NETLOCK Kft.

PKI Disclosure Statement and Abstract

for qualified and non-qualified services

NETLOCK Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Identification number (OID):	**1.3.6.1.4.1.3555.1.62.20161017**
Date of acceptance:	-
Effective Date:	-
Number of pages:	**22, twentytwo page**
Made by:	**Varga Viktor, Chief Architect**
Accepted by:	-

CONTENTS

1 Introduction

This document is the PKI Disclosure Statement and Abstract herein after referred as PDS
This document does not substitute or replace the Certificate Policy and/or Certificate Practice Statement under which digital certificates issued by Netlock Kft (Netlock).
The purpose of this document to summarize the key points of the Netlock CPs and CPSs for the benefit of the Subscribers, Certificate Holders and Relying Parties.
It's a full PKI Disclosure Statement (based ont he modell) with additional sections added to fit for the local legislation.

2 CA Contact info

Name:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Unit:	NETLOCK Kft.
Place of Residence:	1101 Budapest, Expo tér 5-7.
Phone:	(1) 437-6655
Fax:	(1) 700-2828
Web site:	netlock.hu
E-mail:	info@netlock.hu
Opening hours:	As displayed on the home page of Netlock

3 Certificate type, validation procedures and usage

The Netlock issues certificates with predefined Certificate profiles.

The registration and validation are describe below for each type of certificate issued.

3.1 Test certificate

General information
• Issued by a self signed certificate authority (Netlock Test), which is not enrolled into any root programs (Teszt4) • 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 CA
Usage
They are not enrolled into any Root program, they are intended to use for application testing only. It is possible to request test certificate for two purposes: • Testing digital signature • Testing encryption

A CA allowed to issue test certificates for every type of certificates and classes.
If a certificate made for testing purposes, it is displayed in the CN field amd also differenet CP OID set.

3.2 Advanced Signer and Seal certificates

General information
• Issued by one of the following CA-s: Expressz Eat., Üzleti Eat., Közjegyzői Eat. Trust Advanced, Trust Advanced Plus (Trust Advanced Plus issues certificate only on HSM, SCD or SSCD.) • Registration done by applicant or the Netlock Registration Authorities • Natural persons can request this, and also it is possible to display an Organization in the corresponding certificate field. • Organisations can also request this type of certificate (seal) • Natural person also can apply for pseudonym signer certificates
Identification and authentication
Certificate can be issued cryptographic device (SCD) but its not mandatory. Identification based on the in-person presented documents.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation (Üzleti) or a notary validated agreement (Közjegyzői) and copies of documentation or copies of documentation (Expressz). (For CA Trust and Trust Advanced various combinations possible) • in person • by email or mail (notary validated agreement needed in original form) The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant • in Hungary the legislation needs governmental database validation for signer certificates, so its checked against that. If an Organization is also displayed in the certificate, then the organization is checked: • Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet If only an Organization displayed in the certificate, then the followings checked: • Authorization of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, Usage limits

It can be used for digital signing and sealing and authentication.
Normalized Certificate Policies
NCP+ - for certificates stored on SCD NCP – for certificates not stored on SCD

3.3 Authentication certificates

General information
• Issued by one of the following CA-s (Expressz, Üzleti, Közjegyzői, Trust) • Registration done by applicant or the Netlock Registration Authorities • Natural persons can request this, and also it is possible to display an Organisation in the corresponding certificate field. • Organizations can also request this type of certificate • Natural person also can apply for pseudonym signer certificates
Identification and authentication
Certificate can be issued cryptographic device (SCD) but its not mandatory. Identification based on the in-person presented documents or copies. Key escrow is recommended for the users.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation (Üzleti) or a notary validated agreement (Közjegyzői) and copies of documentation or copies of documentation (Expressz) and Trust. • in person • by email The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant If an Organization is also displayed in the certificate, then the organization is checked: • Authorization from the Organization to allow the display of the Company in the certificate.

• Official organization registration documents • Official Specimen signature sheet If only an Organization displayed in the certificate, then the followings checked: • Authorization of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, usage limits
Can be used only for authentication.
Normalized Certificate Policies
NCP+ - for certificates stored on SCD NCP – for certificates not stored on SCD LCP – for certificates requested without in-person presentation

