TLS BR Audit Attestation for

NETLOCK Ltd.

Reference: E-NL26T1_AAL-01.TLS-BR

Budaörs, 2026-11-18

To whom it may concern,

This is to confirm that MATRIX Auditing, Evaluating and Certification Ltd. has audited the CAs of the NETLOCK Informatics and Network Security Services Limited Liability Company, Hungária krt. 17-19., H-1143 Budapest, Hungary without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number E-NL26T1_AAL-01.TLS-BR covers multiple Root-CAs and consists of 21 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

MATRIX Auditing, Evaluating and Certification Ltd.
Szabadság út 290.
H-2040 Budaörs, Hungary
E-Mail: nagy.gabor@matrix-tanusito.hu
Phone: +36306984341

With best regards,

Gábor Nagy
Director of Certification

This attestation is based on the template version 3.5 as of 2026-03-09, 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[1] for the certification of trust services according to EN ISO/IEC 17065:2012" and ETSI EN 319 403-1 V2.3.1 (2020-06). • 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

[1] URL to the accreditation certificate hosted by the national accreditation body

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, Hungária krt. 17-19., H-1143 Budapest, Hungary, registered under 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:	2025-07-24 to 2026-07-23
Point in time date:	none, as audit was a period of time audit
Audit dates:	2026-07-06 to 2026-07-23 (remote) 2026-07-13 to 2026-07-17 (on site)
Audit location:	H-1143 Budapest, Hungária körút 17-19, Hungary H-1101 Budapest, Expo tér 5-7, Hungary H-1087 Budapest, Asztalos Sándor út 13, Hungary

Root 1: Netlock Arany (Class Gold) Főtanúsítvány

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.6.1 (2025-06) • ETSI EN 319 411-1 V1.5.1 (2024-12) • ETSI EN 319 401 V3.2.1 (2026-01) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Chrome Root Program Policy, Version 1.8 (2026-02-05) • Mozilla Root Store Policy, Version 3.1 (2026-07-01) • Microsoft Trusted Root Certificate Program (2025-02-25) • Apple Root Certificate Program (2023-08-15) • Latest S/MIME Baseline Requirements, version 1.0.14 (2026-05-05) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

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

- General Terms and Conditions

Version	Release Date	Effective from	Effective until
250625	2025-06-25	2025-06-25	2025-12-13
251214	2025-12-14	2025-12-14	2026-02-17
260218	2026-02-18	2026-02-18	…

- Extract of Service Practice Statements for Trust Services

Version	Release Date	Effective from	Effective until
250417	2025-04-17	2025-04-17	2026-02-17
20260218	2026-02-18	2026-02-18	…

- PKI Disclosure Statement

Version	Release Date	Effective from	Effective until
250414	2025-04-14	2025-04-14	2026-02-17
260218	2026-02-18	2026-02-18	…

- Service Policy for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	…

- Service Policy for Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-08-22
250724	2025-07-24	2025-08-23	2025-11-05
251007	2025-10-07	2025-11-06	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Qualified Certificate Services

Version	Release Date	Effective from	Effective until
250310	2025-03-10	2025-03-10	2026-02-17
260218	2026-02-18	2026-02-18	2026-04-14
260415	2026-04-15	2026-04-15	…

- Service Practice Statement for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27

251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Policy for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	…

- Mass Revocation Plan

Version	Release Date	Effective from	Effective until
v01	2025-11-06	2025-11-06	…

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

Findings with regard to ETSI EN 319 401:

7.9.3 Reporting

NETLOCK monitoring alerted that an OCSP certification expiry however the alert has not been remeditated in time as an incident occured. [REQ-7.9.3-03]

7.9.3 Reporting

The incident has not been communicated in 24 hours. [REQ-7.9.3-01]

7.9.1 Monitoring and logging

NETLOCK has a compley ,monitoring systems for its network and information systems, however its need development to become more automated to minimize risks. [REQ-7.9.1-07]

7.9.2 Incident response

NETLOCK has a incident management process and documentation however it requires optimalization to receive the reports in time. [REQ-7.9.2-11]

Findings with regard to ETSI EN 319 411-1:

6.6.1 Certificate profile

According to RFC 5280 §4.2.2.1, AIA HTTP URIs must provide a DER-encoded certificate or a DER/BER CMS “certs-only” container, therefore serving PEM content does not comply with the standard. [GEN-6.6.1-01]

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.

