certop

Certificate

Is awarded to

NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.,
as Trust Service Provider

Headquarter: *H-1101 Budapest, Expo tér 5-7.*

for the trust services below

LCP, NCP, NCP+, DVCP, IVCP, OVCP, EVCP, CSCP,
qcp-n-qscd, qcp-l-qscd, qcp-l, qcp-n, qcp-w

roots were audited in a full audit.
Hereby we certify that the roots satisfies the requirements of
ETSI EN 319 401 v2.2.1 (2018-04)
ETSI EN 319 411-1 v1.2.2 (2018-04)
ETSI EN 319 411-2 v2.2.2 (2018-04)
ETSI EN 319 412-1 v1.4.2 (2020-07)
ETSI EN 319 412-2 v2.2.1 (2020-07)
ETSI EN 319 412-3 v1.2.1 (2020-07)
ETSI EN 319 412-4 v1.1.1 (2016-02)
ETSI EN 319 412-5 v2.3.1 (2020-04)
CSCP 2.0 (2020-09)
Audit Standards were used to audit each of the roots respectively.

Audit period	2019-09-04 to 2020-09-03
Expiry Date:	2021-09-29
Registration Number:	20-00573/19-00170
Date of Issue:	Budapest, 2020-10-21

From certification authority:

- -

Dániel Serbán
CERTOP Informatikai Tanúsítási Szolgáltatások Kft.
H-1149 Budapest, Mogyoródi út 32.
www.it.certop.com

Letter of Attestation

Annex to certificate 20-00573/19-00170

AUDIT REPORT

Name of entrusting organisation:	**NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.**
Headquarter:	1101 Budapest, Expo tér 5-7.
Locations for conformity assessment	1101 Budapest, Expo tér 5-7. 1143 Budapest, Hungária krt. 17.
Start date of assessment:	2020-09-04
End date of assessment:	2020-09-29
Lead auditor:	Tamás Horváth
Co-auditors:	György Ruska, Tamás Tusor
Certification body:	Certop Informatikai Tanúsítási Szolgáltatások Kft.

Contents

1   Requirement Standards

The audit requirements are defined in the following standards:

ETSI EN 319 401 v2.2.1 (2018-04)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, Version v2.2.1, 2018-04, European Telecommunications Standards Institute

ETSI EN 319 411-1 v1.2.2 (2018-04)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Version v1.2.2, 2018-04, European Telecommunications Standards Institute

ETSI EN 319 411-2 v2.2.2 (2018-04)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, Version v2.2.2, 2018-04, European Telecommunications Standards Institute

ETSI EN 319 412-1 v1.4.2 (2020-07)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, Version v1.4.2, 2020-07, European Telecommunications Standards Institute

ETSI EN 319 412-2 v2.2.1 (2020-07)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, Version v2.2.1, 2020-07, European Telecommunications Standards Institute

ETSI EN 319 412-3 v1.2.1 (2020-07)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons, Version v1.2.1, 2020-07, European Telecommunications Standards Institute

ETSI EN 319 412-4 v1.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates, Version v1.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 412-5 v2.3.1 (2020-04)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements, Version v2.3.1, 2020-04, European Telecommunications Standards Institute

CSCP 2.0 (2020-09)
Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

2 Documentation review

The conformity assessment started with a documentation review. NETLOCK Kft. provided the relevant regulatory documents to the auditors. Examination of the documentation has shown that they meet the requirements of the standards referred to above.

List of regulatory documents:

