PKI DISCLOSURE STATEMENT

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

NETLOCK Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Document name in Hungarian:	PKI Szabályozási Nyilatkozat
Document name in English:	PKI Disclosure Statement
Document short name:	PDS-EN
Verzió:	20180913
Azonosító szám (OID):	1.3.6.1.4.1.3555.1.15.20180913
Jóváhagyás időpontja:	2018.09.13.
Közzététel időpontja:	2018.09.18.
Hatály kezdőnapja:	2018.10.18.
Oldalak száma:	fedlappal együtt 36 oldal
Készítette:	**Szabó Zoltán** Compliance Manager **Varga Viktor** Chief Architect
Jóváhagyta:	**dr. Fehér Zsófia**, Jogtanácsos

CONTENTS

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 services:

- Qualified trust certificate issuance service
- Qualified trust timestamp service
- Qualified trust archiving service
- Non-qualified trust certificate issuance service
- Non-eIDAS certificate issuance service (encryption, authentication, codesign, DV)

The detailed rules of procedure and opration for certain trust services are governed by the NETLOCK's specific Service Statements and Service Policies.

This extract aggregates the content requested by 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

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-1101 Budapest, Expo tér 5-7.
POSTAL ADDRESS:	H-1439 Budapest, Pf. 663
COMPANY REGISTRATION NUMBER:	01-09-563961
TAX ID:	12201521-2-42
PHONE NUMBER:	(+36 1) 437 6655 | *Application for certificate status change: Press 3*
FAX NUMBER:	(+36 1) 700 2828
WEBSITE:	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

3 Certificate issuance service

3.1 Validity of certificates

The table below shows the validity of each certificate type.

Type	Certificate lifetime	Key-pair usage time
Qualified Signature, Seal and Website Authentication, EV Website Authentication 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 and Website Authentication, EV Website Authentication 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-trust certificate (Authentication, Encryption, Coding 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.
Provider Certificate	Up to 20 years	The certificate is valid for the validity period.
Test 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.

3.2 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 website authentication certificates, there are no suspension and activation.

3.3 Certificate restrictions

The LimitValue value in the qualified certificates is the service provider’s maximum liability value.

3.4 CA certificates availablity

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

3.5 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) and it’s activation data (PIN, password) together

- Do not leave your device (client devices, NLSIGN account) and it’s activation data (PIN, password) together unattended in activated state
- Do not share your device (client devices, NLSIGN account) and it’s activation data (PIN, password)

3.6 Qualified device for qualified certificates

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

3.7 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:

- 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 despute to legal ways.
- fot 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;
- to fulfill its obligation to pay.

3.8 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.

4 Identification for certificate issuance and authentication

4.1 Issue Test certificate

General information
• Issued by a self signed certificate authority (Netlock Test), which is not enrolled into any root programs (Test4) • Registering needs an email address entered on the test requestor page
Identifcation 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

For any certificate type and class, the Service Provider is entitled to issue a test certificate by retaining the requirements of the certificate class. In the case of a test certificate, the Service Provider shall in all cases clearly indicate (indicated in minimum in the CN field) that the certificate may be used solely for testing purposes.

A test certificate may be requested by a Service Provider's employee after the approval of the Service Provider's internal auditor.

4.2 Trust Service Certificate Issuance

4.2.1 Qualified signing certificate on QSCD device

General information
• Issuer: Qualified Trust QSCD CA, CQLCA, CQLSCA • Initial registration is done by the Registration Unit of NETLOCK Kft. • 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.)
Registration process
During the registration, a personal appearance is required before the service provider.
Usage, Usage limits
Only a natural person can use the qualified certificate to create qualified electronic signature.
Certificate Policy
qcp-n-qscd

4.2.2 Qualified seal certificate on QSCD device

General information
• Issuer: Qualified Trust QSCD CA, CQLCA, CQLSCA • Initial registration is done by theRegistration Unit of NETLOCK Kft. • 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.)
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
Only a non-natural person can use the qualified certificate to create a qualified electronic seal.
Certificate Policy
qcp-1-qscd

4.2.3 Qualified signing certificate on SCD device

General information
• Issuer: Qualified Trust SCD CA, CQLCA, CQLSCA • The registration is done by the Registration Unit of NETLOCK Kft. 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.)
Registration process
During the registration, a personal appearance is required before the service provider.
Usage, Usage limits
Only a natural person can use the qualified certificate to create a non-qualified electronic signature based on qualified certificate.
Certificate Policy
qcp-n

