TLS EV Audit Attestation for

DigiCert Europe Netherlands B.V.

Reference: ETS-010/ETS-030

Amsterdam, 2024-09-04

To whom it may concern,

This is to confirm that BSI Group The Netherlands B.V has audited the CAs of DigiCert Europe Netherlands B.V. without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number ETS-010/ETS-030 covers a single Root-CA and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

BSI Group The Netherlands B.V
John M. Keynesplein 9
1066 EP Amsterdam
Netherlands
E-Mail: info.nl@bsigroup.com
Phone: +31 20 3460780

With best regards,

Denelise L'Ecluse (Sep 12, 2024 10:40 GMT+2)

Denelise L'Ecluse
Managing Director Assurance –
Continental Europe

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- BSI Group The Netherlands B.V, John M. Keynesplein 9, 1066 EP Amsterdam, Netherlands, registered under trade registration number 33264284
- Accredited by Dutch Accreditation Council (RvA) under C646[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):
  Marsh Ltd is providing the professional liability insurance coverage.
- Third-party affiliate audit firms involved in the audit:
  None.

Identification and qualification of the audit team

- Number of team members: 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:
  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] https://www.rva.nl/en/alle-geaccrediteerden/c646/

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):	DigiCert Europe Netherlands B.V., Nevelgaarde 56, 3436 ZZ Nieuwegein Registered under: 30237459

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:	2023-06-01 to 2024-05-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-03-04 to 2024-03-29 2024-05-30 to 2024-05-31 2024-06-10 to 2024-06-14
Audit location:	Nieuwegein and Amsterdam, The Netherlands

Root 1: QuoVadis Root CA 2 G3

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, v2.0.2. • Guidelines for the Issuance and Management of Extended Validation Certificates, v1.8.1 Browser Policy Requirements: • Mozilla Root Store Policy, version 2.9 • Microsoft Trusted Root Program, Program Requirements • Google Chrome Root Program Policy, Version 1.5 • Apple Root Certificate Program Other (subordinate to the listed European Standards): • ETSI TS 119 495 v1.6.1 (2022-11) 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:

- DigiCert Europe/QuoVadis - Certification Policy/Certification Practice Statement, v5.2, 1 March 2024
- DigiCert Europe/QuoVadis - PKI Disclosure Statement, v2.0, 22 November, 2023

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

Findings with regard to ETSI EN 319 401:

7.6 Physical Security

The implementation of restricting physical access shall be improved. [ETSI EN 319401 REQ-7.6-02]

7.8 Network Security

The documentation of firewall rule reviews shall be improved [ETSI EN 319401 REQ-7.8-06]

Findings with regard to ETSI EN 319 411-1:

6.3.10 Certificate status services

The external monitoring implementation of the certificate status services shall be improved (ETSI EN 319411-1 CSS-6.3.10-10, CSS-6.3.10-02)

Findings with regard to ETSI EN 319 411-2:

None.

All listed minor non-conformities have been closed before the issuance of this attestation.

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

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=QuoVadis Root CA 2 G3,O=QuoVadis Limited,C=BM	8FE4FB0AF93A4D0D67DB0BEBB23E37C71BF325DCBCDD240EA04DAF58B47E1840	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP

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=QuoVadis Qualified Web ICA G2,O=QuoVadis Trustlink B.V.,C=NL	7FEB9374EAB08D392717C647436DAE06176A24C010607FDA1CCE5E5F0106B472	ETSI EN 319 411-2 V2.4.1, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP ETSI TS 119 495 V1.6.1, QCP-w /QCP-w-psd2

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

Modifications record

Version	Issuing Date	Changes
Version 1	2024-08-22	Initial attestation

End of the audit attestation letter.