthermore qualified certificate service within the framework of the "NETLOCK" cloud service (see: Service Practice Statement for Qualified Certificate Services)
- Qualified timestamp service (see: Service Practice Statement for Qualified Time Stamp Services)
- Non-qualified certificate service (see: Service Practice Statement for Non-qualified Certificate Services)
- Non-eIDAS certificate service (encryption, authentication, DV) (see: Service Practice Statement for Non-eIDAS Certificate Services)

The detailed rules of procedure and operation for certain trust services are governed by the Service Provider's specific Service Statements and Service Policies (see: https://netlock.hu/aktualis-szabalyzatok/).

This extract aggregates the content for services provided by the Service Provider in accordance with the following laws/standards:

- 24/2016 BM Decree on the regulations of extract - typically service provided - content specifications of trust service providers.
- ETSI 319 411-1 Non-Qualified and ETSI 319411-2 Qualified Content Requirements for Certified Release Issue Standards (PDS)
- The ETSI 319 421 Time-Stamp Standard Extract (TDS) Content Requirements

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

2 Provider's data

Company Name:	NETLOCK Informatics and Network Security Services Limited Liability Company
Hungarian name:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Short name (EN/HU):	NETLOCK Ltd. / NETLOCK Kft.
Registered seat:	H-1143 Budapest, Hungária krt. 17-19.
~~Postal address:~~	~~H-1439 Budapest, Pf. 663~~
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
~~Fax number:~~	~~(+36 1) 700 2828~~
Website:	https://netlock.hu/
Statements and Clauses published:	https://netlock.hu/aktualis-szabalyzatok (official Hungarian versions) https://netlock.hu/aktualis-szabalyzatok/#en (English translation)
Customer service e-mail:	info@netlock.hu
For orders, document copies, and agreements:	igenylesek@netlock.hu *or* kerelmek@netlock.hu
NETLOCK Policy Acceptance Unit email:	szee@netlock.hu
Customer service /Business hours:	At the place and within the time interval set out on the website of the Service Provider

formázott: Betűtípus: 10 pt

3 Revisions of the Document

OID	Validity	Description of change	Prepared by
1.3.6.1.4.1.3555.1.62.20180926	26.09.2018 – 23.11.2021.	This document is a translation of the original same titled Hungarian language Service Policy (see Hungarian and English title and the OID on cover).	Szabó Zoltán Varga Viktor
1.3.6.1.4.1.3555.1.6.20210716	24.11.2021.- 13.04.2025	All previous revisions in the same titled Hungarian document added in English translation.	NL Compliance
1.3.6.1.4.1.3555.1.6.20250414 ~~20210716~~	~~from~~ 14.04.2025. – 17/02/2026 ~~until it is withdrawn or until a new version comes into force~~	All previous revisions in the same titled Hungarian document added in English translation.	NL Compliance

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

1.3.6.1.4.1.3555.1.6.20260218	from 18/02/2026 until it is withdrawn or until a new version comes into force	All previous revisions in the same titled Hungarian document added in English translation.	NL Compliance

4 Certificate issuance service

4.1 Validity of certificates

The table below shows the validity of each certificate type.

Type	Certificate lifetime	Key-pair usage time
Qualified Signature, Seal Certificate	Up to 2 years	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.
Non-qualified Signature, Seal Certificate	Up to 2 years	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.
Qualified and non-qualified website authentication certificate, EV website authentication certificate	Up to 1 year	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.
Non-trust certificate (Authentication, Encryption,Signature, DV)	Up to 2 years	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.
Non eIDAS certificate (DV)	Up to 1 year	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.
Provider Certificate	Up to 20 years	The certificate is valid for the validity period.
Test Certificate	Up to 3 years	The Service Provider does not set a limit on the lifetime of the key, but may require the generation of a new key at any time.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

4.2 Revocation and suspension of certificates

Certificates can be suspended or revoked by holders after proper identification for each certificate type. The suspended certificates can be activated by right-holders after proper identification.

In case of the “NETLOCK” cloud service as well as website authentication certificates, there are no suspension and activation.

4.3 Certificate restrictions

The Service Provider does not set a limit on financial transactions. The Usage, Usage limits part in Section 4.2 provides restrictions on the limitation of the scope of certificates in this extract.

4.4 CA certificates availability

The provider's published CA certificates and CRL lists can be found at https://netlock.hu/tanusitvanykiadok/

4.5 Security Recommendations for Using Qualified Certificates

To ensure the safe use of a qualified seal or signatory certificate, at least the following must be observed:

- Do not store your device (client devices, NLSIGN account login data, NETLOCK account login data) and its activation data (PIN, password, activation code) together
- Do not leave your device (client devices, NLSIGN account login data, NETLOCK account login data) and its activation data (PIN, password, activation code) together unattended in activated state
- Do not share your device (client devices, NLSIGN account login data, NETLOCK account login data) and its activation data (PIN, password, activation code)

4.6 Qualified device for qualified certificates

If the Service Provider generates a qualified certificate for creating a qualified signature or seal, it is placed on a QSCD device.