4.2.4 Qualified seal certificate on SCD device

General information
• Issuer: Qualified Trust QSCD CA, CQLCA, CQLSCA • The registration is done by the Registration Unit of NETLOCK Kft. 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.)
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
Only a non-natural person can use the qualified certificate to create a non-qualified electronic signature based on qualified certificate.
Certificate Policy
qcp-1

4.2.5 Software based qualified signature certificate

General information
• Issuer: Qualified Trust CA, • The registration is done by the Registration Unit of NETLOCK Kft. 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.)
Registration process
During the registration, a personal appearance is required before the service provider.
Usage, Usage limits
Only a natural person can use the qualified certificate to create a non-qualified electronic signature based on qualified certificate.
Certificate Policy
qcp-n

4.2.6 Software based qualified seal certificate

General information
• Issuer: Qualified Trust CA, • The registration is done by the Registration Unit of NETLOCK Kft. 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.)
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
Only a non-natural person can use the qualified certificate to create a non-qualified electronic seal based on qualified certificate.
Certificate Policy
qcp-1

4.2.7 Non-qualified signing certificate

General information
• Issuer: Trust Advanced CA, Trust Advanced Plus CA (SCD) • The registration is done by the Registration Unit of NETLOCK Kft. 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.)
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
Only a natural person can use the non-qualified certificate to create a non-qualified electronic signature.
Certificate Policy
NCP + - Extended Normalized Certificate Policy, Extended Authentication Order (Client Device required), OID: 0.4.2042.1.2 NCP - Normalized Certificate Policy, Normalized Certification Policy (Client Device non required), OID: 0.4.0.2042.1.1

4.2.8 Non-qualified seal certificate

General information
• Issuer: Trust Advanced CA, Trust Advanced Plus CA (SCD) • The registration is done by the Registration Unit of NETLOCK Kft. or by the applicant. • Only a non-natural person may apply • The certificate may be issued on a cryptographic device (SCD), but this is not required.
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.)
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
Only a non-natural person can use the non-qualified certificate to create a non-qualified electronic seal.
Certificate Policy
NCP + - Extended Normalized Certificate Policy, Extended Authentication Order (Client Device required), OID: 0.4.2042.1.2 NCP - Normalized Certificate Policy, Normalized Certification Policy (Client Device non required), OID: 0.4.0.2042.1.1

4.2.9 Qualified EV website authentication certificate

General information
• Issuer: Qualified Trust EV CA • The registration is done by the Registration Unit of NETLOCK Kft. or 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.) The domain name will be checked in central databases and via technical checking.
Registration process
During the registration, a personal appearance is required before the service provider.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum EVCP: Certificate Policy: OID: 2.23.140.1.1 and qcp-w

4.2.10 Non-qualified EV SSL certificate

General information
• Issuer: Trust EV CA • The registration is done by the Registration Unit of NETLOCK Kft. or 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.) The domain name will be checked in central databases and via technical checking.
Registration process
During the registration, a personal appearance is required before the service provider.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum EVCP: Certificate Policy: OID: 2.23.140.1.1

4.2.11 Non-qualified OV SSL certificate

General information
• Issuer: Trust SSL CA, Expressz, Üzleti, Közjegyzői • The registration is done by the Registration Unit of NETLOCK Kft. 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.) The domain name will be checked in central databases and via technical checking.
Registration process
During the registration, a personal appearance is not required before the service provider.
Usage, Usage limits
It can be used for SSL / TLS communication.
Certificate Policy
CAB Forum OVCP: Certificate Policy: OID: 2.23.140.1.2.1

4.3 Non-trust Service Certificate Issuance

4.3.1 Authentication Certificate

General information
• Issuer: Trust (for authorities: Üzleti) • The registration is done by the Registration Unit of NETLOCK Kft. • 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), but this is not required.
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.)
Registration process
During the registration, a personal appearance is not necessary before the service provider.
Usage, Usage limits
The certificate can be used for electronic signature.
Certificate Policy
NCP+ - Extended Normalized Certificate Policy, Extended (Client device is required) Certificate Policy, OID: 0.4.2042.1.2 NCP – Normalized Certificate Policy, Normalizált (Client device is not required) Certificate Policy, OID: 0.4.0.2042.1.1 LCP – Lightweight Certificate Policy, Lightweight Certificate Policy, OID: 0.4.0.2042.1.3