3.4 Encryption certificates

General information
• Issued by one of the following CA-s (Expressz, Üzleti, Közjegyzői, Trust) • Registration done by applicant or the Netlock Registration Authorities • Natural persons can request this, and also it is possible to display an Organisation in the corresponding certificate field. • Organizations can also request this type of certificate • Natural person also can apply for pseudonym signer certificates
Identification and authentication
Certificate can be issued cryptographic device (SCD) but its not mandatory. Identification based on the in-person presented documents or copies. Key escrow is recommended for the users.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation (Üzleti) or a notary validated agreement (Közjegyzői) and copies of documentation or copies of documentation (Expressz) and Trust. • in person • by email The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant If an Organization is also displayed in the certificate, then the organization is checked: • Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet If only an Organization displayed in the certificate, then the followings checked: • Authorization of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, usage limits
Can be used only for encryption
Normalized certificate policies
NCP+ - for certificates stored on SCD NCP – for certificates not stored on SCD LCP – for certificates requested without in-person presentation

3.5 Code Signing certificate

General information
• Issued by one of the following CA-s (CodeSign) • Registration done by applicant or the Netlock Registration Authorities • Natural persons can request this, but it is NOT possible to display an Organization in the corresponding certificate field. • Organizations can also request this type of certificate
Identification and authentication
Certificate can be issued cryptographic device (SCD) but its not mandatory. Identification based on the in-person presented documents or copies.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation or a notary validated agreement and copies of documentation. • in person • by email The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant If only an Organization displayed in the certificate, then the followings checked: • Authorization of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, usage limit
It can be used for Code Signing
Normalized Certificate Policies
NCP+ - for certificates stored on SCD NCP – for certificates not stored on SCD CSCP – CAB Forum non-EV CodeSign Policy; OID: 2.23.140.1.4.1

3.6 DV SSL certificates

General information
• Issued by the OnlineSSL CA • Registration done by applicant or the Netlock Registration Authorities
Identification and authentication
Identification based on technical verification.
Registration process
The user registers online, generates request, and adds a specific code to the site or domain, which can be checked by the automated system. After successful technical validations, the certificate will be issued.
Usage, usage limit
It can be used only for SSL/TLS communications.
Normalized Certificate Policies
DVCP, OID: 2.23.140.1.2.1

3.7 OV SSL certificates

General information
• Issued by one of the following CA-s (Expressz, Üzleti, Közjegyzői) • Registration done by applicant or the Netlock Registration Authorities
Identification and authentication
Identification based on the in-person presented documents or copies.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation (Üzleti) or a notary validated agreement (Közjegyzői) and copies of documentation or copies of documentation (Expressz). • in person • by email

The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant Because an Organization is also displayed in the certificate, the organization is checked: Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet • Authorization of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, usage limit
It can be used only for SSL/TLS communications.
Normalized Certificate Policy
OVCP, OID: 2.23.140.1.2.2

3.8 EV SSL certificates

General information
• Issued by one of the following CA-s (Trust EV, Qualfied Trust EV) • Registration done by applicant or the Netlock Registration Authorities
Identification and authentication
Identification based on the in-person presented documents or copies.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation or a notary validated agreement and copies of documentation or copies of documentation (for validation where applicable) • in person • by email

The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant Because an Organization is also displayed in the certificate, the organization is checked: Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet • Authorizatioln of the requestor from its organization to request certificate for them • Official organization registration documents • Official Specimen signature sheet
Usage, usage limit
It can be used only for SSL/TLS communications.
Normalized Certificate Policy
EVCP, OID: 2.23.140.1.1

4 Insurance

The provider has general reliance insurance.

4.1 Qualified signer and seal certificates with SSCD

General information
• Issued by the Qualified Legal and Qualified Legal Spec certificate authority. • Waiting for SuperVisory acceptance: TRUST Qualfied, Trust Qualified SCD, Trust Qualified QSCD • Registration done by the Netlock Registration Authorities • Signer certificate - only natural persons can request this, but it is possible to display an Organisation in the corresponding certificate field. • Seal certificate – only legal person can request this
Identification and authentication
Qualified certificate issued on SSCD for the applicant, based on the presented documents. (presentation could be in-person, trough notary, by post)
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation or a notary validated agreement and copies of documentation: • in person • by email or mail (notary validated agreement needed in original form) The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant • in Hungary the legislation needs governmental database validation for signer certificates, so its checked against that. If an Organization is also displayed in the certificate, also the organization is checked: • Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet
Usage, Usage limits
Qualified signer certificate can be used for digital signing. Qualified seal certificate can be used for digital sealing.

