Standard Audit Attestation for

NETLOCK Ltd.

Reference: I-NL24T1_AAL-03.STANDARD

Budaörs, 2024-08-28

To whom it may concern,

This is to confirm that MATRIX Ltd. has audited the CAs of the NETLOCK Ltd. without critical findings

This present Audit Attestation Letter is registered under the unique identifier number I-NL24T1_AAL-03.STANDARD covers multiple Root-CAs and consists of 21 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

MATRIX Ltd.

Szabadság str. 290.

H-2040 Budaörs, Hungary

E-Mail: molnar.adam@matrix-tanusito.hu

Phone: +36306984341

With best regards,

Ádám Molnár
Managing Director

This attestation is based on the template version 3.1 as of 2023-08-24, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• MATRIX Auditing, Evaluating and Certification Ltd., Szabadság út 290., H-2040 Budaörs, Hungary registered under 13-09-084216 • Accredited by National Accreditation Authority under registration NAH-6-0054/2024/K for the certification of trust services according to EN ISO/IEC 17065:2013 and ETSI EN 319 403-1 V2.3.1 (2020- 06) respectively. • Insurance Carrier (BRG section 8.2): K&H Biztosító Zrt. (K&H Insurance) • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 3 • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is

current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: None. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team:1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	NETLOCK Informatics and Network Security Services Limited Liability Company, Expo tér 5-7., H-1101 Budapest, Hungary, registered under company registration 01-09-563961

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2023-08-25 to 2024-08-24
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-06-14 to 2024-07-26 (remote) 2024-08-13 to 2024-08-15 (on site)
Audit location:	H-1143 Budapest, Hungária körút 17, Hungary H-1101 Budapest, Expo tér 5-7, Hungary

Root 1: NetLock Arany (Class Gold) Főtanúsítvány

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.0 (2024-06) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 2.0.1 • Baseline Requirements for TLS Server Certificates, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9 (2023-09-01) • Microsoft Trusted Root Certificate Program (2024-07-03) • Chrome Root Program Policy, Version 1.5 (2024-01-16) • Apple Root Certificate Program (2023-08-15) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.2.4 (2020-11)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- PKI Disclosure Statement, version 20210716, as of 2021-07-16
- Service Policy for Qualified Certification Services, version 240701, as of 2024-07-01
- Service Policy for Non-Qualified Certification Service, version 20240420, as of 2024-04-20
- Service Policy for Non-eIDAS Certification Service, version 20240716, as of 2024-04-16
- Service Practice Statement for Qualified Certificate Services, version 240420, as of 2024-04-20
- Service Practice Statement for Non-Qualified Certification Service, version 20201119, as of 2024-04-20
- Service Practice Statement for Non-eIDAS Certification Service, version 20240716, as of 2024-07-16
-

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.3.2 Assets inventory and classification

The TSP’s asset inventory (Adapto) contains the personal information assets, however it needs to contain the other information assets of the company. [REQ-7.3.2.01X]

The TSP maintains its asset inventory in Adapto (information assetst) and SnipeIT (Physical assets (HSM, PC, mobile devices, etc.) however the inventories does not contain the following informations about the assets:

e) the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

g) the date and version of the asset's last update or patch;

h) the classification level of the asset;
i) the asset's end of life.
and are not fully consistens with eachother. [REQ-7.3.2.02X]

7.11.2 Backup

The TSP regurarly does backup restore tests with documented procedure, however the test report does not contains the following informations: OID of the applicable policy for the restore test, the restored file ID, time. [REQ-7.11.2-04X]

7.11.3 Crisis management

The TSP have a process for crisis management, however it does not have a documented plan for the process. [REQ-7.11.3.-01X]

The crisis management plan have not been tested yet. [REQ-7.11.3-03X]

