

Letter of Attestation

Annex to certificate 20-00404/16-00117



1 / 15

AUDIT REPORT

Comissioned name of organisation:	NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.
Headquarter:	1101 Budapest, Expo tér 5-7.
The appropriate location for conducting a performance review:	1101 Budapest, Expo tér 5-7.
Start date of review:	2016.09.14.
End date of review:	2016.10.05.
Lead auditor:	Tamás Horváth
Co-auditor:	Gyula Gali
Evaluation of subcontractors involved:	Certop Informatikai Tanúsítási Szolgáltatások Kft.
Certification:	Certop Termék- és Rendszertanúsító Kft.

Content

1	Requirement Standards	2
2	Documentation review.....	3
3	Summary of the Trust Service Provider's information security risk assessment	4
4	Scope of the audit.....	4
5	Audit methodology	5
6	Audit time schedule.....	6
7	Process of the audit	6
8	Findings, results and non-conformities	7
9	Evaluated profiles	13

Letter of Attestation

Annex to certificate 20-00404/16-00117



2 / 15

1 Requirement Standards

The audit requirements are defined in the following standard specifications:

ETSI EN 319 401 v2.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, Version v2.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 411-1 v1.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Version v1.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 411-2 v2.1.1 (2016-02)

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 v2.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 412-1 v1.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, Version v1.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 412-2 v2.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, Version v2.1.1, 2016-02, European Telecommunications Standards Institute

ETSI EN 319 412-3 v1.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons, Version v1.1.1, 2016-02, 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 v2.1.1 (2016-02)

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements, Version v2.1.1, 2016-02, European Telecommunications Standards Institute

Letter of Attestation

Annex to certificate 20-00404/16-00117



3 / 15

2 Documentation review

The conformity assessment started with documentation review. Netlock Kft. made available to audit team the relevant ETSI standards complies with the requirements of content control documents. During the review of documents established that they meet the requirements of the standards referred to above.

List of control documents:

Name of the document	Identifier
NetLock Certificate Policy for non-qualified certifications	1.1
NetLock service regulation for non-qualified certifications	1.3.6.1.4.1.3555.1.59.20160902
Certified and Time-stamping Policy	1
Qualified Service Regulation	1.3.6.1.4.1.3555.1.50.20150921
Quality Management Manual	1.3.6.1.4.1.3555.2.02.20160323
Safety Regulation	1.3.6.1.4.1.3555.2.13.20160414
Personnel Policy	1.3.6.1.4.1.3555.2.17.20150526
Conditions of Acceptance Unit Operating Regulation	1.3.6.1.4.1.3555.2.42.20150413
General terms and conditions	1.3.6.1.4.1.3555.0.1.20160902
Singing certificate policy	1.3.6.1.4.1.3555.1.14.20080206
NCA reliable system of certification service Security Regulation	1.0
NetLock Kft. outsourced service provider operating at Keler Zrt. service regulation	1.3.6.1.4.1.3555.1.51.20160630
Qualified certificate revocation lists and time-stamps profiledefinitions	1.3.6.1.4.1.3555.1.24.20050815
NetLock Kft. outsourced service provider operating at MKB service regulation	1.3.6.1.4.1.3555.1.43.20160630
NetLock Kft. outsourced service provider operating at MNB service regulation	1.3.6.1.4.1.3555.1.13.20160630
NetLock Kft. qualified certification service and non-qualified trust service Rules Extracts	1.3.6.1.4.1.3555.1.62.20160902
NetLock Sign service availability Regulations	1.3.6.1.4.1.3555.1.58.20160530
NetLock Sign service Regulations	1.3.6.1.4.1.3555.1.57.20160630
Terms of Service for NetLock Kft. Qualified certification service and non-qualified trust service	1.3.6.1.4.1.3555.1.62.20160902
Service contracts for non-qualified trust service provided advanced certificate	1
Confidentially handle principle of personal datas	1.3.6.1.4.1.3555.1.4.151204
Encryption, authentication and DV SSL certificate provided Service Regulation	1.3.6.1.4.1.3555.1.49.20160728

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

The audit team evaluated the Risk Assessments Regulation provided by the NetLock Kft. and found to be appropriate. During the on-site audit, the audit team reviewed the internal and external factors, interested parties, then started from the information received and on-site experienced evaluated the results of the organisation's risk assessment. The risk improvement plan approved by the leadership, resources allocated to the measures.