Normalized Certificate Policies
NCP+,QCP public SSCD, qcp-n-qscd, qcp-l-qscd

4.2 Qualified signer and seal certificates with secure device (non-SSCD)

General information
• Issued by the Qualified Legal and Qualified Legal Spec certificate authority. • Waiting for SuperVisory acceptance: TRUST Qualfied, Trust Qualified SCD, Trust Qualified QSCD • Registration done by the Netlock Registration Authorities • Signer certificate - only natural persons can request this, but it is possible to display an Organisation in the corresponding certificate field. • Seal certificate – only legal person can request this
Identification and authentication
Qualified certificate issued on secure device (which is not SSCD) for the applicant, based on the in-person presented documents.
Registration process
The Registration Authority Officer verifies the Government Issued ID presented, is valid, is connected to the requestor and have all the needed security elements. The applicant may present the original documentation or a notary validated agreement and copies of documentation: • in person • by email or mail (notary validated agreement needed in original form) The Registration and authentication process for this certificate profile includes: • Applicant in-person appearance or appearance before notary • one government ID reviewed and photocopied • one additional id with the address of applicant • in Hungary the legislation needs governmental database validation for signer certificates, so its checked against that. If an Organization is also displayed in the certificate, also the organization is checked: • Authorization from the Organization to allow the display of the Company in the certificate. • Official organization registration documents • Official Specimen signature sheet
Usage, Usage limits
This qualified signer certificate can be used for advanced signing with qualified certificates. Qualified seal certificate can be used for advanced sealing with qualified certificates.
Normalized Certificate Policies
NCP+,QCP public (with secure device), qcp-n (with secure device), qcp-l (with secure device)

5 Reliance limits

The minimum general reliance limit for certificates is 3 000 000 HUF. (not displayed in the certificates)

For qualified certificates the reliance limit set into the QcStatements/Limitvalue field which coudl be:

- 5 million HUF,
- 20 million HUF,
- 50 million HUF.

6 Retention period

The service provider kepts the issuance data (logs, documents, etc) no less than 10 years. This retention could be done trough qualfied data preservation service

7 Obligation of Subscribers

The Certificate holders are required to act in accordance of the corresponding CP/CPS and agreement.

The obligations:

- the applicant submits complete an accurate information in connection with an application for a certificate, and will update that information
- comply full with all procedures and information required for identification and authentication requirements relevant to the requested certificate.
- Promptly review, verify and accept, or reject the certificate issued if there is any miss accuracy in it.
- Secure the private key and take all reasonable precautions unauthorized uses of it
- Secure the key activation data (pin, key password, …)
- Exercise sole and complete control and use of Private key.
- Immediately notify the CA if the Private key is compromised
- Take reasonable measures to avoid the compromise of the integrity of Netlock CA.
- In case of revocation or expiration cease use of the certificate.
- Utilize the certificate in accordance of the applicable laws and regulations.
- Using the keys for its intended usage (following the included KU and EKUs)
- Discontinue the use of the certificates.

8 Certificate Status checking obligations for Relying parties

Any party receiving a signed electronic document or a signed code or using a website secured with SSL certificates need

Relying parties are obliged to seek independent assurances before any act based on that document. At minimum the following needs to be checked:

- The appropriateness of the use of certificate for the given purpose, and that purpose is not prohibited by the CP/CPS.
- The digital certificate is being used accordance with its Key Usage extensions.
- The digital certificate was not expired at the time of use.
- The digital certificate was not revoked at the time of use.
  This revocation information could be checked trough OCSP or CRL.

  All end user and intermediate certificate includes its CRL and OCSP access URLs.

9 Limitation of liability

The Netlock is not liable for any direct or indirect loss. (for example: staff time, loss of contracts)

The Netlock's has general liability insurance covers the damages came from the Netlock's faults.

The limits of reliance can be found in this PDS at the Reliance limits section.

10 General rules for fees

The provider publish general price list on its webpage, at minimum including the following items and services:

- Trust services
- Certificate issuance
- Certificate reissue
- Certificate renewalReissue of the certificate with modified data

Optional services:

- REgistration-on-GO
- Delivery of the signature deviceRequesting Corporate data from the REgistration AgencyUnblocking blocked device
- Replacement of hardware deviceSpecial fees

11 Privacy policy

Data contained in the certificates are considered public information-

Personal data obtained during the registration process will not be released without prior consent of the certificate holder, unless required by law.

12 Disputes and complaints management, resolution

Complaints are welcomed by mail, emal, phone or personaly.

When a complaint received by phone, the provider records it, and also records the results of the examination. When no other way was choosen, the provider send the results by email. The maximum time for evaluation of the resolution is 30 days, but the provider can extend it, if the problem needs more examination.

Complaints arriving by mail or by phone are handles in the same way as arreived by phone.

After the examination the provider fix the problem, if possible, and gives report about the results.

If the answer was not accepted by the Customer, disputation process starts. If this disputation is not succesful in 20 days, then its possible to continue on court.