4.7 Customer Responsibilities and Obligations

The Applicant is responsible:

- to provide and validate the data required for the processing of claims;
- for the authenticity, accuracy and validity o
- for the information provided during the registration and application;
- to cooperate in controlling the identity and the information have received during the application - doing everything in his/her power to complete the process as quickly as possible;
- after the release of the certificate and in case of a discrepancy, to notify the Service Provider of the deviation;
- to report promptly any changes in your data and to request suspension or revocation of the certificate or to terminate the use of keys;
- to familiarize with the contents of the relevant Service Policy and these Service Practice Statement, General Terms and Conditions, and Service Agreement before using the service.

The End User is responsible:

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

- to use the devices, keys and certificates correspondent with the policies
- to securely manage the device, key, and activation data;
- for the Provider's prompt notification and full disclosure of disputes relating to the certificate or application before bringing the dispute to legal ways.
- for the proper use of the services in accordance with the law and this extract;
- for use purposes indicated in the certificate and restrictions indicated within;
- for a test-related application of the private keys belonging to the test certificates without real commitment;

- If the End User's Private Key, Client device or activation data has got to any unauthorized person or the same suspected, End-User must immediately notify the Service Provider and initiate the suspension or revocation of the certificate (s) and terminate the use of the certificate.

The Subscriber is responsible:

- Before using the service, to know the regulations of the Service Provider;
- for the reality, accuracy and validity of the data provided during the application;
- to cooperate in controlling the data provided during the application - doing the utmost to complete the process as quickly as possible;
- to initiate the modification, change of key or revocation of the certificate in the required cases and ways;
- to comply with End User Obligations to the extent that they are affected;
- for the prompt notice and complete information of the Provider on any disputes relating to the certificate or application;
- to ensure that unauthorized persons are not able to access the data and tools required to access the service;
- for the fulfilment of the End User's obligation to the extent he has influence on those;
- to fulfill its obligation to pay, unless the Subscriber and the Fee Payer are separate, and payment of the fee is the obligation of the Fee Payer.
-

The Fee Payer is responsible:

- to fulfill its obligation to pay.

4.8 Responsibility of the relying parties

In addition, it is advisable for the Relying Parties concerned to take the prudent procedure required to maintain the level of security guaranteed by the Service Provider:

- in case of trust service, checking the acceptance and rating of the Service on a trust list;
- compliance with the requirements and regulations set forth in the Trust Service Policy and in the Trust Service Practice Statement of the Service Provider;
- use of reliable IT environment and applications;
- check the status of the certificate based on the current CRL or OCSP response;
- Taking into account all restrictions on the use of the certificate (specified in the Service Provider's terms and in the certificate);

The Relying Parties concerned have the right to decide on the acceptance of each certificate and / or the way in which they are used according to their own discretion and / or regulations.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

5 Identification for authentication for each certificate type

The Service Provider issues pre-defined types of certificates described in the sub-sections of this Section. Exact details of identification are contained in Section 3.2 of the relevant Service Practice Statement.

5.1 Issue Test certificate

The Service Provider also issues certificates for testing purpose as per the following.

5.1.1 Issuing of not live test certificates

Not live test certificates are issued by the Service Provider from a test publisher ("Online test"), which are not included in either the EU trust list or any software maker's root program and are solely suitable for the technical testing of signatures or encryption. Their subject in all cases is the "NetLock Test Signature Certificate".

Where to apply? - https://www.netlock.hu/teszttanusitvany
What data should be provided for the application? The e-mail address to be included in the certificate is mandatory.
Identification and authentication: There is no formal identification & authentication for this type of certificates.
Registration process: Electronic registration on the webpage of the service provider
Usage: It's not enrolled into any Root program, it's intended to use for application testing only. It is possible to request test certificate for two purposes: • Testing digital signature • Testing encryption

5.1.2 Issuing of live test certificates

The so-called live test certificates are issued by the Service Provider in the EU trust list (in the case of a trust certificate service) and / or live publishers in the relevant root programs, ensuring that all the certificate types issued by them can be tried. These certificates may be issued only in the context of the relevant Service Practice Statement procedures; however, due to the various testing purposes without legal commitment, the Service Provider does not have to indicate a real natural or legal person in the certificate, so the verification of such subject data is reasonably not expected. At the same time, it is necessary to sign a Service Agreement and to declare the authenticity of the data.