- Bug1978904, NETLOCK: Add NETLOCK's S/MIME & TLS Root https://bugzilla.mozilla.org/show_bug.cgi?id=1978904
- Bug 2001327, NETLOCK: Missing CDP Disclosure in CCADB https://bugzilla.mozilla.org/show_bug.cgi?id=2001327
- Bug 2004699, Netlock: CA in AIA in PEM format https://bugzilla.mozilla.org/show_bug.cgi?id=2004699
- Bug 2007948, NETLOCK: Full Incident Report was not published within 14 days of notification https://bugzilla.mozilla.org/show_bug.cgi?id=2007948
- Bug 2011314, NETLOCK: unspecifed revocation code (0) in CRL https://bugzilla.mozilla.org/show_bug.cgi?id=2011314
- Bug 2021559, NETLOCK: Unavailability of the document repository https://bugzilla.mozilla.org/show_bug.cgi?id=2021559
- Bug 2013400, NETLOCK: did not file a preliminary incident report or respond to a third-party report within the 72-hour timeframe https://bugzilla.mozilla.org/show_bug.cgi?id=2013400
- Bug 2013395, NETLOCK: Missing Related Incidents section in the bug report https://bugzilla.mozilla.org/show_bug.cgi?id=2013395
- Bug 2032939, NETLOCK: Transition Plan for Mozilla Root Store Policy 7.5 by Deadline https://bugzilla.mozilla.org/show_bug.cgi?id=2032939
- Bug, 2033033, NETLOCK: Transition Plan for Existing Dual-Purpose Root https://bugzilla.mozilla.org/show_bug.cgi?id=2033033
- Bug 2051459, NETLOCK: OCSP Service Returning Error for Issued Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=2051459
- Bug 2052541, NETLOCK: Failure to Respond to a Certificate Problem Report Within 24 Hours https://bugzilla.mozilla.org/show_bug.cgi?id=2052541
- Bug 1979287, NETLOCK: Expired Test Website Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=1979287
- Bug 1947691, NETLOCK: Bug 1891331 replacement - delayed revocation - https://bugzilla.mozilla.org/show_bug.cgi?id=1947691

The remediation measures taken by NETLOCK Ltd. as described on Bugzilla (see link above) have been checked by the auditors and properly 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 policy that this Root has been assessed against: 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
Complete subject DN: CN= NETLOCK TLS OV ECC CA, O= NETLOCK Kft., C= HU (expired)	SHA-256 fingerprint of the certificate: D0EB908401F33242602634AFD51991536B3AD7AA901586FDEB4955FE51B0E419	ETSI EN policy that this Root has been assessed against: 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 (expired)	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 (expired)	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 (expired)	001279B949DD8670F1AE6DA407913B726F61AEF78A2FF19C2DA39522B31DC0C7	ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1 DVCP
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 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 Minősített Eat. (Class Q Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU (expired)	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 (expired)	1D93686CA42C70394FBDC2BC1F98461D19871C2A00078B815499312ED9F6FE0C	ETSI EN 319 411-1 V1.3.1, LCP
CN = NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó, O = NetLock Kft., C = HU (expired)	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 (expired)	6B23FAD890180C337B864155DAE0DE9BAD9EF0BDA78D112F2CBDC3D02AD17956	ETSI EN 319 411-1 V1.3.1, OVCP

CN = NetLock Expressz (Class C) Tanúsítványkiadó, O = NetLock Kft., C = HU (expired)	372B8F4CE73BEDFC88718C407BB6B3E6D8F9A79BE957190D0E7101C7B0EF9A32	ETSI EN 319 411-1 V1.3.1, OVCP
CN = MKB Hitelesítő alegység 2, O = NetLock Kft., C = HU (expired)	E53A9D8C0046C6366D3C6A18E23B4F4CBAAADB7D79B8C2F18786821DEE046AF3	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = MKB SubCA 5, O = NetLock Kft., C = HU (revoked)	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 (expired)	73C27704C3B312807D18155B3AD06907DC9A374B66FBEDC2BC2973031A6BE988	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = MNB Hitelesítő Alegység 2., O = NetLock Kft., C = HU (expired)	4A3BB05DB15EE3BE9774206B8B6AFE229C6F7C87C3A5CFA08861568EBDCE7DB3	ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-l
CN = Keler Hitelesítő Alegység Eat., O = NetLock Kft., C = HU (expired)	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 (revoked)	CC9F72544FF617C14CEBE8283194A70F1E8981CF163D5A3FD8DCCFD846D5DC1A	ETSI EN 319 411-1 V1.3.1, DVCP
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 (expired)	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