7.14 Supply chain

The TSP's evaluation process is the owner group companies evaluation process which does not contain evaluation of the cybersecurity requirements. The TSP shall make a supply chain evaluation process of its own which contains the evaluation of the suppliers cybersecurity conformity [REQ-7.14.1-01X]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1889570, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1889570#c11
- Bug 1891331, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates - delayed revocation
  https://bugzilla.mozilla.org/show_bug.cgi?id=1891331
- Bug 1905509, NETLOCK: CPR was not responded to in 24 hours:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1905509
- Bug 1906115, Netlock: Delayed reply from CPR sent to contact listed in section 1.5.2 of CP/S:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1906115
- Bug 1907568, NETLOCK: CPS 1.5.2. problem and contact information update:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1907568
- Bug 1819105, NETLOCK: Disclosed CRL is expired:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1819105#c6

The remediation measures taken by NETLOCK Ltd. as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN= NetLock Arany (Class Gold) Főtanúsítvány, O= NetLock Kft., C= HU	SHA-256 fingerprint of the certificate: 6C61DAC3A2DEF031506BE036D2A6FE401994FBD13DF9C8D466599274C446EC98	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, OVCP, EVCP, LCP, NCP, NCP+, DVCP

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = NETLOCK Trust Advanced Plus CA, O = NetLock Kft., C = HU	F2603670BEDEAD1D977D6992FA6554E6CA595BC50F3B03F416DCF0F20DAC36C2	ETSI EN 319 411-1 V1.3.1, LCP
CN = NETLOCK Trust Advanced CA, O = NetLock Kft., C = HU	D82F87F93D31D5FC818DD66BD50E7F319AE179FC1C5D00547B658E8EB3F4CE56	ETSI EN 319 411-1 V1.3.1, LCP
CN = NETLOCK Trust CA, O = NetLock Kft., C = HU	58D7A197F09A6EA552B8EA6B1A53185A030A3AD8D52220C00C44E3F450E4FB90	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
CN = NETLOCK Trust SSL CA, O = NetLock Kft., C = HU (revoked)	0A778BF9DD7F75B2F983FB7FA705C987CCCB5877404BE7EB5D8BA0B73545D0D9	ETSI EN 319 411-1 V1.3.1, OVCP
CN = NETLOCK Trust EV CA, O = NetLock Kft., C = HU (revoked)	A476FE1FBFEBA08175A0C34807990B86E63B5AA2D6CE579C4F456C95575BB1F6	ETSI EN 319 411-1 V1.3.1, OVCP, EVCP
CN = NETLOCK Trust EV CA 2, O = NetLock Kft., C = HU (revoked)	CD0CC3A6F6857D427D6D98F6BF877E0845E365C5BAC61C9BAF27AE0AC3681A57	ETSI EN 319 411-1 V1.3.1, OVCP, EVCP
CN = NETLOCK Trust EV CA 3, O = NetLock Kft., C = HU	047795785CDCFF9E6E0AE122492E5B7BF08A9E5C49762E2BCB52747C69031561	ETSI EN 319 411-1 V1.3.1, OVCP, EVCP
CN = NetLock CodeSign CA, O = NetLock Kft., C = HU	C56F0F286618C1E7B0E112C97B9EE96FEB4D71E79496C151FA1FE8A8CEBD06CD	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
CN = NETLOCK DVSSL CA, O = NetLock Kft., C = HU	F91606D1BC52C610136CAA856AB500C48C3B993BAC4808CD82BC4B78ABF24156	ETSI EN 319 411-1 V1.3.1, DVCP