4.3.2 Encryption Certificate

General information
• Issuer: Trust CA • The registration is done by the Registration Unit of NETLOCK Kft. • A natural person may ask, the organization field can be displayed to the organization to which it belongs • Enryption certificate can be issued for organizations • The certificate may be issued on a cryptographic device (SCD), but this is not required. • 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.)
Registration process
During the registration, a personal appearance is not necessary before the service provider.
Usage, Usage limits
It can only be used for encryption and decryption.
Certificate Policy
NCP+ - Extended Normalized Certificate Policy, Extended (Client device is required) Certificate Policy, OID: 0.4.2042.1.2 NCP – Normalized Certificate Policy, Normalizált (Client device is not required) Certificate Policy, OID: 0.4.0.2042.1.1 LCP – Lightweight Certificate Policy, Lightweight Certificate Policy, OID: 0.4.0.2042.1.3

4.3.3 Code sign Certificate

General information

• Issuer: CodeSign • The registration is done by the Registration Unit of NETLOCK Kft. • A natural person may ask for his/her own • A code signing certificate may be issued to a non-natural person also • The certificate may be issued on a cryptographic device (SCD), but this is not required.
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.)
Registration process
During the registration, a personal appearance is not necessary before the service provider.
Usage, Usage limits
Use only for code signature
Certificate Policy
Non-EV Code Signing, Certificate Policy, OID: 2.23.140.1.4.1

4.3.4 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: Certificate Policy: OID:2.23.140.1.2.2

5 Qualified Trust Time Stamp Service

5.1 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 and SHA512 prints
- its validity can not be estimated (signatures matched to the 2048 bit SHA256 signature hash has no estimated expiration 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).

5.2 Retention

The retention time for logs are 10 years.

5.3 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.

5.4 Subscriber Obligations

The Applicant is responsibler:

- 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.

5.5 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.

6 Qualified Trust Archiving Service

6.1 Conditions for access of third parties

Customer can assign access to third-party access to uploaded files. To do so, customer must send an invitation to each person, and the person must be registered in the system (by prior or subsequent registration). Shared access may be limited (read-only) or complete (including expiration date modification, deletion of the file). Assignment can be revoked.

6.2 Maintain meaningfulness

Maintaining interpretations is provided by the service provider to digitally signed PDF and XML files.

6.3 Archiving only the imprint

When archiving only the imprint, but no the complete document, the Customers needs to archive those again periocialy, but no later than when the Supervisory Authority mandatest the algorithm switchinh.

If this is not done by the Client at the latest when the algorithm is weakened, its archived files will be void, their probative, legal power will be lost.

6.4 The scope of information required for long-term validation

For a signed / stamped document, the information required for long-term validation:

- a qualified timestamp on a document
- the publishing chain of the signature-related certificate
- certificate and publisher chain revocation information (CRL or OCSP)
- the publishing chain of the certificate associated with the time stamp
- certificate and publisher chain revocation information associated with time stamp (CRL or OCSP)

In the absence of the above information, the file can not be archived.

7 Insurance

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.

According to the Service Provider's insurance contract, the Service Provider's liability value is minimum 3,000,000 (three million HUF) 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 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
    - Certificate issuance service;
    - Certificate issuance repetition service;
    - Certificate renewal service;
    - Certificate modification service;
    - Certificate rekey service.
- Qualified Timestamp Service
- Qualified Preservation 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 informations: 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 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 Identification, control and role of trademarks

The Service Provider performs an external conformity assessment 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.

Voluntary accreditation, other qualifications:

- ISO 9001
- ISO 27001 standard
- ETSI 319 401, 319 411, 319 412 and 319 421

The necessary conformity assesment for providing eIDAS qualified trust services (according to eIDAS article 20 paragraph (1)) is comleted by MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. (as a conformity assesment body accorndance to eIDAS article 3, point 18), in May 2017. The conformity assessment is annually reconsidered. The scope of the assesment procedur was the following:

- Szolgáltatási Rend Minősített Tanúsítványszolgáltatásokra,
- a Szolgáltatási Szabályzat Minősített Tanúsítványszolgáltatásokra,
- Szolgáltatási Rend Minősített Időbélyeg-szolgáltatásra,
- Szolgáltatási Szabályzat Minősített Időbélyeg-szolgáltatásra,
- Szolgáltatási Rend Minősített Archiválásszolgáltatásra,
- Szolgáltatási Szabályzat Minősített Archiválásszolgáltatásra,
- and also all of the eIDAS qualified trust services and the practices of the Provider relating these services, as well as the conformity to the laws and standards below.