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 V2.6.1 (2025-06) • ETSI EN 319 411-1 V1.5.1 (2024-12) • ETSI EN 319 401 V3.2.1 (2026-01) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Chrome Root Program Policy, Version 1.8 (2026-02-05) • Mozilla Root Store Policy, Version 3.1 (2026-07-01) • Microsoft Trusted Root Certificate Program (2025-02-25) • Apple Root Certificate Program (2023-08-15) • Latest S/MIME Baseline Requirements, version 1.0.14 (2026-05-05) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

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

- General Terms and Conditions

Version	Release Date	Effective from	Effective until
250625	2025-06-25	2025-06-25	2025-12-13
251214	2025-12-14	2025-12-14	2026-02-17
260218	2026-02-18	2026-02-18	…

- Extract of Service Practice Statements for Trust Services

Version	Release Date	Effective from	Effective until
250417	2025-04-17	2025-04-17	2026-02-17
20260218	2026-02-18	2026-02-18	…

- PKI Disclosure Statement

Version	Release Date	Effective from	Effective until
250414	2025-04-14	2025-04-14	2026-02-17

260218	2026-02-18	2026-02-18	…

- Service Policy for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	…

- Service Policy for Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-08-22
250724	2025-07-24	2025-08-23	2025-11-05
251007	2025-10-07	2025-11-06	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Qualified Certificate Services

Version	Release Date	Effective from	Effective until
250310	2025-03-10	2025-03-10	2026-02-17
260218	2026-02-18	2026-02-18	2026-04-14
260415	2026-04-15	2026-04-15	…

- Service Practice Statement for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Policy for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	…

- Mass Revocation Plan

Version	Release Date	Effective from	Effective until
v01	2025-11-06	2025-11-06	…

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

Findings with regard to ETSI EN 319 401:

7.9.3 Reporting

NETLOCK monitoring alerted that an OCSP certification expiry however the alert has not been remeditated in time as an incident occured. [REQ-7.9.3-03]

7.9.3 Reporting

The incident has not been communicated in 24 hours. [REQ-7.9.3-01]

7.9.1 Monitoring and logging

NETLOCK has a compley ,monitoring systems for its network and information systems, however its need development to become more automated to minimize risks. [REQ-7.9.1-07]

7.9.2 Incident response

NETLOCK has a incident management process and documentation however it requires optimalization to receive the reports in time. [REQ-7.9.2-11]

Findings with regard to ETSI EN 319 411-1:

6.6.1 Certificate profile

According to RFC 5280 §4.2.2.1, AIA HTTP URIs must provide a DER-encoded certificate or a DER/BER CMS “certs-only” container, therefore serving PEM content does not comply with the standard. [GEN-6.6.1-01]

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.

- Bug1978904, NETLOCK: Add NETLOCK's S/MIME & TLS Root https://bugzilla.mozilla.org/show_bug.cgi?id=1978904
- Bug 2001327, NETLOCK: Missing CDP Disclosure in CCADB https://bugzilla.mozilla.org/show_bug.cgi?id=2001327
- Bug 2004699, NETLOCK: CA in AIA in PEM format https://bugzilla.mozilla.org/show_bug.cgi?id=2004699
- Bug 2007948, NETLOCK: Full Incident Report was not published within 14 days of notification https://bugzilla.mozilla.org/show_bug.cgi?id=2007948
- Bug 2011314, Netlock: unspecifed revocation code (0) in CRL https://bugzilla.mozilla.org/show_bug.cgi?id=2011314
- Bug 2021559, NETLOCK: Unavailability of the document repository https://bugzilla.mozilla.org/show_bug.cgi?id=2021559
- Bug 2013400, NETLOCK: did not file a preliminary incident report or respond to a third-party report within the 72-hour timeframe https://bugzilla.mozilla.org/show_bug.cgi?id=2013400
- Bug 2013395, NETLOCK: Missing Related Incidents section in the bug report https://bugzilla.mozilla.org/show_bug.cgi?id=2013395
- Bug 2032939, NETLOCK: Transition Plan for Mozilla Root Store Policy 7.5 by Deadline https://bugzilla.mozilla.org/show_bug.cgi?id=2032939
- Bug, 2033033, NETLOCK: Transition Plan for Existing Dual-Purpose Root https://bugzilla.mozilla.org/show_bug.cgi?id=2033033
- Bug 2051459, NETLOCK: OCSP Service Returning Error for Issued Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=2051459
- Bug 2052541, NETLOCK: Failure to Respond to a Certificate Problem Report Within 24 Hours https://bugzilla.mozilla.org/show_bug.cgi?id=2052541
- Bug 1979287, NETLOCK: Expired Test Website Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=1979287
- Bug 1947691, NETLOCK: Bug 1891331 replacement - delayed revocation - https://bugzilla.mozilla.org/show_bug.cgi?id=1947691