CN = NETLOCK Public Administration CA, O = NetLock Kft., C = hu	DB71EC6A5F220A7FB90FE0D18AAA0CFE16CFD0FA63F279DAC4FF3A73FC82C4A0	ETSI EN 319 411-1 V1.3.1, NCP+
CN = NETLOCK Trust Qualified QSCD CA, O = NetLock Kft., C = HU	9E4362A918A89009877C7B8B190E763AE012AD47C1CCA5FCCF166FC092BC2ADE	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd, QCP-l-qscd
CN = NETLOCK Trust Qualified RQSCD CA, O = NetLock Kft., C = HU	A59F880816A50886D4D5996E64918DD9D401472AA685D28E7DECA5299F05FCE0	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd, QCP-l-qscd
CN = NETLOCK Trust Qualified SCD CA, O = NetLock Kft., C = HU	7CE1DB7D16E9BFE80693214A3D7C6263AA24789E399017E69EDE4802ECF6F711	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = NETLOCK Trust Qualified CA, O = NetLock Kft., C = HU	5498963DFFA651604F467E108E65A183470FA9B557C129DDF8C9D812B4F0BF96	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = NETLOCK Trust Qualified EV CA, O = NetLock Kft., C = HU (revoked)	B0F25A6D9A96315C7CDAEA3E490E7BFA9FB17310B0701B7CD6FF432530837730	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QEVCP-w
CN = NETLOCK Trust Qualified EV CA 2, O = NetLock Kft., C = HU (revoked)	36EFD13AE5DC6D01B6C1956841B45D18CE8085FBC197D90E8A8A21A9B01EBFBA	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QEVCP-w
CN = NETLOCK Trust Qualified EV CA 3, O = NetLock Kft., C = HU	7ECACA4A3585A3B40E25574415512D56B57999B753017856F2AB15FA1F21F6D0	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QEVCP-w
CN = NETLOCK Qualified Public Administration CA, O = NetLock Kft., C = HU	9E48A8B70E6CF4CF7099DB8995EE9EF5179911DC8830369BF66518CD5FA8AC01	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd
CN = NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU	6284A03BAFAE861A30E3A25A030428306F7EB52BD0BA577A1D962A809A830C9E	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd
CN = NetLock Minősített Eat. Spec.(Class Q Legal Spec.) Tanúsítványkiadó, O = NetLock Kft., C = HU	A5F2FD0D66DB4DD77A2914ED3C747CBD97E734CF4E2B6F217FB41AA4EAFDEAD2	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd
CN = NetLock Közjegyzői Eat. (Class A Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU	AD47883A48C86A3469E32C972B39A3EE155804D32BF53FF002000BCA11D295D9	ETSI EN 319 411-1 V1.3.1, LCP
CN = NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU	1D93686CA42C70394FBDC2BC1F98461D19871C2A00078B815499312ED9F6FE0C	ETSI EN 319 411-1 V1.3.1, LCP

CN = NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU	BB661D750C53166181807A6898FD464065CE59298986AD66D9D6FFFCBBD4738A	ETSI EN 319 411-1 V1.3.1, LCP
CN = NetLock Közjegyzői (Class A) Tanúsítványkiadó, O = NetLock Kft., C = HU	75894D4C94C22D7296EE19FB447623258C2591B17031288BB386A20AA1F0E0A6	ETSI EN 319 411-1 V1.3.1, OVCP
CN = NetLock Üzleti (Class B) Tanúsítványkiadó, O = NetLock Kft., C = HU	6B23FAD890180C337B864155DAE0DE9BAD9EF0BDA78D112F2CBDC3D02AD17956	ETSI EN 319 411-1 V1.3.1, OVCP
CN = NetLock Expressz (Class C) Tanúsítványkiadó, O = NetLock Kft., C = HU	372B8F4CE73BEDFC88718C407BB6B3E6D8F9A79BE957190D0E7101C7B0EF9A32	ETSI EN 319 411-1 V1.3.1, OVCP
CN = MKB Hitelesítő alegység 2, O = NetLock Kft., C = HU (revoked)	E53A9D8C0046C6366D3C6A18E23B4F4CBAAADB7D79B8C2F18786821DEE046AF3	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = MKB SubCA 5, O = NetLock Kft., C = HU (renewed)	BC81F4A347BCBE1D53AF1C71B0D7E403246389D7465D5296D3B963AB208C2080	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = MNB Hitelesítő Alegység 2. Eat., O = NetLock Kft., C = HU (expired)	878EF628267A15493D2BD9B1BA12311874680BD8E1C4F04A8B369241DB034DFA	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = Keler Hitelesítő Alegység Eat., O = NetLock Kft., C = HU (revoked)	73C27704C3B312807D18155B3AD06907DC9A374B66FBEDC2BC2973031A6BE988	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = MNB Hitelesítő Alegység 2., O = NetLock Kft., C = HU	4A3BB05DB15EE3BE9774206B8B6AFE229C6F7C87C3A5CFA08861568EBDCE7DB3	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = Keler Hitelesítő Alegység Eat., O = NetLock Kft., C = HU (revoked)	EE2723FB2591671774DE5EF80BEC656A7AF01F3B24067AF269EE35301891AC51	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = NetLock Uzleti (Class B) Tanusitvanykiado, O = NetLock Halozatbiztonsagi Kft., C = HU (expired)	39DF7B682B7B938F84715481CCDE8D60D8F22EC598877D0AAAC12B59182B0312	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP
CN = NetLock OnlineSSL (Class Online) Tanúsítványkiadó, O = NetLock Kft., C = HU	CC9F72544FF617C14CEBE8283194A70F1E8981CF163D5A3FD8DCCFD846D5DC1A	ETSI EN 319 411-1 V1.3.1, DVCP
CN = KGYHSZ (Public Administration Root CA - Hungary), C = hu	833492D73A6CF4E319C59F358D37DFB55198ED38A98890FE471091F4E3DF2720	0.2.216.1.100.42.1.200.2, cPSuri = http://cp.kgyhsz.gov.hu