Name of the document	Identifier (OID) / Issuance
NETLOCK Extract of the Service Practice Statements	1.3.6.1.4.1.3555.1.62. 20200618
NETLOCK General Terms and Conditions	1.3.6.1.4.1.3555.0.1.20181127
Service Policy for Qualified Certification Services	1.3.6.1.4.1.3555.1.14.20200731
Service Policy for Preservation Service	1.3.6.1.4.1.3555.1.48.20200714
Service Policy for Timestamp Service	1.3.6.1.4.1.3555.1.16.20180817
Service Policy for Non-Qualified Certification Service	1.3.6.1.4.1.3555.1.60.20200731
Service Policy for Non-eIDAS Certification Service	1.3.6.1.4.1.3555.1.65.20200731
Service Practice Statement for Qualified Certification Services	1.3.6.1.4.1.3555.1.15. 20200731
Service Practice Statement for Qualified Preservation Service	1.3.6.1.4.1.3555.1.47.20200714
Service Practice Statement for Qualified Timestamp Service	1.3.6.1.4.1.3555.1.63. 20191205
Service Practice Statement for Non-Qualified Certification Service	1.3.6.1.4.1.3555.1.59.20200731
Service Practice Statement for Non-eIDAS Certification Service	1.3.6.1.4.1.3555.1.49.20200731
RA/CA Policy	1.3.6.1.4.1.3555.3.2.20200506
Operating Regulations	1.3.6.1.4.1.3555.2.40.8.20190829
Business Continuity and Disaster Recovery Plan	1.3.6.1.4.1.3555.2.16.20190626
Security Policy	1.3.6.1.4.1.3555.2.13.20200415
Regulation of Risk Management	1.3.6.1.4.1.3555.2.11.20180817
Cryptographic hardware and lifecycle policy	1.3.6.1.4.1.3555.2.57.20190829
Staff Policy	1.3.6.1.4.1.3555.2.17.20200420
Termination Plan	1.3.6.1.4.1.3555.2.59.20190829
Backup policy	1.3.6.1.4.1.3555.2.58.20190829
Data Privacy Information	1.3.6.1.4.1.3555.1.67.20200618

3   Scope of the audit

The audit assessment of the following certificate policies were considered:

LCP	Lightweight CP
NCP	Normalized CP
NCP+	Extended Normalized CP
DVCP	Domain Validation CP
IVCP	Individual Validation CP
OVCP	Organizational Validation CP
EVCP	Extended Validation CP
CSCP	CodeSign CP
qcp-n	Qualified CP –for natural persons
qcp-l	Qualified CP –for legal persons
qcp-n-qscd	Qualified CP –for natural persons with qscd
qcp-l-qscd	Qualified CP –for legal persons with qscd
qcp-w	Qualified CP –for web site certificates

4   Audit methodology

Conformity assessment was performed by the audit team using the audit method.

Auditing: A systematic, independent, documented process for obtaining records, statements, or other relevant information about facts and evaluating them objectively to determine the extent to which necessary requirements are being met.

The objective evidence was collected by the audit team with the following techinuques:

  ➢ Documentation evaluation
  ➢ Visual inspection
  ➢ Interviewing
  ➢ Technical review

Documentation evaluation: Evaluation of policies, procedures and regulatory documents received from the organization.

Visual inspection: During the on-site audit, evaluation of the existence and application of administrative security measures and physical security protection measures.

Interviewing: Monitoring with targeted questions the activities of the persons participating in the trust services and evaluating the areas related to the processes and information security performed by them.

Technical review: Evaluation of logical protection measures and technical configuration regulations in the IT system.

The audit was performed by the audit team on the basis of a checklist issued by ETSI in a separate standard:

> ➢ ETSI TR 119 411-4 v1.1.1 (2018.05.)

5 Audit schedule

The full audit took 16 days.

Start date of the audit: 2020-09-04	End of the audit: 2020-09-29	
Documentation inspection:	2020-09-04 to 2020-09-08	3 days
Risk analysis evaluation:	2020-09-09 to 2020-09-10	2 days
On-site audit:	2020-09-11 to 2020-09-28	12 days
Audit report preparation:	2020-09-29	1 day

Description of deviations from the audit plan:

During the audit, the members of the audit team carried out the assessmnet according to the audit plan, so the audit did not deviate from the planned schedule.

6 Audit process

The audit took place at the headquater and the operational site of the NETLOCK Kft. (1101 Budapest, Expo tér 5-7. and 1143 Budapest, Hungária krt. 17.). The audit began with a documentation evaluation. Following the identification of the trust services provided by the organization and the stakeholders involved in them, the risk assessment was examined. The risk assessment was followed by a visual inspection of the physical protection measures and then a technical inspection of the logical measures, involving the persons affected the trust services. During the audit, the certificate policies and certificate policy statementes for qualified and non-qualified trust services, the related regulations, the terms and conditions and their end products, the certificates were evaluated.

Persons involved in the audit:

> ➢ Dr. Zsófia Fehér, legal adviser, head of compliance NETLOCK Kft.
> ➢ Viktor Varga, PKI expert, senior adviser
> ➢ Zoltán Kővári-Szabó, compliance manager, NETLOCK Kft.
> ➢ Éva Varga-Szabó, junior compliance manager, NETLOCK Kft.
> ➢ dr. Dóra Káli, legal clerk, NETLOCK Kft.
> ➢ Krisztina Seres, senior registration administrator, NETLOCK Kft.