13 Refund principles

When it's justifiable, the provider refunds the fee or the part of fee of the ordered services, on individual case basis, as it's published in General Terms

When it's justifiable, time-bound charges are refunded pro rata.

One time fees are refunded at once. Monthly fees can refunded when the loyality period was over. In this case only the part of the latest month could be refunded partialy.

14 Applicable law

The applicable law is the Hungarian law.

Dispute is possible before the Chamber of Commerce in Hungary.

.

15 Trust marks of the provider

The provider doesnot guarantee its Trademarks in the certificates. From the customers side, owning a Trade Mark doesn't means that a certificate should issued. By requesting a certificate the Requestor accepts, that ithe request should not contain any content which infringe any third party rights. The provder is not mandated to evaluate the Trade Marks.

16 Assesments of the Trust Service Provider

The Provider annualy evaluates its service, and it's service points.

The provider also follows the EU legislations, so the Supervisory Authority also audits the provider and also takes a site visit yearly.

Assesments and certifications:

- ISO 9001 (from 2001)
- BS 7799-2 (2005)
- ISO/IEC 27001 (from 2005)
- ETSI 102.042 V2.4.1 audit és az ETSI 101456 V1.4.3 audit - auditált TÜV Rheinland által

17 Trust List

As requested by the eIDAS the provider was registrated by the Supervisory Authority at: trust services for electronic transactions Its registration date: 2016. 06. 30.

Previously registration was done on 19th march 2003 . Its registration number: MH-1372-12/2003.

Data preservation service registration was done on 15th september 2010. It's registration number: HL/18188-4/2010.

18 Applicable agreements, certificate practice statement, certificate policy

The following documents are available at https://www.netlock.hu/USERHU/html/dok.html

- General terms
- Qualified CP and CPS
- Non-qualified signatory CP and CPS
- Non-qualified non signatory CP and CPS
- Time Stamping Policy and TSA PS
- E-archiving policy

The documents are available at: http://www.netlock.hu/docs/

19 Compliance with the legislation in force

The provider works as the in force legislation and standards reqiests it. The compilance with the legislation in force also proved that the Supervisor Authority published the providers CA certicicates on the EU Trust List.

The following rules and standards are currently in force: (local laws are displayed in local language)

- **eIDAS:** 910/2014/EC

- **Eüt.:** 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- **BM rendelet:** a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016 (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
- **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
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre
- Kriptográfiai hardver eszköz alkalmazását megkövetelő egységesített hitelesítési rendek:
- Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend
    - /Azonosító: [EHR+_Ü], OID: 0.2.216.1.100.42.101.3.2.1/

- Közigazgatási, köztisztviselőkhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend
    - /Azonosító: [EHR+_K], OID: 0.2.216.1.100.42.101.4.2.1/
- Kriptográfiai hardver eszköz alkalmazását nem megkövetelő egységesített hitelesítési rendek:
- Közigazgatási, ügyfélhez kapcsolódó, egységesített hitelesítési rend
    - /Azonosító: [EHR_Ü], OID: 0.2.216.1.100.42.101.5.2.1
- Közigazgatási, ügyfél által működtetett automatizmushoz kapcsolódó, egységesített hitelesítési rend
    - /Azonosító: [EHR_ÜA], OID: 0.2.216.1.100.42.101.6.2.1
- Közigazgatási, köztisztviselőkhöz kapcsolódó, egységesített hitelesítési rend
    - /Azonosító: [EHR_K], OID: 0.2.216.1.100.42.101.7.2.1
- Közigazgatási, közigazgatást képviselő automatizmushoz kapcsolódó, egységesített hitelesítési rend
    - /Azonosító: [EHR_KA], OID: 0.2.216.1.100.42.101.8.2.1
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára
- Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési Szabályzat
- General Terms– NETLOCK Ltd
- ISO 3166 English Country Names and Code Elements
- FIPS PUB 140-2
- RFC 5280 (previously RFC 3280)
- RFC 3647 (previously RFC 2527)
- International Telecommunication Union X.509 “Information technology” PKI Framework
- ETSI 102 042 v1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates
- RFC 2560 Online Certificate Status Protocol (OCSP)

- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- ETSI EN 319 412-1 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 organizations
- 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
- CSCP: Code Signing Certificate Policy (non EV), OID: 2.23.140.1.4.1
- OVCP: Organizational Validation Certificate Policy Jogi személyek SSL tanúsítványára vonatkozó Hitelesítési Rend, OID: 0.4.0.2042.1.7
- IVCP: Individual Validation Certificate Policy OID: 2.23.140.1.2.3

Any other rules can be found in the CP, CPS and in the General Terms.