During the audit it was found that the NetLock Kft. adequately handle the risks identified in relation to the potential.

The documents used in risk management rating is the current Risk Management Regulation owns by the NetLock Kft.

NetLock Kft. as trusted service provider shall identify and evaluate the risks as follows in annual:

- Identify the foreseen internal and external threats, which may allow the certificate datas or certificate management processes unauthorized access, disclosure, alteration, destruction or other abuse.
- It discovers these threats and the expected probability of occurrence in the event of damage.
- Evaluate the processes used to eliminate the identified threats, security measures and systems are appropriate.

4 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

5 Audit methodology

The conformity assessment performed the audit team auditing method.

Auditing: Systematic, independent, documented process facts on records, claims or other important informations acquisition and their objective evaluation in order to determine to what extent the requirements are met.

The objective evidence collected by the audit team with the following techniques:

- Documentation evaluation
- Visual inspection
- Interviewing
- Technical review

Documentation evaluation: Policies from the organization, certificate policies and evaluation of regulatory documents.

Visual inspection: During the on-site audit on the basis of administrative security measures and physical security protection measures in existence and application of visual assessment of audit along the route.

Interviewing: Observation persons involved in the certificate policies and in the process they have done, evaluation in targeted areas of assessment issues related to information security.

Technical review: The logical security provisions, technical configuration regulations evaluation of the IT system.

The audit was conducted by the audit team checklists published by ETSI:

- EN319411-1v111-checklist.xlsx
- EN319411-2v211-checklist.xlsx

In addition, the ETSI EN 319 401 and ETSI EN 319 412 standards checklist produced were used in the course of the audit:

- Checklist_ETSI_319401.docx
- Checklist_ETSI_319412.docx

During the audit examination of the ETSI EN 319 41x standards and compliance with ETSI compliance as well as 102 042 and ETSI 101 456 standards have been met, which confirm this report provides.

Letter of Attestation

Annex to certificate 20-00404/16-00117



6 / 15

6 Audit time schedule

The full audit took 14 days. The risk analysis assessment requirements described in ETSI 319411-1 consideration of section 7.1.

Start date of the audit: 2016.09.14.		End of the audit: 2016.10.05.
Documentation inspection:	2016.09.14.-09.16.	3 days
Risk analysis evaluation:	2016.09.19.-09.20.	2 days
On-site audit:	2016.09.21.-09.30.	8 days
Audit report preparation:	2016.10.05.	1 day

Description of the changes to the audit plan:

During the audit, the audit team members worked in accordance with the audit plan, so the audit did not differ from the planned schedule.

7 Process of the audit

The audit took place the headquarter of the NetLock Kft. 1101 Budapest, Expo tér 5-7. IT began with documentation and followed the interviewing people involved in the trust services. The identification of stakeholders and confidence in trust services offered by the organization and after the examination of the risk assessment. The risk assessment was followed by visual inspection of the physical protection measures, and technical measures to control this logic. In the audit evaluated qualified and non-qualified trust services made in Certificate Policies and related regulations, service processes of terms and conditions and their end products to certificate profiles were evaluated.

Persons involved in the audit:

- Imre Madarász, manager, NetLock Kft.
- János Almási, product development leader, NetLock Kft.
- Dr. Katalin Szűcs, policy leader, NetLock Kft.
- Viktor Varga, chief architect, senior PKI specialist, NetLock Kft.
- Dr. Anett Barabás, official officer, internal auditor NetLock Kft.
- Katalin Varga, deputy authentication lead, NetLock Kft.

Letter of Attestation

Annex to certificate 20-00404/16-00117



7 / 15

8 Findings, results and non-conformities

The audit report by TRI/ISU/2/2015 issued on 2015.10.22. did not reveal any non-conformity.