7 Summary of the Trust Service Provider's information security risk assessment

The audit team assessed the risk management regulations submitted by NETLOCK Kft. and found them appropriate. During the on-site audit, the audit team reviewed the internal and external factors, stakeholders, and then evaluated the results of the organization's risk assessment, based on the received information and the on-site experience. The risk improvement plan was approved by the management and resources were allocated to the measures.

During the audit, it was established that NETLOCK Kft. manages the identified risks in accordance with its possibilities. NETLOCK Kft. uses the CARISMA risk management software, which we examined in detailes during the audit process. (The Organization is planning to replace the software, so they have started to use the ADAPTO software in parallel.)

The valid Regulation of Risk Management of NETLOCK Kft. were used in the assessment.

NETLOCK Kft., as a trust service provider, identifies and evaluates its risks annually and in case of changes as follows:

➢ Identifies foreseeable internal and external threats that may allow unauthorized access, disclosure, alteration, destruction, or other misuse of certificate data or certificate management processes.
➢ Assesses the likelihood of these threats occurring and the expected damage if they do occur.
➢ Evaluates the adequacy of the processes, protection measures and IT systems used to address the identified threats.

8 Findings, results and non-conformities

The conformity assessment found that the trust services are performed in accordance with the trust policies established in accordance with the requirements described in the identified standards.

During the audit, non-conformity was not recorded by the audit team.

Further audit evidences are in the audit records.

ETSI EN 319 401 V2.2.1 (2018-04)

Risk Assessment	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
TSP has a comprehensive risk management practice.			

Policies and practices	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
TSP specify the set of policies and practices for the operation required. The defined policies make it available to everyone on the TSP's website. The TSP prepared and enforces security policies approved by the top management.			

TSP management and operation			
Internal organization	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP presented the evidences of the reliable operation. The proper segregation of duties and responsibilities ensure to reduce the opportunities of unauthorized or unintentional modification or misuse assets-			
Human resources	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has appropriate staff and contractors to support its trustworthiness operations.			
Asset management	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP introduced appropriate level of protection of its assets including information assets.			
Access control	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP's system access is limited to authorized individuals.			
Cryptographic controls	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has the appropriate regulations and enforce them during the managing of cryptographic keys and any cryptographic devices.			
Physical and environmental security	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has adequate physical security controlls in place.			
Operation security	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP uses trustworthy systems that are protected against modification and ensure the technical security and reliability of supported the processes.			
Network security	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP protect its network and systems from attacks.			
Incident management	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
System activities concerning access to IT systems, use of IT systems, and service requests are monitored.			

Collection of evidence	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has sufficiently detailed audit entries on components in providing the services.			

Business continuity management	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has sufficient business continuity and disaster recovery plans.			

TSP termination and termination plans	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP documents in details and makes available procedures and plans relating to the cessation of its services.			

Compliance	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP operates in a legal and trustworthy manner.			

ETSI EN 319 411-1 V1.2.2 (2018-04) és ETSI EN 319 411-2 V2.2.2 (2018-04)

General provisions on Certification Practice Statement and Certificate Policies			

General requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The details of controls met an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a TSP can employ in issuing certificates.			

CPS requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP prepared and enforces security policies approved by top management.			

CP name and identification	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.			

PKI participants	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The CA is identified in the certificate as the issuer and its private key is used to sign certificates.			

Certificate usage	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐

The policies NCP, NCP+ and LCP place no constraints on the user community and applicability of the certificate, however the other CPs.

TSP practice			
Publication and repository responsibilities	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP makes the certificates available to subscribers, subjects and relying parties.			
Identification and authentication	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP verifies the identity of the subscriber and subject and check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of the identity.			
Certificate Life-Cycle operational requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP issues certificates securely to maintain their authenticity.			
Facility, management, and operational controls	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP prepared and enforces security policies approved by the top management. The TSP implemented proper controlls to protect the physical and information assets.			
Technical security controls	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has the proper regulations and enforces them in asset management processes.			
Certificate, CRL, and OCSP profiles	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates met the requirements, specified in recommendation X.509.			
Compliance audit and other assessment	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The organization issues certificates compliant with the requirements of relevant requirements.			
Other business and legal matters	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP has the proper regulations for the other business and legal matters (e. g. privacy and warranty).			
Other provisions	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐

The TSP provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

Framework for the definition of other certificate policies			
CP management	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The authority issuing a CP other than the ones defined in clause 5 demonstrate that the CP is effective.			
Additional requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Subscribers and relying parties are informed ont he proper way.			