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

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = NetLock Platina (Class Platinum) Főtanúsítvány, O = NetLock Kft., C = HU	SHA-256 fingerprint of the certificate: EB7E05AA58E7BD328A282BF8867033F3C035342B516EE85C01673DFFFFBBFE58	ETSI EN policy that this Root has been assessed against: 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
Complete subject DN: CN = NETLOCK Domain Validated CA, O = NETLOCK Ltd., C = HU	SHA-256 fingerprint of the certificate: A1663E37B8992D819C69FB89707065CABDFE3D53C278FC3EC2601001798602F8	ETSI EN policy that this Root has been assessed against: 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 V2.6.1 (2025-06) • ETSI EN 319 411-1 V1.5.1 (2024-12) • ETSI EN 319 401 V3.2.1 (2026-01) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Chrome Root Program Policy, Version 1.8 (2026-02-05) • Mozilla Root Store Policy, Version 3.1 (2026-07-01) • Microsoft Trusted Root Certificate Program (2025-02-25) • 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 V1.3.1 (2023-03)

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

- General Terms and Conditions

Version	Release Date	Effective from	Effective until
250625	2025-06-25	2025-06-25	2025-12-13
251214	2025-12-14	2025-12-14	2026-02-17
260218	2026-02-18	2026-02-18	…

- Extract of Service Practice Statements for Trust Services

Version	Release Date	Effective from	Effective until
250417	2025-04-17	2025-04-17	2026-02-17
20260218	2026-02-18	2026-02-18	…

- PKI Disclosure Statement

Version	Release Date	Effective from	Effective until
250414	2025-04-14	2025-04-14	2026-02-17
260218	2026-02-18	2026-02-18	…

- Service Policy for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Non-Qualified Certification Services

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	
…	…	…	…

- Service Policy for Qualified Certification Services

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-08-22
250724	2025-07-24	2025-08-23	2025-11-05
251007	2025-10-07	2025-11-06	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-05-24
260525	2026-05-25	2026-05-25	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Practice Statement for Qualified Certificate Services

Version	Release Date	Effective from	Effective until
250310	2025-03-10	2025-03-10	2026-02-17
260218	2026-02-18	2026-02-18	2026-04-14
260415	2026-04-15	2026-04-15	…

- Service Practice Statement for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250517	2025-05-17	2025-05-17	2025-12-27
251228	2025-12-28	2025-12-28	2026-02-17
260218	2026-02-18	2026-02-18	2026-07-21
260722	2026-06-22	2026-07-22	…

- Service Policy for Non-eIDAS Certification Service

Version	Release Date	Effective from	Effective until
250409	2025-04-09	2025-04-09	2026-02-17
260218	2026-02-18	2026-02-18	…

- Mass Revocation Plan

Version	Release Date	Effective from	Effective until
v01	2025-11-06	2025-11-06	…

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

Findings with regard to ETSI EN 319 401:

7.9.3 Reporting

NETLOCK monitoring alerted that an OCSP certification expiry however the alert has not been remeditated in time as an incident occured. [REQ-7.9.3-03]

7.9.3 Reporting

The incident has not been communicated in 24 hours. [REQ-7.9.3-01]

7.9.1 Monitoring and logging

NETLOCK has a compley ,monitoring systems for its network and information systems, however its need development to become more automated to minimize risks. [REQ-7.9.1-07]

7.9.2 Incident response

NETLOCK has a incident management process and documentation however it requires optimalization to receive the reports in time. [REQ-7.9.2-11]

Findings with regard to ETSI EN 319 411-1:

6.6.1 Certificate profile

According to RFC 5280 §4.2.2.1, AIA HTTP URIs must provide a DER-encoded certificate or a DER/BER CMS “certs-only” container, therefore serving PEM content does not comply with the standard. [GEN-6.6.1-01]

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.

