TLS BR Audit Attestation for

Digi- ja väestötietovirasto (DVV)

Reference: 071026-2-AL

Thessaloniki, 2026-10-07

To whom it may concern,

This is to confirm that “QMSCERT Audits Inspections Certifications S.A. (Q-CERT S.A.)” has audited the CAs of the Digi- ja väestötietovirasto (DVV) with critical findings.

This present Audit Attestation Letter is registered under the unique identifier number 071026-2-AL covers multiple Root-CAs and consists of 11 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Q-CERT S.A.
5, Maria Kallas Str.
555 35 Pylaia, Thessaloniki, Greece
E-Mail: ict-certification@qmscert.com
Phone: +30 2310 443041

With best regards,

ELENI BAKIRTZI
Digitally signed by ELENI BAKIRTZI
Date: 2026.10.07 12:39:34 +03'00'

Eleni Bakirtzi
Head of Conformity Assessment Body

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• QMSCERT Audits Inspections Certifications S.A. (Q-CERT S.A.), 5 Maria Kallas Str., 555 35, Pylaia, Thessaloniki, Greece, registered under nº 042094606000 • Accredited by ACCREDIA under registration no. 01326[1] for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.2.2 (2015-08)" / "ETSI EN 319 403-1 V2.3.1 (2020-06)". • Insurance Carrier (BRG section 8.2): AIG Europe S.A., Policy No. P2301004773 • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: Two (2) • 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:

[1] https://services.accredia.it/ppsearch/accredia_orgmask.jsp?ID_LINK=1733&area=310&PPSEARCH_ORG_SEARCH_MASK_ORG=3761&PPSEARCH_ORG_SEARCH_MASK_SCHEMI=&PPSEARCH_ORG_SEARCH_MASK_SCHEMI_ALTRI=&PPSEARCH_ODC_SEARCH_MASK_SETTORE_ACCR=&PPSEARCH_ORG_SEARCH_MASK_CITTA=&PPSEARCH_ORG_SEARCH_MASK_PROVINCIA=&PPSEARCH_ORG_SEARCH_MASK_REGIONE=&PPSEARCH_ORG_SEARCH_MASK_STATO=&orgtype=all&PPSEARCH_ORG_SEARCH_MASK_SCOPO=&PPSEARCH_ORG_SEARCH_MASK_PDFACCREDITAMENTO=&submitBtn=Cerca

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: Two (2) • 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):	Digi- ja väestötietovirasto (DVV), Lintulahdenkuja 2, 00531, Helsinki, Finland registered under 0245437-2

Type of audit:	☒ Period of time, full audit
Audit period covered for all policies:	2025-07-11 to 2026-07-10

Point in time date:	none, as audit was a period of time audit
Audit dates:	2026-04-27 (remotely) 2026-05-04 to 2026-05-07 (on site) 2026-07-14 (remotely)
Audit location:	Helsinki, Finland

Root 1: VRK Gov. Root CA - G2

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 1.7 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:

- [CP] CERTIFICATE POLICY SERVICE CERTIFICATES, version 1.8, as of 2025-09-15.
- [CPS] CERTIFICATION PRACTICE STATEMENT FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY'S SERVER CERTIFICATES, version 1.8, as of 2025-09-15.

No major or minor non-conformities have been identified during the audit.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=VRK Gov. Root CA - G2,OU=Varmennepalvelut,OU=Certification Authority Services,O=Vaestorekisterikeskus CA,C=FI	34FF2A4409DC1383E9F8966E8ADFE5719EBA373FD0AD5E2F49F90EE07CF5D4C1	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

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=VRK Gov. CA for Citizen Certificates - G3,OU=Valtion kansalaisvarmenteet,O=Vaestorekisterikeskus CA,C=FI	39A835B14B6B6313F778371C79CB434DD518C8FD325B749D9BE669DFF20384E8	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=VRK CA for Organisational Certificates - G3,OU=Organisaatiovarmenteet,O=Vaestorekisterikeskus CA,C=FI	9C0B9EBEA95590D0FAFE4A46C62E49DD0BA6CC0A80F89019A23D037E1A4C1B5B	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=VRK CA for Social Welfare and Healthcare Prof. Certs,OU=Sosiaali- ja terveydenhuollon ammattivarmenteet,O=Vaestorekisterikeskus CA,C=FI	0E839EE68B1EEF721D31E62E589E692C03180FAADADE48A71837C25090B3ACC4	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=VRK CA for Social Welfare and Healthcare Service Providers - G2,OU=Sosiaali- ja terveydenhuollon palveluvarmenteet,O=Vaestorekisterikeskus CA,C=FI	A6B34F7B0E87446362BB1A2BF3EE95DD56D8BA97A9FFB03DF41031377ECDD6F8	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=VRK CA for Service Providers - G4,OU=Palveluvarmenteet,O=Vaestorekisterikeskus CA,C=FI	1BD3870B842FF0A637284268017E18E455A7FD2D84468F3CDF7D587C7AB35C9D	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

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

Root 2: DVV Gov. Root CA - G3 RSA

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 2.0.5 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:

- [CP] CERTIFICATE POLICY SERVICE CERTIFICATES G3, version 1.5, as of 2025-01-08.
- [CPS] CERTIFICATION PRACTICES FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY’S SERVICE CERTIFICATES, version 1.7, as of 2025-11-01.

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

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.1.1 - Reasons for Revoking a Subscriber Certificate

During the assessment of the incident reported under Mozilla Bugzilla 2032481, it was identified that a population of TLS server certificates had been issued with certificate profiles that did not conform to the applicable CA/Browser Forum Baseline Requirements. DVV identified the affected certificate population and implemented corrective changes to the certificate profiles on 09/02/2026. Examination of certificate samples issued before and after the corrective action confirmed that the identified profile issue was corrected for subsequent certificate issuance.