ETSI EN 319 412 family

ETSI EN 319 412 certificate profiles	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
All the certificate profiles specified in ETSI EN 319 412.			

ETSI EN 319 412-1 v1.4.2 (2020-07)

Common data structures			
Semantics identifiers	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Subject and issuer names include attributes that do not disclose the semantics of its information content.			
Certificate Extensions regarding Validity Assured Certificate	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates are compliant with the standard.			

ETSI EN 319 412-2 v2.2.1 (2020-07)

General certificate profile requirements			
Generic requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
All certificate fields and extensions are compliant with IETF RFC 5280.			
Basic certificate fields	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐

All the basic fields are compliant with the standard requirements.			
Standard certificate extensions	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The standard extensions are used according to the standard requirements.			
IETF RFC 5280 internet certificate extensions	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The Authority Information Access extension is available.			

EU qualified certificate requirements			
EU QCStatements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
EU qualified certificates include QCStatements in accordance with ETSI EN 319 412-5			
Certificate policies	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
EU qualified certificates include, in the certificate policies extension, one of the certificate policy identifiers defined in the ETSI EN 319 411-2.			

ETSI EN 319 412-3 v1.2.1 (2020-07)

Profile requirements			
Generic requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
All certificate fields and extensions comply with ETSI EN 319 412-2.			
Basic certificate fields	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The subject field include at least the following attributes: ➢ countryName; ➢ organizationName; ➢ organizationIdentifier; ➢ commonName.			
Standard certificate extensions	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates are compliant with the standard.			

319 412-4 v1.1.1 (2016-02)

Profile requirements			

Generic requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates are compliant with the standard.			

EU Qualified Certificate statements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
EU Qualified Certificates includes QCStatements as specified in ETSI EN 319 412-5.			

Certificate policies	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates are compliant with the standard.			

319 412-5 v2.3.1 (2020-04)

Qualified certificate statements			
General requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Defined number of individual QCStatements are included in the QCStatements extension.			
QCStatements claiming compliance with the EU legislation	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Certificates are compliants with the EU legislations.			
Generic QCStatements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
QCStatement declares a limitation on the value of transaction for which a certificate can be used.			

Requirements on QCStatements in EU qualified certificates			
Generic requirements	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Specified EU qualified certificates include QCStatements.			

CSBR 2.0 (2020-09)

Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates			
Certificate Warranties and Representations	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐

The TSP'S policies contain the necessary warranties.			
Community and Applicability	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP's operation is compliant with laws, regulatory requirements and related standards.			
Certificate Content and Profile	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificates are compliant with the requirements.			
Certificate Request	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The certificate request processes are defined in the TSP's policies.			
Verification Practices	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The verification processes are defined in the TSP's policies.			
Certificate Issuance by a Root CA	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Only the trusted persons of the TSP's staff can execute these type of processes.			
Certificate Revocation and Status Checking	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The revocation and status checking processes are defines in the TSP's policies.			
Employees and Third Parties	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
Only trustworthy persons (employees or contractors) are involved in the trust services.			
Data Records	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
All the necessary logs created.			
Data Security and Private Key Protection	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
All the necessary physical and logical safeguards are applied.			
Audit	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐
The TSP is audited regularly according to the relevant ETSI standards.			
Liability and Indemnification	Yes	Part of	No
Meets the standard requirements.	☑	☐	☐

The TSP is compliant with the BR requirements.

9 Evaluated profiles

List of profiles reviewed the audit, according to the requiremented standard.