In the case of a test certificate, the Service Provider shall in all cases clearly indicate (at least in the CN field) that the certificate may only be used for testing purposes.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

5.1.3 Hybrid test certificate

The so-called hybrid test certificates are issued by the Service Provider from a test publisher ("NETLOCK TEST ROOT CA") that has been announced on the EU Trust List; however, it is not listed in the root program of software manufacturers and are only suitable for the testing of signature creation. These certificates may be issued only in the context of the relevant Service Practice Statement procedures; however, due to the testing purposes without legal commitment,

Where to apply? Following the registration, it can be applied for in the NETLOCK Client menu available through the Service Provider's website or in the NETLOCK Sign service end-user account.
What data should be provided for the application? According to the Service Practice Statement for the live certificate type to be tested.
Identification and authentication
The Service Provider shall refrain from carrying out identification and authentication, but the Client shall declare the authenticity of the data to be included in the certificate
Registration process
According to the Service Practice Statement for the live certificate type to be tested.
Usage
Test certificates are allowed for testing purposes only without real commitment.

the Service Provider does not have to verify the subject data listed in the certificate. At the same time, it is necessary to sign a Service Agreement and to declare the authenticity of the data.

A hybrid test certificate can only be requested on the so-called demo interface of "NETLOCK cloud services" for trial.

Where to apply? https://demo.netlock.com/
What data should be provided for the application? According to the Service Practice Statement for qualified certificate services.
Identification and authentication The Service Provider shall refrain from carrying out identification and authentication, but the Client shall declare the authenticity of the data to be included in the certificate.
Registration process According to the Service Practice Statement for qualified certificate services.
Usage Test certificates are allowed for testing purposes only without real commitment.

5.2 Qualified and non-qualified certificate services

5.2.1 Qualified signature certificate RQSCD (VideoRA) – within the framework of the "NETLOCK" cloud service

General information
• Issuer: NETLOCK Trust Qualified RQSCD CA, NETLOCK Trust Qualified RQSCD VRA ECC CA, NETLOCK Trust Qualified RQSCD VRA ECC CA 2025 • Initial registration is performed by video technology identification by the Registration unit of the Service Provider. • Only a natural person can request it, but organizational data can also be displayed in the corresponding fields of the certificate.
Identification and authentication
In the initial identification, the Service Provider takes a video recording of the Applicant, in which the Applicant needs to show his/her identification document (among other tasks).

Validity of the document and its data will be verified in trustworthy public database (For Hungarian documents always, for foreign documents, if such a database is available). The data of a non-natural person in the certificate will also be verified in trustworthy public database (if a credible database is not available, verification can be performed based on authentic documents). The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic sources.
Usage, Usage limits
Only a natural person can use the qualified certificate to create a qualified electronic signature with a remote signature service available under the “NETLOCK” cloud service. No other use is allowed.
Certificate Policy
qcp-n-qscd

5.2.2 Qualified seal certificate RQSCD (VideoRA) – within the framework of the “NETLOCK” cloud service

General information
• Issuer: NETLOCK Trust Qualified RQSCD CA, NETLOCK Trust Qualified RQSCD VRA ECC CA, NETLOCK Trust Qualified RQSCD VRA ECC CA 2025 • Initial registration of the Applicant is performed by video technology identification by the Registration unit of the Service Provider. • Can only be request by non-natural (legal) persons
Identification and authentication
In the initial identification, the Service Provider takes a video recording of the Applicant, as a natural person acting on a non-natural (legal) person, in which the Applicant needs to show his/her identification document (among other tasks). Validity of the document and its data will be verified in trustworthy public database (in all cases for Hungarian documents, in the case of foreign documents, if such a database is available). The data of a non-natural person in the certificate will also be verified in trustworthy public database (if a credible database is not available, verification can be performed based on authentic documents). The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic sources.
Usage, Usage limits
Only a non-natural (legal) person can use the qualified certificate to create a qualified seal with a remote signature service available within the framework of the “NETLOCK” cloud service. No other use is allowed.
Certificate Policy
qcp-l-qscd

5.2.3 Qualifiled pseudonym signing certificate with RQSCD key storage

General information
• Issuer: NETLOCK Trust Qualified QSCD ECC CA 2025 • The registration is done by the applicant. • Only a natural person can request it
Identification and authentication
The basis for initial identification is the qualified personal profile signing certificate already issued to the Applicant by the Service Provider. The data of the natural person included in the certificate are checked.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

formázott: Betűtípus: 10 pt, Nem Dőlt, Betűszín: 1. jelölőszín

formázott: Betűtípus: 10 pt, Nem Dőlt, Betűszín: 1. jelölőszín

formázott: Balra igazított, Jobb: 0 cm, Térköz Előtte: 2 pt, Sorköz: Többszörös 1,08 s.

formázott: Balra igazított, Jobb: 0 cm, Sorköz: szimpla

formázott: magyar

Usage, Usage limits
Only a natural person can use the qualified certificate to create a qualified electronic signature. No other use is allowed.
Certificate Policy
qcp-n-qscd

~~5.2.3~~5.2.4 Qualified signing certificate with QSCD or RQSCD key storage – smart card key storage or within the framework of the NLSign service