CN = NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó, O = NetLock Kft., C = HU (expired)	EBA22784D20902A9F9AF3F640D14889A53D7F3C4B5B0697016B8D749ADE97F3E	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd
CN = NetLock Közigazgatási (Class B) Tanúsítványkiadó, O = NetLock Kft., C = HU (expired)	F7F8CD8A0BCFEF0376B4DE06904BD4F179BF3B54257FCF305CDCCF7ED7F3524	ETSI EN 319 411-1 V1.3.1, NCP+
CN = NetLock Uzleti (Class B) Tanusitvanykiado, O = NetLock Halozatbiztonsagi Kft., C = HU (expired)	39DF7B682B7B938F84715481CCDE8D60D8F22EC598877D0AAAC12B59182B0312	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP
CN = NetLock Minositett Kozjegyzoi (Class QA) Tanúsítványkiadó, O = NetLock Kft., C = HU	E606DDEEE2EE7F5CDEF5D9058FF8B7D0A9F042877F6A171ED8FF6960E4CC5EA5	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
CN = NetLock Kozjegyzoi (Class A) Tanusitvanykiado O = NetLock Halozatbiztonsagi Kft., C = HU (expired)	7F12CD5F7E5E290EC7D85179D5B72C20A5BE7508FFDB5BF81AB9684A7FC9F667	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP
CN=NetLock Expressz (Class C) Tanusitvanykiado, O=NetLock Halozatbiztonsagi Kft., C=HU (expired)	0B5EED4E846403CF55E065848440ED2A82758BF5B9AA1F253D4613CFA080FF3F	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+, OVCP
CN= NETLOCK TLS OV ECC CA, O= NETLOCK Kft., C= HU	D0EB908401F33242602634AFD51991536B3AD7AA901586FDEB4955FE51B0E419	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, OVCP
CN= NETLOCK TLS EV ECC CA, O= NETLOCK Kft., C= HU	F37E7AD92ECEA12F307501C126B3E2D6DE2C7417D3E1B72D26069C1370E78894	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, EVCP
CN= NETLOCK TLS Qualified EV ECC CA, O= NetLock Kft., C= HU	17771F6947FA3472786D3A44B5ADE2AACBA9ADA203BA31EBD4BD8CEBAFCE494A	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QEVCP-w
CN= NETLOCK TLS DV ECC CA, O= NETLOCK Kft., C= HU	001279B949DD8670F1AE6DA407913B726F61AEF78A2FF19C2DA39522B31DC0C7	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1 DVCP

Table 2: Sub-CA’s issued by the Root-CA 1 or its Sub-CA’s in scope of the audit

Root 2: NetLock Platina (Class Platinum) Főtanúsítvány

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.0 (2024-06) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 2.0.1 • Baseline Requirements for TLS Server Certificates, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9 (2023-09-01) • Microsoft Trusted Root Certificate Program (2024-07-03) • Chrome Root Program Policy, Version 1.5 (2024-01-16) • Apple Root Certificate Program (2023-08-15) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.2.4 (2020-11)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- PKI Disclosure Statement, version 20210716, as of 2021-07-16
- Service Policy for Qualified Certification Services, version 240701, as of 2024-07-01
- Service Policy for Non-Qualified Certification Service, version 20240420, as of 2024-04-20
- Service Policy for Non-eIDAS Certification Service, version 20240716, as of 2024-04-16
- Service Practice Statement for Qualified Certificate Services, version 240420, as of 2024-04-20
- Service Practice Statement for Non-Qualified Certification Service, version 20201119, as of 2024-04-20
- Service Practice Statement for Non-eIDAS Certification Service, version 20240716, as of 2024-07-16