Type of the profiles	Standard that describes the profile		Fulfill the requirement		
			Yes	Part of	No
Personal	ETSI EN 319 412-2	For natural persons	☑	☐	☐
Organizational	ETSI EN 319 412-3	For legal perons, organizations	☑	☐	☐
SSL web	ETSI EN 319 412-4	For web certifications	☑	☐	☐
QCStatements (qualified personal)	ETSI EN 319 412-5	Profiles completed with Qualified Certificate Statements	☑	☐	☐
Code signing	CSBR 2.0	For code signing	☑	☐	☐

The audit covered the following certifications:

Short name in the structure	Full name	CA availability	Fingerprint
SHA2 GOLD	NetLock Arany (Class Gold) Főtanúsítvány	www.NetLock.hu/index.cgi?ca=gold	6C61DAC3A2DEF031506BE036D2A6FE401994FBD13DF9C8D466599274C446EC98
SHA2 PLATINUM	NetLock Platina (Class Platinum) Főtanúsítvány	www.NetLock.hu/index.cgi?ca=platinum	EB7E05AA58E7BD328A282BF8867033F3C035342B516EE85C01673DFFFFBBFE58
TRUSTADV+	NETLOCK Trust Advanced Plus CA	www.NetLock.hu/index.cgi?ca=trustap	F2603670BEDEAD1D977D6992FA6554E6CA595BC50F3B03F416DCF0F20DAC36C2
TRUSTADV	NETLOCK Trust Advanced CA	www.NetLock.hu/index.cgi?ca=trusta	D82F87F93D31D5FC818DD66BD50E7F319AE179FC1C5D00547B658E8EB3F4CE56
TRUST	NETLOCK Trust CA	www.NetLock.hu/index.cgi?ca=trust	58D7A197F09A6EA552B8EA6B1A53185A030A3AD8D52220C00C44E3F450E4FB90
TRUSTSSL (revoked)	NETLOCK Trust SSL CA	www.NetLock.hu/index.cgi?ca=trustssl	0A778BF9DD7F75B2F983FB7FA705C987CCCB5877404BE7EB5D8BA0B73545D0D9
TRUSTEV (revoked)	NETLOCK Trust EV CA	www.NetLock.hu/index.cgi?ca=trustev	A476FE1FBFEBA08175A0C34807990B86E63B5AA2D6CE579C4F456C95575BB1F6
TRUSTEV2 (revoked)	NETLOCK Trust EV CA 2	www.NetLock.hu/index.cgi?ca=trustev2	CD0CC3A6F6857D427D6D98F6BF877E0845E365C5BAC61C9BAF27AE0AC3681A57
TRUSTEV3	NETLOCK Trust EV CA 3	www.NetLock.hu/index.cgi?ca=trustev3	047795785CDCFF9E6E0AE122492E5B7BF08A9E5C49762E2BCB52747C69031561
CODESIGNCA	NetLock CodeSign CA	www.NetLock.hu/index.cgi?ca=codesignca	C56F0F286618C1E7B0E112C97B9EE96FEB4D71E79496C151FA1FE8A8CEBD06CD

Short name in the structure	Full name	CA availability	Fingerprint
QTRUSTQSCD	NETLOCK Trust Qualified QSCD CA	www.NetLock.hu/index.cgi?ca=qtrustqscd	9E4362A918A89009877C7B8B190E763AE012AD47C1CCA5FCCF166FC092BC2ADE
QTRUSTSCD	NETLOCK Trust Qualified SCD CA	www.NetLock.hu/index.cgi?ca=qtrustscd	7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711
QTRUST	NETLOCK Trust Qualified CA	www.NetLock.hu/index.cgi?ca=qtrust	5498963DFFA651604F467E108E65A183470FA9B557C129DDF8C9D812B4F0BF96
QTRUSTEV (revoked)	NETLOCK Trust Qualified EV CA	www.NetLock.hu/index.cgi?ca=qtrustev	B0F25A6D9A96315C7CDAEA3E490E7BFA9FB17310B0701B7CD6FF432530837730
QTRUSTEV2 (revoked)	NETLOCK Trust Qualified EV CA 2	https//www.netlock.hu/index.cgi?ca=qtrustev2	36EFD13AE5DC6D01B6C1956841B45D18CE8085FBC197D90E8A8A21A9B01EBFBA
QTRUSTEV3	NETLOCK Trust Qualified EV CA 3	https//www.netlock.hu/index.cgi?ca=qtrustev3	7ECACA4A3585A3B40E25574415512D56B57999B753017856F2AB15FA1F21F6D0
SHA2 Q EAT	NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cqlca	6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E
SHA2 QS EAT	NetLock Minősített Eat. (Class Q Legal S) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cqlsca	A5F2FD0D66DB4DD77A2914ED3C747CBD97E734CF4E2B6F217FB41AA4EAFDEAD2
SHA2 A EAT	NetLock Közjegyzői Eat. (Class A Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=calca	AD47883A48C86A3469E32C972B39A3EE155804D32BF53FF002000BCA11D295D9
SHA2 B EAT	NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cblca	1D93686CA42C70394FBDC2BC1F98461D19871C2A00078B815499312ED9F6FE0C