General information
• Issuer: NETLOCK Trust Qualified QSCD CA, CQLCA, CQLSCA and NETLOCK Trust Qualified QSCD ECC CA, NETLOCK Trust Qualified QSCD ECC CA 2025 • Registration is done by the Registration Unit of the Service Provider. • Only a natural person can apply but the data of the organization can also be displayed in the corresponding fields of the certificate
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A qualified signature certificate and associated keys can only be used to create and verify a qualified electronic signature of a natural person. No other use is allowed.
Certificate Policy
ETSI: QCP-n-qscd; OID: 0.4.0.194112.1.2

~~5.2.4~~5.2.5 Qualified seal certificate with QSCD or RQSCD key storage – smart card key storage or within the framework of the NLSign service

General information
• Issuer: NETLOCK Trust Qualified QSCD CA, CQLCA, CQLSCA and NETLOCK Trust Qualified QSCD ECC CA, NETLOCK Trust Qualified QSCD ECC CA 2025 • Registration is done by the Registration Unit of the Service Provider • Only a non-natural person may apply
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

Formázott táblázat

formázott: Sorkiegyenlítés, Sorköz: Többszörös 1,15 s.

formázott: Sorkiegyenlítés, Sorköz: Többszörös 1,15 s.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

A qualified seal certificate and associated keys can only be used to create and verify a qualified seal of a legal entity. No other use is allowed.
Certificate Policy
ETSI: QCP-l-qscd; OID: 0.4.0.194112.1.3

~~5.2.5~~5.2.6 Qualified signing certificate on SCD device – with smart card key storage or within the framework of the NLSign service

General information
• Issuer: NETLOCK Qualified SCD CA, CQLCA, CQLSCA and NETLOCK Trust Qualified SCD ECC CA • The registration is done by the Registration Unit of the Service Provider or by the applicant. • Only a natural person can apply but the name of the organization can also be displayed in the corresponding field of the certificate (field O)
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A qualified signature certificate and associated keys can only be used to create an advanced electronic signature based on a qualified certificate of a natural person. No other use is allowed.
Certificate Policy
ETSI: QCP-n; OID: 0.4.0.194112.1.0

~~5.2.6~~5.2.7 Qualified seal certificate on SCD device – with smart card key storage or within the framework of the NLSign service

General information
• Issuer: NETLOCK Trust Qualified SCD CA, CQLCA, CQLSCA and NETLOCK Trust Qualified SCD ECC CA • The registration is done by the Registration Unit of the Service Provider or by the applicant. • Only a-non-natural person may apply
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

A qualified seal certificate and associated keys can only be used for creating advanced seals based on a qualified certificate of a legal entity. No other use is allowed.
Certificate Policy
ETSI: QCP-l; OID: 0.4.0.194112.1.1

~~5.2.7~~5.2.8 Qualified signature certificate with software-based key storage

General information
• Issuer: NETLOCK Trust Qualified CA, NETLOCK Trust Qualified ECC CA • The registration is done by the applicant. • Only a natural person can apply but the name of the organization can also be displayed in the corresponding field of the certificate (field O)
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A qualified signature certificate and associated keys can only be used to create an advanced electronic signature based on a qualified certificate of a natural person. No other use is allowed.
Certificate Policy
ETSI: QCP-n; OID: 0.4.0.194112.1.0

~~5.2.8~~5.2.9 Qualified seal certificate with software-based key storage

General information
• Issuer: NETLOCK Trust Qualified CA, NETLOCK Trust Qualified ECC CA • The registration is done by the applicant. • Only a-non-natural person may apply
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A qualified seal certificate and associated keys can only be used for creating advanced seals based on a qualified certificate of a legal entity. No other use is allowed.
Certificate Policy
ETSI: QCP-l; OID: 0.4.0.194112.1.3

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

~~5.2.9~~5.2.10 Non-qualified signing certificate with SCD key storage – smart card key storage

General information
• Issuer: NETLOCK Trust Advanced Plus CA, NETLOCK Trust Advanced Plus ECC CA • The registration is done by the Registration Unit of the Service Provider or by the applicant. • Only a natural person can apply but the name of the organization can also be displayed in the corresponding field of the certificate (field O)
Identification and authentication
The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A non-qualified signature certificate and associated keys can only be used to create an advanced electronic signature of a natural person. No other use is allowed.
Certificate Policy
NCP+; OID: 0.4.2042.1.2

~~5.2.10~~5.2.11 Non-qualified signing certificate with software-based key storage

General information
• Issuer: NETLOCK Trust Advanced CA, NETLOCK Trust Advanced ECC CA • The registration is done by the applicant. • Only a natural person can apply but the name of the organization can also be displayed in the corresponding field of the certificate (field O)
Identification and authentication
The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A non-qualified signature certificate and associated keys can only be used to create an advanced electronic signature of a natural person. No other use is allowed.
Certificate Policy
LCP

