

AUDIT REPORT (TRI/ISU/1/2015, 15/10/2015)

Audit Requirements

The audit requirements are defined in the technical specification ETSI TS 102 042: ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates", Version 2.4.1, 2013-02, European Telecommunications Standards Institute, with reference to CA/BROWSER FORUM Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0.

The applicable ETSI certification policies are: **NCP, NCP+, DVCP, OVCP**

The audit object is the following Netlock's Certification Authority services:

- Issuing and management of qualified digital signature certificates (NCP+)
- Issuing and management of digital signature certificates (NCP, NCP+)
- Issuing and management of SSL Server Certificates (DVCP, OVCP)
- Issuing and management of encryption Certificates (NCP, NCP+)
- Issuing and management of authentication Certificates (NCP, NCP+)
- Issuing and management of CodeSigning Certificates (Non-EV) (NCP, NCP+)

Audit result:

The audit object fulfils all applicable requirements from the audit criteria, as detailed in TRI/ISU/1/2015, 15/10/2015.

- All requirements for a CA Practice according to chapter 7 of the rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policies (NCP, NCP+, DVCP, OVCP).
- The audited CA also takes the responsibility for the norm requirements fulfilment
- The CA provides the certification services according to the definitions of the Certificate Practice Statement.
- The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.
- Netlock's CA services meets the following ETSI 102042 defined Normalized Certification Policies:
 - Issuing and management of qualified digital signature certificates
NCP, NCP+
 - Issuing and management of digital signature certificates

Date of issue:

Budapest, 2015.10.20.



- Issuing and management of SSL Server Certificates (DV, OV)
DVCP, OVCP
- Issuing and management of encryption Certificates
NCP, NCP+
- Issuing and management of authentication Certificates
NCP, NCP+
- Issuing and management of CodeSigning Certificates (Non-EV)
NCP, NCP+

Summary of the audit requirements

The ETSI specification ETSI TS 102 042 contains the following requirements:

1 Certification Practice Statement (CPS)

The CA has a presentation of its practices and policies.

2 Public Key Infrastructure – key management life cycle

The CA ensures that CA keys are created under controlled conditions.

The CA ensures that private CA keys are treated confidentially and that their integrity is maintained.

The CA ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved.

The CA does not generate nor store private signature keys of the certification owner (subject).

3 Public key infrastructure – certificate management life cycle

The CA ensures that the identification confirmation of a participant (subscriber) and of a certificate owner (subject) as well as the correctness of their names and their related data are either checked as part of the defined service or proved by attestations from appropriate and licensed sources. It also ensures that applications for a certificate take place in a correct and authorized way, completely according to the collected proofs respectively attestations.

The CA ensures that the certificates are handed out in a secure way so that their authenticity is maintained.

The CA ensures that the legal terms and conditions are made available to the participants (subscriber) and to the relying parties.

The CA ensures that certificates are made available to the participants (subscriber), certificate owners (subject) and relying parties to the extent necessary.

The CA ensures that certificates are blocked at short notice using authorized and verified blocking queries.

Date of issue:

Budapest, 2015.10.20.



4 CA Management and Operation

The CA ensures that the applied administrative and management methods are appropriate and correspond to acknowledged standards.

The CA ensures that the objects and information worthy of protection receive an appropriate protection.

The CA ensures that the employees and the hiring procedures amplify and support the CA Company's trustability.

The CA ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized.

The CA ensures that the CA systems are operated safely, according to specification.

The CA ensures that the access to the CA systems is restricted to appropriate, authorized persons.

The CA is to use trustworthy systems and products that are protected against modifications.

The CA ensures that in case of a catastrophe the operation is restored as soon as possible.

The CA ensures that in case of a cessation of the CA operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given.

The CA ensures that statutory requirements are met.

The CA ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

5 Organization

The CA ensures that its organization is reliable.

6 Additional requirements

The CA allows third parties to check and test their certificates.

The CA does not make use of Cross Certificates that identify the CA as the Subject.

Confirmation (Annex E requirement)

The examination was conducted in accordance with European Standards/Specifications, in particular the present document and TS 119 403 [i.2] and, where applicable, has considered all current CA/Browser Forum Requirements.

Date of issue:

Budapest, 2015.10.20.



Microsoft Root program conformance

Examination was also conducted in accordance the Microsoft root program and the CA conform with these Requirements too.

Scope clarifications

The audit took place in between 12-14 of October, 2015.

The audit period was from 15.10.2014 to 14.10.2015.

The Certificate and its annex was issued on 15.10.2015. The Annex of the certificate was modified on 20.10.2015. due to the request of Netlock.

The certificate and the annex is considered the same as the letter of attestation in the local legal and technical environment.

The audit covered all roots, non-limited sub-roots, and cross-signed non-enrolled roots, under the root, and the scope of the audit contained the full PKI hierarchy, as it is documented in the PDS version of Netlock in 14.10.2015.

The audit covered the following roots and sub-roots specifically:

| Short name in 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 |
| 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?ca=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 | www.netlock.hu/index.cgi?ca | www.netlock.hu/index.c |

Date of issue:

Budapest, 2015.10.20.



| | | | |
|----------------|---|---|--|
| | A) Tanúsítványkiadó | =caca | gi?crl=caca |
| SHA2 B | NetLock Üzleti (Class B) Tanúsítványkiadó | www.netlock.hu/index.cgi?ca=caca | www.netlock.hu/index.cgi?crl=caca |
| SHA2 C | NetLock Expressz (Class C) Tanúsítványkiadó | www.netlock.hu/index.cgi?ca=caca | www.netlock.hu/index.cgi?crl=caca |
| SHA2 MKB EAT | MKB 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 Eat. Tanúsítványkiadó | http://www.keler.hu/crl/lhsz2.crt | http://www.keler.hu/crl/lhsz2.crl |
| 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 QA | Netlock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado | www.netlock.hu/index.cgi?ca=mshea | www.netlock.hu/index.cgi?crl=mshea |
| SHA1 A | Netlock Kozjegyzoi (Class A) Tanusitvanykiado | www.netlock.hu/index.cgi?ca=kozjegyzoi | www.netlock.hu/index.cgi?crl=kozjegyzoi |
| SHA1 B | Netlock Uzleti (Class B) Tanusitvanykiado | www.netlock.hu/index.cgi?ca=uzleti | www.netlock.hu/index.cgi?crl=uzleti |
| SHA1 C | Netlock Expressz (Class C) Tanusitvanykiado | www.netlock.hu/index.cgi?ca=expressz | www.netlock.hu/index.cgi?crl=expressz |
| SHA1 MKB | Netlock controlled CA for MKB Bank, Hungary | already archived | already archived |
| SHA1 MNB | Netlock controlled CA for MNB Bank, Hungary | already archived | already archived |
| SHA1 OnlineSSL | Netlock OnlineSSL Hitelesito Alegysege | already archived | already archived |
| SHA2 KI Q | NetLock Minositett Kozigazgatasi (Class Q) Tanusitvanykiado | https://www.netlock.hu/index.cgi?ca=mkozig256 | https://www.netlock.hu/index.cgi?crl=mkozig256 |
| SHA2 KI B | NetLock Kozigazgatasi Uzleti (Class B) Tanusitvanykiado | https://www.netlock.hu/index.cgi?ca=bkozig256 | https://www.netlock.hu/index.cgi?crl=bkozig256 |

Date of issue:

Budapest, 2015.10.20.



TÜV Rheinland InterCert Kft. – Product Certification Body — H-1132 Budapest, Váci út 48/A-B — www.tuv.hu