However, the certificates issued prior to the corrective action and identified by DVV as affected were not revoked. The applicable CA/Browser Forum Baseline Requirements require the CA to revoke a Subscriber Certificate when the CA obtains evidence that the certificate was not issued in accordance with the applicable requirements or the CA's Certificate Policy or Certification Practice Statement.

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

- Bug 2032481, Digi- ja väestötietovirasto Misissuance detected by PKIMetal https://bugzilla.mozilla.org/show_bug.cgi?id=2032481

The remediation measures taken by Digi- ja väestötietovirasto as described on Bugzilla (see link above) have been checked by the auditors and did not properly address the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=DVV Gov. Root CA - G3 RSA,OU=Varmennepalvelut,OU=Certification Authority Services,O=Digi- ja vaestotietovirasto CA,C=FI	D3ED3FC40AD26B52E001E1E18F4B9449529DEB75A81D5EB680D7B62DB23BA96D	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-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=DVV Citizen Certificates - G4R,OU=Valtion kansalaisvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	2176C05E69EE24946A140D13F9EFA222B3F1E768E1E2A67B313969CC03B82064	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Organisational Certificates - G4R,OU=Organisaatiovarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	DFC3E965176F883A9CF0F68CEAEEAB663EDFD8E79DE3294373C28A856984006F	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Social Welfare and Healthcare Prof. Certificates - G2R,OU=Sosiaali- ja terveydenhuollon ammattivarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	6073359DE6BDFBF83874CBD53D4BDE3D8165A8E7A9F772F02A7C6A48A8E7B77B	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R,OU=Sosiaali- ja terveydenhuollon tilapaisammattivarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	6E73C6A3422AE3BB37AF6D3933092A1F6959C09EB17F0A7E14F539665F50C949	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Social Welfare and Healthcare Service Certificates - G3R,OU=Sosiaali- ja terveydenhuollon palveluvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	9D433C237C3AEE7A676C9A2ED4ECCB9E40ED17914655571624F0A89969B634BF	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Service Certificates - G5R,OU=Palveluvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	46319C69041DB9A0D93DAE802E3002CC615365931FE0976D392E8863E3F3BE31	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Temporary Certificates - G3R,OU=Tilapaisvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	428089726472CA75A47F8E011AEB6483036973C72CF05478953B2FC2E012B731	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

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

Root 3: DVV Gov. Root CA - G3 ECC

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.8 • Network and Certificate System Security Requirements, version 2.0.5 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:

- [CP] CERTIFICATE POLICY SERVICE CERTIFICATES G3, version 1.5, as of 2025-01-08.
- [CPS] CERTIFICATION PRACTICES FOR THE DIGITAL AND POPULATION DATA SERVICES AGENCY’S SERVICE CERTIFICATES, version 1.7, as of 2025-11-01

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

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.1.1 - Reasons for Revoking a Subscriber Certificate

During the assessment of the incident reported under Mozilla Bugzilla 2032481, it was identified that a population of TLS server certificates had been issued with certificate profiles that did not conform to the applicable CA/Browser Forum Baseline Requirements. DVV identified the affected certificate population and implemented corrective changes to the certificate profiles on 09/02/2026. Examination of certificate samples issued before and after the corrective action confirmed that the identified profile issue was corrected for subsequent certificate issuance.

However, the certificates issued prior to the corrective action and identified by DVV as affected were not revoked. The applicable CA/Browser Forum Baseline Requirements require the CA to revoke a Subscriber Certificate when the CA obtains evidence that the certificate was not issued in accordance with the applicable requirements or the CA's Certificate Policy or Certification Practice Statement.

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

- Bug 2032481, Digi- ja väestötietovirasto Misissuance detected by PKIMetal https://bugzilla.mozilla.org/show_bug.cgi?id=2032481

The remediation measures taken by Digi- ja väestötietovirasto as described on Bugzilla (see link above) have been checked by the auditors and did not properly address the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=DVV Gov. Root CA - G3 ECC,OU=Varmennepalvelut,OU=Certification Authority Services,O=Digi- ja vaestotietovirasto CA,C=FI	5546A52504FBA74F61FFD4890067529ADE3B9C9D07E502592831CCDA9B369FD3	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

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
CN=DVV Citizen Certificates - G4E,OU=Valtion kansalaisvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	AAD1BEAC4696102A88BF9D518D64F8B014F78F9B152579C959998313197924D7	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Organisational Certificates - G4E,OU=Organisaatiovarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	8FDBDCCB5820F1C79EF8BCE190E2B3CD2CC3D0B6BD8311B1F75FBD48BBC230D4	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Social Welfare and Healthcare Prof. Certificates - G2E,OU=Sosiaali- ja terveydenhuollon ammattivarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	A155B9FB8A372683A3825054F9A5265C55430A68616BAD8A1726E70F09F95A26	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Social Welfare and Healthcare Service Certificates - G3E,OU=Sosiaali- ja terveydenhuollon palveluvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	A5C53CF6843A395E6EC244E9B27D58413295428DED97586FD4F67AA4AB8D49A0	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w
CN=DVV Service Certificates - G5E,OU=Palveluvarmenteet,O=Digi- ja vaestotietovirasto CA,C=FI	93C176167ECA02A1B262B16517AC5FB5FC25D3568D97ECDDD04E3A6126B6C7BA	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

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

Modifications record

Version	Issuing Date	Changes
Version 1	2026-10-07	Initial attestation

End of the audit attestation letter.