~~5.2.11~~5.2.12 Non-qualified seal certificate with SCD key storage – smart card key storage

General information
• Issuer: Trust Advanced Plus CA, NETLOCK Trust Advanced Plus ECC CA

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

• The registration is done by the Registration Unit of the Service Provider or by the applicant. • Only a non-natural person may apply
Identification and authentication
The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A non-qualified seal certificate and associated keys can only be used to create and verify an advanced seal of a legal entity. No other use is allowed.
Certificate Policy
NCP+; OID: 0.4.2042.1.2

~~5.2.12~~5.2.13 Non-qualified seal certificate with software-based key storage

General information
• Issuer: NETLOCK Trust Advanced CA, NETLOCK Trust Advanced ECC CA • The registration is done by the applicant. • Only a non-natural person may apply
Identification and authentication
The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
A non-qualified seal certificate and associated keys can only be used to create and verify an advanced seal of a legal entity. No other use is allowed.
Certificate Policy
LCP; OID: 0.4.0.2042.1.1

~~5.2.13~~5.2.14 Qualified EV website authentication certificate

General information
• Issuers: NETLOCK Trust Qualified EV CA, NETLOCK Trust Qualified EV CA 2, NETLOCK Trust Qualified EV CA 3, NETLOCK TLS Qualified EV ECC CA • The registration is done by the applicant. • Only a non-natural person may apply
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.) The domain name will be checked in central databases and via technical checking.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
ETSI: QCP-w; OID: 0.4.0.194112.1.4

~~5.2.14~~5.2.15 Qualified website authentication certificate

General information
• Issuers: NETLOCK Trust Qualified EV CA, NETLOCK Trust Qualified EV CA 2, NETLOCK Trust Qualified EV CA 3, NETLOCK TLS Qualified EV ECC CA • The registration is done by the applicant. • Only a non-natural person may apply
Identification and authentication
Initial identification requires a personal appearance before the Service Provider or notary. The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.) The domain name will be checked in central databases and via technical checking.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
ETSI: QCP-w; OID: 0.4.0.194112.1.4

~~5.2.15~~5.2.16 Non-qualified EV website authentication certificate

General information
• Issuers: NETLOCK Trust EV CA, NETLOCK Trust EV CA 2, NETLOCK Trust EV CA 3, NETLOCK TLS EV ECC CA • The registration is done by the applicant. • Only a non-natural person may apply
Identification and authentication
The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.) The domain name will be checked in central databases and via technical checking.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum: EVCP; OID: 2.23.140.1.1

~~5.2.16~~5.2.17 Non-qualified OV website authentication certificate

General information
• Issuer: Trust SSL CA, Expressz, Üzleti, Közjegyzői and NETLOCK TLS OV ECC CA • The registration is done by the applicant. • Only a non-natural person may apply
Identification and authentication
The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.) The domain name will be checked in central databases and via technical checking.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum: OVCP; OID:2.23.140.1.2.1

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

5.3 Non-eIDAS Service Certificate Issuance

5.3.1 Authentication Certificate

General information
• Issuer: Trust CA (for authorities: Üzleti), NETLOCK TLS DV ECC CA • The registration is done by the Registration Unit of the Service Provider or by the applicant. • A natural person may ask, the organization field can be displayed to the organization to which it belongs. • Authentication certificate can be issued for organizations. • The certificate may be issued on a cryptographic device (SCD) or with software-based key storage.
Identification and authentication
The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)
Usage, Usage limits
The certificate can be used for user authentication.
Certificate Policy
NCP+; OID: 0.4.2042.1.2 or NCP; OID: 0.4.0.2042.1.1 or LCP; OID: 0.4.0.2042.1.3

5.3.2 Encryption Certificate

General information
• Issuer: Trust CA, NETLOCK Trust Advanced ECC CA • The registration is done by the Registration Unit of the Service Provider or by the applicant. • A natural person may ask, the organization field can be displayed to the organization to which it belongs • Encryption certificate can be issued for organizations. • The certificate may be issued on a cryptographic device (SCD) or with software-based key storage. • Key recovery is recommended for users.
Identification and authentication
The data of the natural person in the certificate will be verified in trustworthy public database. The data of a non-natural person in the certificate will be verified in trustworthy public database. The procedural rights of a person acting on behalf of a non-natural person will be verified through a public credentials database and a mandate. Additional data can be checked based on authentic documents. (If a credible database is not available, verification can be performed based on authentic documents. If no authentic document is available, the Client's statement in the Service Agreement guarantees the authenticity of the data.)