Short name in the structure	Full name	CA availability	Fingerprint
SHA2 C EAT	NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cclca	BB661D750C53166181807A6898FD464065CE59298986AD66D9D6FFFCBBD4738A
SHA2 A	NetLock Közjegyzői (Class A) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=caca	75894D4C94C22D7296EE19FB447623258C2591B17031288BB386A20AA1F0E0A
SHA2 B	NetLock Üzleti (Class B) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cbca	6B23FAD890180C337B864155DAE0DE9BAD9EF0BDA78D112F2CBDC3D02AD17956
SHA2 C	NetLock Expressz (Class C) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=ccca	372B8F4CE73BEDFC88718C407BB6B3E6D8F9A79BE957190D0E7101C7B0EF9A32
SHA2 MKB EAT (revoked)	MKB Tanúsítványkiadó	http://crl.mkb.hu/CA4.crt	E53A9D8C0046C6366D3C6A18E23B4F4CBAAADB7D79B8C2F18786821DEE046AF3
MKB 5 SUBCA (renewed)	MKB SubCA 5	http://crl.mkb.hu/MKBSubCA5.crt	BC81F4A347BCBE1D53AF1C71B0D7E403246389D7465D5296D3B963AB208C2080
SHA2 MNB EAT (expired)	MNB Eat. Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	878EF628267A15493D2BD9B1BA12311874680BD8E1C4F04A8B369241DB034DFA
SHA2 KELER EAT (revoked)	KELER Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	73C27704C3B312807D18155B3AD06907DC9A374B66FBEDC2BC2973031A6BE988
SHA1 QA	NetLock Minositett Kozjegyzoi (Class QA) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=mshea	E606DDEEE2EE7F5CDEF5D9058FF8B7D0A9F042877F6A171ED8FF6960E4CC5EA5
SHA2 MNB	MNB Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	4A3BB05DB15EE3BE9774206B8B6AFE229C6F7C87C3A5CFA08861568EBDCE7DB3

Short name in the structure	Full name	CA availability	Fingerprint
SHA2 KELER (revoked)	KELER Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	E2723FB2591671774DE5EF80BEC656A7AF01F3B24067AF269EE35301891AC51
SHA1 A	NetLock Kozjegyzoi (Class A) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=kozjegyzoi	7F12CD5F7E5E290EC7D85179D5B72C20A5BE7508FFDB5BF81AB9684A7FC9F667
SHA1 B	NetLock Üzleti (Class B) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=uzleti	39DF7B682B7B938F84715481CCDE8D60D8F22EC598877D0AAAC12B59182B0312
SHA1 C	NetLock Expressz (Class C) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=expressz	0B5EED4E846403CF55E065848440ED2A82758BF5B9AA1F253D4613CFA080FF3F
SHA2 OnlineSSL	NETLOCK OnlineSSL Tanúsítványkiadó	http//www.netlock.hu/index.cgi?crl=olsslgca	A4C463FAA16CC470A829B058058F1E3DFA8B839797B3861819F75807CAF1F02C
PDVCA	NETLOCK Domain Validated CA	http//www.netlock.hu/index.cgi?ca=pdvca	A1663E37B8992D819C69FB89707065CABDFE3D53C278FC3EC2601001798602F8
SHA2 KGYHSZ	KGYHSZ (Publikus Admin Tanúsítvány CA - Magyarország) Kormányzati tanúsítvány Magyarország, nem a NetLock tulajdona.	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer	833492D73A6CF4E319C59F358D37DFB55198ED38A98890FE471091F4E3DF2720
SHA2 KI Q	NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó	https://www.NetLock.hu/index.cgi?ca=mkozig256	EBA22784D20902A9F9AF3F640D14889A53D7F3C4B5B0697016B8D749ADE97F3E

Short name in the structure	Full name	CA availability	Fingerprint
SHA2 KI B	NetLock Közigazgatási Üzleti (Class B) Tanúsítványkiadó	https://www.NetLock.hu/index.cgi?ca=bkozig256	F7F8CD8A0BCFEF0376B4DE06904BD4F179BF3B54257FCF305CDCCF7ED7F3524