- Bug1978904, NETLOCK: Add NETLOCK's S/MIME & TLS Root https://bugzilla.mozilla.org/show_bug.cgi?id=1978904
- Bug 2001327, NETLOCK: Missing CDP Disclosure in CCADB https://bugzilla.mozilla.org/show_bug.cgi?id=2001327
- Bug 2004699, NETLOCK: CA in AIA in PEM format https://bugzilla.mozilla.org/show_bug.cgi?id=2004699
- Bug 2007948, NETLOCK: Full Incident Report was not published within 14 days of notification https://bugzilla.mozilla.org/show_bug.cgi?id=2007948
- Bug 2011314, NETLOCK: unspecifed revocation code (0) in CRL https://bugzilla.mozilla.org/show_bug.cgi?id=2011314
- Bug 2021559, NETLOCK: Unavailability of the document repository https://bugzilla.mozilla.org/show_bug.cgi?id=2021559
- Bug 2013400, NETLOCK: did not file a preliminary incident report or respond to a third-party report within the 72-hour timeframe https://bugzilla.mozilla.org/show_bug.cgi?id=2013400
- Bug 2013395, NETLOCK: Missing Related Incidents section in the bug report https://bugzilla.mozilla.org/show_bug.cgi?id=2013395
- Bug 2032939, NETLOCK: Transition Plan for Mozilla Root Store Policy 7.5 by Deadline https://bugzilla.mozilla.org/show_bug.cgi?id=2032939
- Bug, 2033033, NETLOCK: Transition Plan for Existing Dual-Purpose Root https://bugzilla.mozilla.org/show_bug.cgi?id=2033033
- Bug 2051459, NETLOCK: OCSP Service Returning Error for Issued Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=2051459
- Bug 2052541, NETLOCK: Failure to Respond to a Certificate Problem Report Within 24 Hours https://bugzilla.mozilla.org/show_bug.cgi?id=2052541
- Bug 1979287, NETLOCK: Expired Test Website Certificate https://bugzilla.mozilla.org/show_bug.cgi?id=1979287
- Bug 1947691, NETLOCK: Bug 1891331 replacement - delayed revocation - https://bugzilla.mozilla.org/show_bug.cgi?id=1947691

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

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = NETLOCK Root ECC CA, O = NETLOCK Kft., C = HU	SHA-256 fingerprint of the certificate: 00F12C1ECFE26D34A28FC6BF9FB35085302C7D53A9AC3588ED7CD86C9C7423AA	ETSI EN policy that this Root has been assessed against: 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 n 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
Complete subject DN: NETLOCK Trust Qualified ECC CA 2026	SHA-256 fingerprint of the certificate: 05EE261E9FF93FA261CA51174B54A2B95DBAE6024D221663A1E0590B1A1A5BB1	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
NETLOCK Trust Advanced ECC CA 2026	D5893410DA88054289FBD9B03DB26A75B669A23F6A33DC3F7A1D61D2615E86D7	ETSI EN 319 411-1 V1.3.1, LCP
NETLOCK Trust Advanced Plus ECC CA 2026	DB58B42A5AD846BA520C79F454AC506EA4B32D1DD83962B2741437253AA01D1F	ETSI EN 319 411-1 V1.3.1, LCP
NETLOCK Trust ECC CA 2026	D0955697ECBA930013AA3BE4CFA6BFAE9DCAEAF256A3DA53CB241AE316AB5568	ETSI EN 319 411-1 V1.3.1, LCP, NCP, NCP+
NETLOCK Trust Qualified QSCD ECC CA 2025	63288D82F29D8630FDD6DEA5A4D54882690F14E3323322F163C89E3C0AF2EA9C	X509v3 Any Policy
NETLOCK Trust Qualified RQSCD VRA ECC CA 2025	DB005D09D59F952F80FA2848FC179754DD4015061ACB696728846062E522E4DE	X509v3 Any Policy

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

Modifications record

Version	Issuing Date	Changes
Version 1	2026-07-24	Initial attestation
Version 1.2	2026-11-18	Minor documentation update audit period

End of the audit attestation letter.