During the conformity assessment, according to requirements described in the identified standards carried out by the certificate policies performed trust services.

ETSI EN 319 401 V2.1.1 (2016-02)

Risk Assessment	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CA has comprehensive risk management.			

Policies and practices	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CA specify the set of policies and practices for the operation required. The defined policies make it available to everyone on the CA website. The CA has prepared and enforces security policies approved by higher management.			

TSP management and operation	Yes	Part of	No
<i>Internal organization</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA organization aspects of work reliably and specific duties and entitlements separates. The CA in it's internal regulations and external partners in contracts concluded with ensuring compliance with regulations established by the CA.			
<i>Asset management</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has introduced appropriate level of protection of its assets including information assets.			
<i>Access control</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA's system access are limited to authorized individuals.			
<i>Cryptographic controls</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has the appropriate regulations and enforce compliance with them in the managing of security devices.			
<i>Physical and environmental security</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has adequate physical security environment.			

Letter of Attestation

Annex to certificate 20-00404/16-00117



8 / 15

<i>Operation security</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA use trustworthy systems that are protected against modification and ensure the technical security and reliability of the processes supported by them.			
<i>Network security</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA protect its network and systems from attack.			
<i>Incident management</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System activities concerning access to IT systems, use of IT systems, and service requests are monitored.			
<i>Collection of evidence</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has sufficiently detailed audit entries on components in providing the service.			
<i>Business continuity management</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has sufficient detail and content business continuity and disaster recovery plan.			
<i>TSP termination and termination plans</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA document in detail and make available procedures and plans relating to the expiry of the contract.			
<i>Compliance</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA operates in a legal and trustworthy manner.			

ETSI EN 319 411 V2.1.1 (2016-02)

General provisions on Certification Practice Statement and Certificate Policies			
<i>General requirements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The details of controls met an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a CA can employ in issuing certificates.			
<i>CPS requirements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has prepared and enforces security policies approved by higher management.			

Letter of Attestation

Annex to certificate 20-00404/16-00117



9 / 15

<i>CP name and identification</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.			
<i>PKI participants</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA is identified in the certificate as the issuer and its private key is used to sign certificates.			
<i>Certificate usage</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The policies NCP, NCP+ and LCP place no constraints on the user community and applicability of the certificate, however the other CPs.			

TSP practice			
<i>Publication and repository responsibilities</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CA make certificates available to subscribers, subjects and relying parties.			
<i>Identification and authentication</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA verify 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 identity.			
<i>Certificate Life-Cycle operational requirements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA issue certificates securely to maintain their authenticity.			
<i>Facility, management, and operational controls</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has prepared and enforces security policies approved by higher management. The CA implemented to protect the physical and informatics asset items.			
<i>Technical security controls</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA has the proper regulations and enforces them in asset management process.			

Letter of Attestation

Annex to certificate 20-00404/16-00117



<i>Certificate, CRL, and OCSP profiles</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The certificates met the requirements, specified in Recommendation ISO/IEC 9594-8 or IETF RFC 5280.			
<i>Compliance audit and other assessment</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The organization issued certificates compliance the requirements of standards requirements.			
<i>Other business and legal matters</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Under this section, there are not meant to imply any restrictions on charging for CA services.			
<i>Other provisions</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The CA provide the capability to allow third parties to check and test all the certificate types that the CA issues.			

Framework for the definition of other certificate policies			
<i>CP management</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The authority issuing a CP other than the ones defined in clause 5 demonstrate that the CP is effective.			
<i>Additional requirements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Subscribers and relying parties are informed, as part of implementing the requirements defined in clause 6.9.4, of the ways in which the specific policy adds to or further constrains the requirements of the CP.			

Letter of Attestation

Annex to certificate 20-00404/16-00117



11 / 15

ETSI EN 319 412 V2.1.1 (2016-02)

ETSI EN 319 412 certificate profiles	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All the certificate profiles specified in ETSI EN 319 412.			

Common data structures			
<i>Semantics identifiers</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Subject and issuer names include attributes that do not disclose the semantics of its information content.			