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

Usage, Usage limits
It can only be used for encryption and decryption.
Certificate Policy
NCP+; OID: 0.4.2042.1.2 or NCP; OID: 0.4.0.2042.1.1 or LCP; OID: 0.4.0.2042.1.3

5.3.3 DV SSL Certificate

General information
• Issuer: Online SSL CA, • The registration is done by the applicant.
Identification and authentication
Technical inspection.
Registration process
The Applicant registers online with a domain name, the registration is checked by an automated process and the certificate is issued after successful technical inspection.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum: DVCP, OID:2.23.140.1.2.2

6 Qualified Time Stamp Service

6.1 The type of timestamps and their use

Qualified timestamps to be served have the following parameters:

- comply with the standard BTSP Certification Policy
- the timestamp responses to SHA256, SHA512 and ecdsa with SHA384 fingerprints
- validity in accordance with standard specifications: signatures matched to the **2048 bit SHA256** hash expire on 31.12.2028.
- validity in accordance with standard specifications: **ecdsa-with-SHA384 hash** signature currently has no expiry date
- Checking the generated time stamps can take place by checking the time stamp certificate and chain certificates and their revocation information (CRL or OCSP).

6.2 Retention

The retention time for logs are 10 years.

6.3 Accuracy

The service provider responds to a time stamp request with a precision of 1s specified in the BTSP order and indicates it by positioning the ID of the BTSP Certificate Policy or the corresponding service provider ID in the reply.

6.4 Subscriber Obligations

The Applicant is responsible:

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

- to provide and validate the data required for the processing of claims
- the authenticity, accuracy and validity of the information provided during the registration and the application;
- to cooperate in controlling your identity and the information you have received during your application - doing everything in your power to complete the process as quickly as possible;
- to report promptly to changes in the applicants data;
- for prior to using the service, to familiarize with the contents of the relevant Services Policy and Service Practice Statement and the terms of the General Terms and Conditions and the Service Agreement.

The End User is responsible:

- to manage the timestamp URL safely;
- to Provide the Service Provider with prompt notice and complete information on disputes relating to the time stamps, certificates, or applications issued to them before filing a lawsuit;
- for the use of the services in accordance with the law and this Code.

The Subscriber is responsible:

- for Before using the service, to know the rules of the Service Provider;
- for the reality, accuracy and validity of the data provided during the application;
- to cooperate in controlling the data provided during the application - doing its utmost to complete the process as quickly as possible;
- to comply with End User Obligations to the extent that they are affected
- to provide the Service Provider with prompt notice and complete information on disputes relating to time stamps, certificates, or applications;
- to ensure that no timeshare URLs required for the use of the service are accessible to unauthorized persons;
- to fulfill its obligation to pay.

6.5 Recommendations for relying parties

In addition, it is advisable for the Parties concerned to take the prudent procedure required to maintain the level of security guaranteed by the Service Provider:

- checking the acceptance and rating of the Service on a trust list;
- compliance with the requirements and Practice Statements set forth in the Service Policy of the Service Provider;
- use of reliable IT environment and applications;
- check the status of the time stamp credentials with the appropriate CRL or OCSP response.

The Parties concerned have the right to decide on the acceptance of each certificate and / or the way in which they are used according to their own discretion and / or regulations.

7 Insurance

Against the Customer and/or Subscriber, the Service Provider is responsible for the damage caused by the Certificate in accordance with the rules of liability for breach of contract as defined in the Civil Code in force at any time when it violates its statutory obligations.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

According to the Service Provider's insurance contract, the Service Provider's liability value is in case of non-qualified certificate service HUF 3,000,000 (three million), while in case of qualified certificate service minimum HUF 5,000,000 (five million) per loss event. A time-related injury event for several reasons is considered as an insurance event.

8 Responsibility Value

The Service Provider's insurance company for damages caused by the Service Provider's liability for its own fault or omission will pay compensation for the limit mentioned in the insurance, or in the certificate.

9 Preservation rules

The Service Provider retains the electronic information related to the certificates and the related personal data from the date of their origin for a period of at least ten years from the expiration of the validity of the certificate and the final legal dispute on the electronic signature and the electronic document signed thereon and, by the same deadline, provides a means by which the certificate Content can be established. The Service Provider may also fulfill this obligation of retention by using a qualified electronic archiving service provider.

10 Customer Responsibilities

By signing the contract for the service provided by the Service Provider, the Customer undertakes to comply with the following provisions:

- Must know and accept the Service Provider's applicable Service Practice Statement, Service Policy, GTC, and other requirements for using the Service;
- Provide accurate data or datas to the Service Provider in cooperation with the Service Provider in order to obtain and complete the services and to monitor the data in order to complete the audit as soon as possible;
- Must notify the Service Provider of any changes in any of the data recorded in the Contract. If failure to notify data change causes damage or causes the Service Provider to be disadvantaged, it may serve as termination of service by the Service Provider. The Customer shall be liable according to the general rules of civil law for damages resulting from his failure to fulfill this obligation;
- Must use the services solely for purposes permitted by law or not prohibited for use in accordance with the Terms of Service;
- To be responsible for ensuring that the data and tools (passwords, secret codes, smart cards, secret keys) required for the use of the services are accessible to the authorized persons only, for the damages resulting from failure to do so, in accordance with the general rules of civil law;
- To be obliged to use the services in a manner that does not hinder the provision of services in accordance with current legislation, in the interests of service to other customers and the availability of services.