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.3.2 Assets inventory and classification

The TSP’s asset inventory (Adapto) contains the personal information assets, however it needs to contain the other information assets of the company. [REQ-7.3.2.01X]

The TSP maintains its asset inventory in Adapto (information assetst) and SnipeIT (Physical assets (HSM, PC, mobile devices, etc.) however the inventories does not contain the following informations about the assets:

e) the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

g) the date and version of the asset's last update or patch;

h) the classification level of the asset;

i) the asset's end of life.

and are not fully consistens with eachother. [REQ-7.3.2.02X]

7.11.2 Backup

The TSP regurarly does backup restore tests with documented procedure, however the test report does not contains the following informations: OID of the applicable policy for the restore test, the restored file ID, time. [REQ-7.11.2-04X]

7.11.3 Crisis management

The TSP have a process for crisis management, however it does not have a documented plan for the process. [REQ-7.11.3.-01X]

The crisis management plan have not been tested yet. [REQ-7.11.3-03X]

7.14 Supply chain

The TSP's evaluation process is the owner group companies evaluation process which does not contain evaluation of the cybersecurity requirements. The TSP shall make a supply chain evaluation process of its own which contains the evaluation of the suppliers cybersecurity conformity [REQ-7.14.1-01X]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1889570, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1889570#c11
- Bug 1891331, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates - delayed revocation
  https://bugzilla.mozilla.org/show_bug.cgi?id=1891331
- Bug 1905509, NETLOCK: CPR was not responded to in 24 hours:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1905509
- Bug 1906115, Netlock: Delayed reply from CPR sent to contact listed in section 1.5.2 of CP/S:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1906115
- Bug 1907568, NETLOCK: CPS 1.5.2. problem and contact information update:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1907568
- Bug 1819105, NETLOCK: Disclosed CRL is expired:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1819105#c6

The remediation measures taken by NETLOCK Ltd. as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = NetLock Platina (Class Platinum) Főtanúsítvány, O = NetLock Kft., C = HU	EB7E05AA58E7BD328A282BF8867033F3C035342B516EE85C01673DFFFFBBFE58	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, DVCP, QEVCP-w

Table 3: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = NETLOCK Domain Validated CA, O = NETLOCK Ltd., C = HU	A1663E37B8992D819C69FB89707065CABDFE3D53C278FC3EC2601001798602F8	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, DVCP, QEVCP-w

Table 4: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s in scope of the audit

Root 3: NETLOCK Root ECC CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.0 (2024-06) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 2.0.1 • Baseline Requirements for TLS Server Certificates, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9 (2023-09-01) • Microsoft Trusted Root Certificate Program (2024-07-03) • Chrome Root Program Policy, Version 1.5 (2024-01-16) • Apple Root Certificate Program (2023-08-15) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.2.4 (2020-11)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- PKI Disclosure Statement, version 20210716, as of 2021-07-16
- Service Policy for Qualified Certification Services, version 240701, as of 2024-07-01
- Service Policy for Non-Qualified Certification Service, version 20240420, as of 2024-04-20
- Service Policy for Non-eIDAS Certification Service, version 20240716, as of 2024-04-16
- Service Practice Statement for Qualified Certificate Services, version 240420, as of 2024-04-20
- Service Practice Statement for Non-Qualified Certification Service, version 20201119, as of 2024-04-20
- Service Practice Statement for Non-eIDAS Certification Service, version 20240716, as of 2024-07-16

In the following areas, non-conformities have been identified throughout the audit:
Findings with regard to ETSI EN 319 401:

7.3.2 Assets inventory and classification

The TSP’s asset inventory (Adapto) contains the personal information assets, however it needs to contain the other information assets of the company. [REQ-7.3.2.01X]