  Laws including normative requirement of the assessment: (assessment report ID: EJ-01.JOGSZABALY):
  - 910/2014/EU rendelet (eIDAS)
  - 2015. évi CCXXII törvény (Eüt.)
  - 24/2016. BM rendelet
  - 26/2016. BM rendelet
  - 114/2007. GKM rendelet

  Standards including normative requirement of the assessment: (assessment report ID: EJ-01.JOGSZABALY):
  - EN 319 401
  - EN 319 411-1
  - EN 319 411-2
  - EN 319 412-1-5
  - EN 319 421 v1.1.1
  - EN 319 422 v1.1.1

18 Trust List

The Service Provider has announced its services to the Trust Authority on 30 June 2016 as a non-qualified service provider in accordance with the provisions of eIDAS. Contact details of the National Media and Communications Authority: http://webpub-ext.nmhh.hu/esign2016/ Availability of trust list:

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

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

According to the Eat. As a qualified service provider, the FSA registered the Supplier on March 19, 2003. Registration Number: MH-1372-12 / 2003.

According to the Eat. As a qualified archiving service provider, was registered by the FSA on September 15, 2010. Registration Number: HL / 18188-4 / 2010.

In the 15. May 2017 TSP has submitted intention to start providing eIDAS qualified trust service in the 1st of July 2017 to the Supervisory Body.

19 Service Provider Contract, Service Practice Statements, Service Policies

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

- General Terms and Conditions
- Service Policy for Qualified Certificate Service
- Service Policy for Qualified Archiving Service
- Service Policy for Qualified Time Stamp Service
- Services Practice Statement for Qualified Certificate Services
- Services Policy for Qualified Archiving 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 between other documents: https://netlock.hu/aktualis-szabalyzatok/#dataprotection.

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:** az Európai Parlament és Tanács 910/2014/EU Rendelet (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- **Eüt.:** 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- **470/2017 Korm. rendelet:** a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016 (VI. 30.) BM rendelet
- **26/2016 BM rendelet: a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről szóló 26/2016. (VI. 30.) BM rendelet**
- **Közigazgatási Rendelet:** az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI.13.) Korm. rendelet
- **Eat**.: 2001. évi XXXV. törvény az elektronikus aláírásról szóló **(nem hatályos)**
- **Nytv.:**1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
- **Szmtv.:** 2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról
- **Harmtv:** 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról
- **Ket:** 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól és ennek végrehajtási rendeletei
- **Ptk.:** 2013. évi V. törvény a Polgári Törvénykönyvről
- 45/2014 (II. 26.) Kormányrendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- az Európai Parlament és a Tanács személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve, és
- Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési Szabályzat
- Általános Szerződési Feltételek (ÁSZF) – NETLOCK Kft., mindenkor hatályos változata
- ISO 3166 English Country Names and Code Elements
- FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei"
- RFC 5280 (korábban RFC 3280) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil
- RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer

- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer”
- RFC 6960 (korábban RFC 2560) 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, Könnyített Hitelesítési Rend, OID: 0.4.0.2042.1.3
- NCP: Normalized Certificate Policy, Normalizált Hitelesítési Rend, OID: 0.4.0.2042.1.1
- NCP+: Extended Normalized Certificate Policy, Kiterjesztett (Ügyféleszköz használatát megkövetelő) Hitelesítési Rend, OID: 0.4.2042.1.2
- CAB Forum EVCP: Hitelesítési rend: OID: 2.23.140.1.1
- CAB Forum OVCP: Hitelesítési rend: OID:2.23.140.1.2.1
- CAB Forum DVCP: Hitelesítési rend: OID:2.23.140.1.2.2
- QCP-n: certificate policy for EU qualified certificates issued to natural persons; Hitelesítési rend: OID:0.4.0.194112.1.0
- QCP-l: certificate policy for EU qualified certificates issued to legal persons; Hitelesítési rend: 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; Hitelesítési rend: 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; Hitelesítési rend: OID:0.4.0.194112.1.3
- QCP-w: certificate policy for EU qualified website authentication certificates; Hitelesítési rend: OID:0.4.0.194112.1.4

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