General certificate profile requirements			
<i>Generic requirements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All certificate fields and extensions shall comply with IETF RFC 5280.			
<i>Basic certificate fields</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The authentication key identifier is available and includes the issuing CA's public key is a key identifier.			
<i>IETF RFC 5280 internet certificate extensions</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The Authority Information Access extension is available. Include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA.			

EU qualified certificate requirements			
<i>EU QCStatements</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EU qualified certificates include QCStatements in accordance with ETSI EN 319 412-5.			
<i>Certificate policies</i>	Yes	Part of	No
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EU qualified certificates include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.2 of ETSI EN 319 411-2.			

Letter of Attestation

Annex to certificate 20-00404/16-00117



12 / 15

Profile requirements			
	Yes	Part of	No
<i>Generic requirements</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All certificate fields and extensions comply with ETSI EN 319 412-2 with the amendments.			
<i>Basic certificate fields</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The subject field include at least the following attributes: <ul style="list-style-type: none"> ➤ countryName; ➤ organizationName; ➤ organizationIdentifier; ➤ commonName. 			

Qualified certificate statements			
	Yes	Part of	No
<i>General requirements</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Defined a number of individual QCStatements are included in the QCStatements extension.			
<i>QCStatements claiming compliance with the EU legislation</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Meet all requirements that certificate, which contains the QCStatements statement.			
<i>Generic QCStatements</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
QCStatement declares a limitation on the value of transaction for which a certificate can be used.			

Requirements on QCStatements in EU qualified certificates			
	Yes	Part of	No
<i>Generic requirements</i>			
Meets the standard requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specified EU qualified certificates include QCStatements.			

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

Further audit evidence are in the audit report.

Letter of Attestation

Annex to certificate 20-00404/16-00117



13 / 15

9 Evaluated profiles

List of profiles reviewed the audit, according to the requirement 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Organizational	ETSI EN 319 412-3	For legal persons, organizations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSL web	ETSI EN 319 412-4	For web certifications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
QCStatements (qualified personal)	ETSI EN 319 412-5	Profiles completed with Qualified Certificate Statements	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The audit covered the following certifications:

Short name in the structure	Full name	CA availability	CRL availability
SHA2 GOLD	NetLock Arany (Class Gold) Főtanúsítvány	www.NetLock.hu/index.cgi?ca=gold	www.NetLock.hu/index.cgi?crl=gold
SHA2 PLATINUM	NetLock Platina (Class Platinum) Főtanúsítvány	www.NetLock.hu/index.cgi?ca=platinum	www.NetLock.hu/index.cgi?crl=platinum
TRUSTADV+	NETLOCK Trust Advanced Plus CA	www.NetLock.hu/index.cgi?ca=trustap	www.NetLock.hu/index.cgi?crl=trustap
TRUSTADV	NETLOCK Trust Advanced CA	www.NetLock.hu/index.cgi?ca=trusta	www.NetLock.hu/index.cgi?crl=trusta
TRUST	NETLOCK Trust CA	www.NetLock.hu/index.cgi?ca=trust	www.NetLock.hu/index.cgi?crl=trust
TRUSTEV	NETLOCK Trust EV CA	www.NetLock.hu/index.cgi?ca=trustev	www.NetLock.hu/index.cgi?crl=trustev
QTRUSTQSCD	NETLOCK Trust Qualified QSCD CA	www.NetLock.hu/index.cgi?ca=qtrustqscd	www.NetLock.hu/index.cgi?crl=qtrustqscd
QTRUSTSCD	NETLOCK Trust Qualified SCD CA	www.NetLock.hu/index.cgi?ca=qtrustscd	www.NetLock.hu/index.cgi?crl=qtrustscd
QTRUST	NETLOCK Trust Qualified CA	www.NetLock.hu/index.cgi?ca=qtrust	www.NetLock.hu/index.cgi?crl=qtrust