The TSP maintains its asset inventory in Adapto (information assetst) and SnipeIT (Physical assets (HSM, PC, mobile devices, etc.) however the inventories does not contain the following informations about the assets:

e) the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

g) the date and version of the asset's last update or patch;

h) the classification level of the asset;
i) the asset's end of life.
and are not fully consistens with eachother. [REQ-7.3.2.02X]

7.11.2 Backup

The TSP regurarly does backup restore tests with documented procedure, however the test report does not contains the following informations: OID of the applicable policy for the restore test, the restored file ID, time. [REQ-7.11.2-04X]

7.11.3 Crisis management

The TSP have a process for crisis management, which have been reviewed recently and needs to be updated and have to update it in the documentation. [REQ-7.11.3.-01X]

The crisis management plan have not been tested yet. [REQ-7.11.3-03X]

7.14 Supply chain

The TSP's evaluation process is the owner group companies evaluation process which does not contain evaluation of the cybersecurity requirements. The TSP shall make a supply chain evaluation process of its own which contains the evaluation of the suppliers cybersecurity conformity [REQ-7.14.1-01X]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1889570, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1889570#c11
- Bug 1891331, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates - delayed revocation
  https://bugzilla.mozilla.org/show_bug.cgi?id=1891331
- Bug 1904041, NETLOCK: Intermediate CA Certificate not disclosed to CCADB:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1904041
- Bug 1905509, NETLOCK: CPR was not responded to in 24 hours:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1905509
- Bug 1906115, Netlock: Delayed reply from CPR sent to contact listed in section 1.5.2 of CP/S:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1906115
- Bug 1907568, NETLOCK: CPS 1.5.2. problem and contact information update:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1907568
- Bug 1819105, NETLOCK: Disclosed CRL is expired:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1819105#c6

The remediation measures taken by NETLOCK Ltd. as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = NETLOCK Root ECC CA, O = NETLOCK Kft., C = HU	00F12C1ECFE26D34A28FC6BF9FB35085302C7D53A9AC3588ED7CD86C9C7423AA	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, OVCP, EVCP, LCP, NCP, NCP+, DVCP

Table 5: Root-CA 3 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
NETLOCK Trust Qualified ECC CA	4282734163BF9FF8424F1EEFB06839FF25DE67D6C1FD50793691740B6045B76C	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
NETLOCK Trust Qualified SCD ECC CA	7DCA097AB7649E648217D0ADE6B33992EBF2DD794B38BCCF1B2B5FA52064BB2C	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
NETLOCK Trust Qualified QSCD ECC CA	CAD759BAF84AB3079377C32AF8353D08C3C599E76F5ADEA203E45C42047D6C66	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd, QCP-l-qscd
NETLOCK Trust Qualified RQSCD VRA ECC CA	905C5EFA99F8984D03F8C1345DD976AB097FC8CA51C6CA12D1B2780D8128174F	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd, QCP-l-qscd
NETLOCK Trust Advanced ECC CA	958289D7DFAD053866B6891CB6AD197739203DB8EF043C9D4E2C6767ED5D7D44	ETSI EN 319 411-1 V1.3.1, LCP
NETLOCK Trust Advanced Plus ECC CA	E26BD57346D8873CF5FF88E0D4DD0037CB5F27DFE67150B70D4D1EEA9741423D	ETSI EN 319 411-1 V1.3.1, LCP
NETLOCK Trust ECC CA	6C8AD28655A95D47E9E26EDEC96FD866A053010115FC25095E75FAE6A71D8520	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+

Table 6: Sub-CA’s issued by the Root-CA 3 or its Sub-CA’s in scope of the audit

Root 4: NETLOCK TLS ECC CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.0 (2024-06) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 2.0.1 • Baseline Requirements for TLS Server Certificates, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, Version 2.9 (2023-09-01) • Microsoft Trusted Root Certificate Program (2024-07-03) • Chrome Root Program Policy, Version 1.5 (2024-01-16) • Apple Root Certificate Program (2023-08-15) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.2.4 (2020-11)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- PKI Disclosure Statement, version 20210716, as of 2021-07-16
- Service Policy for Qualified Certification Services, version 240701, as of 2024-07-01
- Service Policy for Non-Qualified Certification Service, version 20240420, as of 2024-04-20
- Service Policy for Non-eIDAS Certification Service, version 20240716, as of 2024-04-16
- Service Practice Statement for Qualified Certificate Services, version 240420, as of 2024-04-20
- Service Practice Statement for Non-Qualified Certification Service, version 20201119, as of 2024-04-20
- Service Practice Statement for Non-eIDAS Certification Service, version 20240716, as of 2024-07-16