11 General rules on fees

The Service Provider determines, in particular, but not limited to, the fees of the following Trusted Services and related Optional Services listed on the website.

Trust services:

- Services for qualified and nonqualified certificates

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

  - Certificate issuance service;
  - Certificate issuance repetition service;
  - Certificate renewal service;
  - Certificate modification service;
  - Certificate rekey service.
- Qualified Timestamp Service

Optional Services:

- Mobile registration service;
- Transfer of a client device by a service agent;
- Post payment;
- Accelerated issuing
- Unlocking blocked client tools;
- Replacement of a customer base;
- Unique administration fee.

Pricelist and payment information: https://netlock.hu/uj-arlista/

12 Protecting Personal Information

The Service Provider protects the data provided to you against unauthorized access and modification, as well as loss of data, damage, and unauthorized processing.

In addition, the Service Provider uses only the information on the right of information self-determination and the Law on Freedom of Information.

13 Dispute issues, handling and settling complaints

In the event of any disputes or complaints arising, the Customer shall be obliged to the Customer, the Affected Party or any third party to promptly notify and fully inform the Service Provider of any dispute concerning the matter before submitting the dispute to legal channels. The parties are always trying to settle their debates in a peaceful, negotiated way.

In the event that the Customer is considered a consumer, it is possible to conclude a contract, its validity, its effects and termination, and in the event of a breach of contract and its legal effects, a conciliation body or other dispute settlement organization may be contacted.

Complaints will be received by the Service Provider by e-mail at info@netlock.hu, by telephone and in person.

The Service Provider receives a separate record of the complaint received on the phone and informs the complainant by e-mail of the outcome of the investigation, except in the case of a different agreement between the parties. The deadline for the investigation of the complaint is 30 calendar days from the date of filing, if the investigation takes longer than the nature of the complaint, the Service Provider shall inform the Party separately.

In order to investigate a complaint by e-mail and mail, the rules for investigating a complaint on a telephone will be governed by the fact that a separate record is included in this case.

The Service Provider shall, after the complaint has been investigated, rectify the defect in the reasonably justified time and inform the notifier in writing of all such activities. If the respondent does not accept, you must initiate a consultation with the Service Provider. If the Service Provider

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

refuses to do so, or if the consultation between the parties has not been successful within 20 working days of its commencement, the Applicant may file a legal action.

14 Refund Principle

In justified cases, the Service Provider shall reimburse the Subscriber according to the relevant provisions of the General Terms and Conditions and the Service Practice Statements, on the basis of an individual judgment and, if so interpreted, in proportion to the trust services and related optional services.

In justified cases, the Service Provider reimburses certain fees related to the issuance of certificates for a specified period (eg certificate storage fee) on an individual basis. One-off charges are refunded in one installment. In the case of a payment, if it is interpreted, after the expiration of the loyalty period, the Customer is entitled to a refund in such a way that the Service Provider reimburses the pro rata portion of the subscription fee for the month concerned.

15 Applicable law

The Service Provider performs its activities in accordance with the applicable Hungarian and European Union legislation at all times. The Service Provider's contracts and Practice Statements, and their performance, are governed by Hungarian law and are to be interpreted under Hungarian law.

16 Identification, control and role of trademarks

The Service Provider does not warrant the representation of a trademark in the certificate based on the DBA, trademark, product name or product ID owned by the Customer. The Customer's acquisition of a trademark can not be considered an event necessarily resulting in the renewal of a certificate. With the certificate request and acceptance, the Customer expresses that the names, trademarks and other information contained therein are without prejudice to the rights of third parties. The service provider is not obliged to control the legitimate use of the trademarks.

17 Audits of the Trust Service Provider (compliance audits)

The Service Provider performs an external conformity assessment (Compliance assessment procedure according to eIDAS Article 20 section [1]) every year. If the Service Provider operates an outsources Registration Unit, it processes its processes annually.

The Service Provider's activities are supervised by the National Media and Communications Authority as a Trust Authority in accordance with European Union regulations. The FSA regularly holds an on-site visit at the headquarters and premises of the Trust Service Provider on a minimum annual basis.

The results of the checks and the documents made on them are confidential, access is granted only to persons with the appropriate privileges.

In addition to the external audit, the Service Provider performs its own internal audits (once a year), which regularly reviews compliance with previous audits and takes the necessary steps in case of discrepancies.

Other qualifications:

- ISO 9001 standard (continuously since 2001)
- ISO 27001 standard (continuously since 2005)

Certificates are available on the website of the Service Provider at: https://netlock.hu/egyeb-dokumentumok/

18 Trust List

The Service Provider acts as a qualified and non-qualified Trust Service Provider in accordance with the provisions of the eIDAS.