Letter of Attestation

Annex to certificate 20-00404/16-00117



14 / 15

QTRUSTEV	NETLOCK Trust Qualified EV CA	www.NetLock.hu/index.cgi?ca=qtrustev	www.NetLock.hu/index.cgi?crl=qtrustev
SHA2 Q EAT	NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cqlca	www.NetLock.hu/index.cgi?crl=cqlca
SHA2 QS EAT	NetLock Minősített Eat. (Class Q Legal S) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cqlsca	www.NetLock.hu/index.cgi?crl=cqlsca
SHA2 A EAT	NetLock Közjegyzői Eat. (Class A Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=calca	www.NetLock.hu/index.cgi?crl=calca
SHA2 B EAT	NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cblca	www.NetLock.hu/index.cgi?crl=cblca
SHA2 C EAT	NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cclca	www.NetLock.hu/index.cgi?crl=cclca
SHA2 A	NetLock Közjegyzői (Class A) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=caca	www.NetLock.hu/index.cgi?crl=caca
SHA2 B	NetLock Üzleti (Class B) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=cbca	www.NetLock.hu/index.cgi?crl=cbca
SHA2 C	NetLock Expressz (Class C) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=ccca	www.NetLock.hu/index.cgi?crl=ccca
SHA2 MKB EAT	MNB Tanúsítványkiadó	http://crl.mkb.hu/CA4.crt	http://crl.mkb.hu/CA4.crl
SHA2 MNB EAT	MNB Eat. Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	http://cdp.mnb.hu/LHSZ1.crl
SHA2 KELER EAT	KELER Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	http://www.keler.hu/crl/lhsz2.crl
SHA1 QA	NetLock Minositett Kozjegyzoi (Class QA) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=mshea	www.NetLock.hu/index.cgi?crl=mshea
SHA2 MNB	MNB Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	http://cdp.mnb.hu/LHSZ1.crl
SHA2 KELER	KELER Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	http://www.keler.hu/crl/lhsz2.crl
SHA1 A	NetLock Kozjegyzoi (Class A) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=kozjegyzoi	www.NetLock.hu/index.cgi?crl=kozjegyzoi
SHA1 B	NetLock Üzleti (Class B) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=uzleti	www.NetLock.hu/index.cgi?crl=uzleti
SHA1 C	NetLock Expressz (Class C) Tanúsítványkiadó	www.NetLock.hu/index.cgi?ca=expressz	www.NetLock.hu/index.cgi?crl=expressz

Letter of Attestation

Annex to certificate 20-00404/16-00117



15 / 15

SHA1 MKB	NetLock CA irányított az MKB Bank felé, Magyarország	already archived	already archived
SHA1 MNB	NetLock CA irányított az MKB Bank felé, Magyarország	already archived	already archived
SHA1 OnlineSSL	NetLock OnlineSSL Hitelesítő Alegység	already archived	already archived
SHA1 KGYHSZ	KGYHSZ (Publikus Admin Tanúsítvány CA - Magyarország) Kormányzati tanúsítvány Magyarország, nem a NetLock tulajdona.	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.cer	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20060719.crl
SHA1 KIQA	NetLock Minosított Kozjegyzoi (Class QA) Tanusitvanykiado	https://www.NetLock.hu/index.cgi?ca=mkozig	https://www.NetLock.hu/index.cgi?crl=mkozig
SHA1 KI A	NetLock (Class A) Közigazgatási Tanúsítványkiadó	already archived	already archived
SHA1 KI B	(NetLock (Class B) Közigazgatási Tanúsítványkiadó)	https://www.NetLock.hu/index.cgi?ca=bkozig	https://www.NetLock.hu/index.cgi?crl=bkozig
SHA2 KGYHSZ	KGYHSZ (Publikus Admin Tanúsítvány CA - Magyarország) Kormányzati tanúsítvány Magyarország, nem a NetLock tulajdona.	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.crl
SHA2 KI Q	NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó	https://www.NetLock.hu/index.cgi?ca=mkozig256	https://www.NetLock.hu/index.cgi?crl=mkozig256
SHA2 KI B	NetLock Közigazgatási Üzleti (Class B) Tanúsítványkiadó	https://www.NetLock.hu/index.cgi?ca=bkozig256	https://www.NetLock.hu/index.cgi?crl=bkozig256