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.3.2 Assets inventory and classification

The TSP’s asset inventory (Adapto) contains the personal information assets, however it needs to contain the other information assets of the company. [REQ-7.3.2.01X]

The TSP maintains its asset inventory in Adapto (information assetst) and SnipeIT (Physical assets (HSM, PC, mobile devices, etc.) however the inventories does not contain the following informations about the assets:

e) the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

g) the date and version of the asset's last update or patch;
h) the classification level of the asset;
i) the asset's end of life.
and are not fully consistens with eachother. [REQ-7.3.2.02X]

7.11.2 Backup

The TSP regurarly does backup restore tests with documented procedure, however the test report does not contains the following informations: OID of the applicable policy for the restore test, the restored file ID, time. [REQ-7.11.2-04X]

7.11.3 Crisis management

The TSP have a process for crisis management, which have been reviewed recently and needs to be updated and have to update it in the documentation. [REQ-7.11.3.-01X]

The crisis management plan have not been tested yet. [REQ-7.11.3-03X]

7.14 Supply chain

The TSP's evaluation process is the owner group companies evaluation process which does not contain evaluation of the cybersecurity requirements. The TSP shall make a supply chain evaluation process of its own which contains the evaluation of the suppliers cybersecurity conformity [REQ-7.14.1-01X]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1889570, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1889570#c11
- Bug 1891331, NETLOCK: Policy Qualifiers other than id-qt-cps is included in TLS certificates - delayed revocation
  https://bugzilla.mozilla.org/show_bug.cgi?id=1891331
- Bug 1904041, NETLOCK: Intermediate CA Certificate not disclosed to CCADB:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1904041
- Bug 1905509, NETLOCK: CPR was not responded to in 24 hours:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1905509
- Bug 1906115, Netlock: Delayed reply from CPR sent to contact listed in section 1.5.2 of CP/S:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1906115
- Bug 1907568, NETLOCK: CPS 1.5.2. problem and contact information update:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1907568
- Bug 1819105, NETLOCK: Disclosed CRL is expired:
  https://bugzilla.mozilla.org/show_bug.cgi?id=1819105#c6

The remediation measures taken by NETLOCK Ltd. as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = NETLOCK TLS ECC CA, O = NETLOCK Kft., C = HU	DC4261667AFE21DDD01CFA52D2CCADFD70ABAF26315DC6A15A32B76C899AE261	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, OVCP, EVCP,QEVCP LCP, NCP, NCP+, DVCP

Table 7: Root-CA 4 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN= NETLOCK TLS DV ECC CA, O= NETLOCK Kft., C= HU	34F55889DC80E1EE5E4E8A2CFF4CC79BB9D0A492ED360B52F3B64D0971657192	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, DVCP
CN= NETLOCK TLS EV ECC CA, C= NETLOCK Kft., C= HU	C093804E8E15E5973BC471AB64E895FB5A4A007C9A5C994125678E4805BB4BA0	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, EVCP
CN= NETLOCK TLS OV ECC CA, O= NETLOCK Kft., C= HU	62B5852AB9461E9C237C7C63941E4B771D33B3CBB72133046B659DB7DA608419	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, OVCP
CN= NETLOCK TLS Qualified EV ECC CA , O= NETLOCK Kft., C= HU	F0FD5DEF6430CBDCDE8037E24112E2B4B6F0188B7F64C44D9FA0271069734296	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, QEVCP-w

Table 8: Sub-CA’s issued by the Root-CA 4 or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2024-08-26	Initial attestation
Version 2	2024-08-28	SHA-256 Fingerprint format updates

End of the audit attestation letter.