The National Media and Infocommunications Authority as a Trust Service Supervisory Body has registered the Service Provider

- as a Non-Qualified Trust Service Provider since 30 June 2016,
- as a Qualified Trust Service Provider since 19 June 2017.

The Authority's registration is available at the link below:

https://esign.nmhh.hu/esign/

Availability of the trust list maintained and published by the Trust Service Supervisory Body:

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

- readable (pdf) format: http://nmhh.hu/tl/pub/EN_TL.pdf

In the European Union's trust list, the Service Provider can be found at the following link: https://eidas.ec.europa.eu/efda/home

19 Service Provider Contract, Service Practice Statements, Service Policies

For the Service Provider's activities, the following documents are available:

- General Terms and Conditions
- Data Privacy Policy
- Service Policy for Qualified Certificate Service
- Service Policy for Qualified Time Stamp Service
- Service Policy for non-Qualified Certificate Service
- Service Policy for non eIDAS Certificate Service
- Services Practice Statement for Qualified Certificate Services
- Services Practice Statement for Qualified Time Stamp Service
- Services Practice Statement for non-Qualified Certificate Service
- Services Practice Statement for non eIDAS Certificate Service
- ~~Services Policy for Qualified Time Stamp Service~~
- Terms of Service Extract

19.1 Access to regulatory documents

Service Provider Contract, Service Policies, Authentication Policies:
http://www.netlock.hu/szabalyzatok/

20 Privacy Policy Extract Availability

The Service Provider has published information on the privacy and data security rules published for customers on the following link under the Data Protection and Data Security section: https://netlock.hu/aktualis-szabalyzatok/#dataprotection.

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

formázott: Betűtípus: Arial, 11 pt

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

21 Compliance with Existing Legislation

The Service Provider performs its activity in accordance with applicable laws and standards. The operation in accordance with the laws in force is justified by the registration of the Service Provider and the trust services by the Trust Authority.

The Service Provider performs its activity in accordance with the following legal requirements, standards and other regulations:

- **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
- **DÁP:** Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services
- **BM Decree:** Decree 24/2016 of 30 June of the Minister for the Interior on the detailed requirements pertaining to trust services and their providers
- Decree of the Ministry of Interior 25/2016 on the administrative service fees payable to the Trust Service Supervisory Body (VI. 30.);
- Government Decree 321/2024 (XI. 6.) on certain rules of digital citizenship
- **Decree 470/2017** 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

- **Consumer Protection Act:** Act CLV of 1997 on Consumer Protection
- **Records Act:** Act LXVI of 1992 on the Records of Civilian Private Information and Addresses
- **Free Movement Act:** Act I of 2007 on the Admission and Residence of Persons with the Right of Free Movement and Residence
- **Third-Country Nationals Act:** Act II of 2007 on the Admission and Residence of Third-Country Nationals
- **Civil Code:** Act V of 2013 on the Civil Code
- **Government Decree 45/2014** of 26 February on the detailed rules on agreements between consumers and companies
- **Information Act:** Act CXII of 2011 on Informational Self-Determination and Freedom of Information
- **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)
- Közigazgatási Gyökér Hitelesítés-Szolgáltató [Public Administrative Root Authentication Service Provider] Authentication Regulations

- ISO 3166 English Country Names and Code Elements
- FIPS PUB 140-2 (May 2001): “Security Requirements for Cryptographic Modules”

formázott: Tabulátorok: 1,67 cm, Balra igazított + Nincs 8 cm + 16 cm

- 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)
- RFC 6962 Certificate Transparency

- 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 319411-2 Policy and security requirements for Trust Service Providers issuing certificates;
  Part 2: Requirements for trust service 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 319412-5 Certificate Profiles; Part 5: QCStatements
- ETSI EN 319421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- LCP: Lightweight Certificate Policy, OID: 0.4.0.2042.1.3
- NCP: Normalized Certificate Policy, OID: 0.4.0.2042.1.1
- NCP+: Extended Normalized Certificate Policy, OID: 0.4.2042.1.2
- CAB Forum EVCP: OID: 2.23.140.1.1
- CAB Forum OVCP: OID:2.23.140.1.2.1
- CAB Forum DVCP: OID:2.23.140.1.2.2
- QCP-n: certificate policy for EU qualified certificates issued to natural persons; OID:0.4.0.194112.1.0
- QCP-l: certificate policy for EU qualified certificates issued to legal persons; OID:0.4.0.194112.1.1
- QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; OID:0.4.0.194112.1.2
- QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD; OID:0.4.0.194112.1.3
- QCP-w: certificate policy for EU qualified website authentication certificates; OID:0.4.0.194112.1.4
- 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

All further provisions and detailed rules for the services requested are contained in the Service Provider's applicable Service Policies and Terms of Service.