SMIME BR Audit Attestation for

DigiCert Europe Netherlands B.V., DigiCert Europe Belgium B.V.

Reference: PCEB-N 26/03/02

"Prague, 2026-03-31"

To whom it may concern,

This is to confirm that "TAYLLORCOX PCEB established by TAYLLORCOX s.r.o." has audited the CAs of the "DigiCert Europe Netherlands B.V., DigiCert Europe Belgium B.V." without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PCEB-N 26/03/02" covers multiple Root-CAs and consists of 16 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

TAYLLORCOX PCEB established by TAYLLORCOX s.r.o.
Křižíkova 2136/2a
186 00 Prague 8, Czech Republic
E-Mail: audit@tayllorcox.com
Phone: +420 725 536 797

With best regards,

Ing. Martin Dudek
Lead auditor

This attestation is based on the template version 3.4 as of 2025-07-08, 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
• TAYLLORCOX PCEB established by TAYLLORCOX s.r.o., Křižíkova 2136/2a, 186 00 Prague 8, Czech Republic, registered under company ID 0027902587. • Accredited by Český institut pro akreditaci, o.p.s. (Czech Accreditation Institute) under registration https://www.cai.cz/?subjekt=3239-tayllorcox-s-ro&lang=en[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): Allianz pojišťovna, a.s., Ke Štvanici 656/3 186 00 Praha 8, Czech Republic, registered under company national ID 47115971. • 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;

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

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):	DigiCert Europe Netherlands B.V., DigiCert Europe Belgium B.V. **DigiCert Europe Netherlands B.V.** Nevelgaarde 56 Noord 3436 ZZ Nieuwegein Netherlands registered under NTRNL-30237459, **DigiCert Europe Belgium B.V.** Schaliënhoevedreef 20T 2800 Mechelen Belgium registered under VATBE-0537698318.

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:	2025-01-01 to 2025-12-31
Point in time date:	none
Audit dates:	2025-10-20 to 2025-12-31 2026-03-31 (finalising of report)
Audit location:	CAB office – validation of TSP documentation, DigiCert Europe NL, BE branches - providing evidence for audit purposes (remotely)

Root 1: QUOVADIS ROOT CA 1 G3

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • 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 S/MIME Certificates, version 1.0.12 • 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) • ETSI TS 119 403-3 V1.1.1 (2019-03)

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

- CP/CPS for Trust Anchor Root CA (Private), version 1.0 (7 March 2016)
- DigiCert Europe CP/CPS, version 6.08 (24 October 2025)
- DigiCert Europe/QuoVadis PKI Disclosure Statement v2.02 (30 May 2025)

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

Findings with regard to ETSI EN 319 401:
None.

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

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

During the audit period, no S/MIME certificates (as defined in the S/MIME Baseline Requirements) were issued by the audited PKI infrastructure mentioned in the report.

All 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 audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = QuoVadis Root CA 1 G3, O = QuoVadis Limited, C = BM	8A866FD1B276B57E578E921C65828A2BED58E9F2F288054134B7F1F4BFC9CC74	

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 = DigiCert QuoVadis G3 Qualified Europe RSA4096 SHA256 2023 CA1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	B36425F1491B2EE08EC87B69C23EA6A76EBF769C4C34FE3798A4CB9A1990E070	ETSI EN 319 411-1 V1.3.1, NCP, NCP+ ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-QSCD
CN = DigiCert QuoVadis G3 Qualified BE RSA4096 SHA256 2023 CA1, 2.5.4.97 = NTRBE-0537698318, O = DigiCert Europe Belgium B.V., C = BE	2CB07880B4E584F366E083791511BB48812FF5164C5BA3BBB3C1688AA456B13C	ETSI EN 319 411-1 V1.3.1, NCP, NCP+ ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-QSCD
CN = QuoVadis EU Issuing Certification Authority G4, O = QuoVadis TrustLink B.V., C = NL	1D24222B5EEC71FE99BE9D700FA5FF72312DB3EB0FCB4A4F3BCC135DA36C1355	ETSI EN 319 411-1 V1.3.1, NCP, NCP+ ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-l (PSD2), QCP-l-qscd (PSD2)
CN = DigiCert QuoVadis G3 Qualified BE itsme RSA4096 SHA256 2023 CA1, 2.5.4.97 = NTRBE-0537698318, C = BE	C0EE0CCED463096DF07D27257AF79C986FF92B678F669C109FFF570F32AB433F	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd
CN = DigiCert QuoVadis G3 Qualified BE itsme RIV RSA4096 256 2023 CA1, 2.5.4.97 = NTRBE-0537698318 , C = BE	A610AD2025ED0AA84259EBB9289E828267D35082430CBFB5562F3066DEBC2E88	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd

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

Root 2 QUOVADIS ROOT CA 2 G3

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • 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 S/MIME Certificates, version 1.0.12 • 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) • ETSI TS 119 403-3 V1.1.1 (2019-03)

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

- CP/CPS for Trust Anchor Root CA (Private), version 1.0 (7 March 2016)
- DigiCert Europe CP/CPS, version 6.08 (24 October 2025)
- DigiCert Europe/QuoVadis PKI Disclosure Statement v2.02 (30 May 2025)

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

Findings with regard to ETSI EN 319 401:
None.

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

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

During the audit period, no S/MIME certificates (as defined in the S/MIME Baseline Requirements) were issued by the audited PKI infrastructure mentioned in the report.

All 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 audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	8FE4FB0AF93A4D0D67DB0BEBB23E37C71BF325DCBCDD240EA04DAF58B47E1840	

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 = DigiCert QuoVadis G3 Qualified TLS RSA4096 SHA256 2023 CA1 2.5.4.97 = NTRNL-30237459 O = QuoVadis Trustlink B.V. C = NL	FE3CBED838D30BAB900184C1F21A4B27D3211CB5C9257D7E985C2AE43AC6A89F	ETSI EN 319 411-2 V2.4.1, QCP-w, QCP-w-psd2, QEVCP-w ETSI EN 319 411-1 V1.3.1, EVCP, OVCP
CN = QuoVadis Qualified Web ICA G2 O = QuoVadis Trustlink B.V. C = NL	7FEB9374EAB08D392717C647436DAE06176A24C010607FDA1CCE5E5F0106B472	ETSI EN 319 411-2 V2.4.1, QCP-w, QCP-w-psd2
CN = QuoVadis Qualified Web ICA G3 O = QuoVadis Trustlink B.V. C = NL	3F225BDBCD788CE924870CAF92F814B7C6FF4EDABABAD93F1D3A9177252CF1D1	ETSI EN 319 411-2 V2.4.1, QCP-w, QCP-w-psd2

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

Root 3: Staat der Nederlanden Root CA - G3 (not in scope but relevant to ICAs in scope of the audit)

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • 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 S/MIME Certificates, version 1.0.12 • 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) • ETSI TS 119 403-3 V1.1.1 (2019-03)

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

- QuoVadis PKIoverheid CPS v2.02 (26 May 2025)
- QuoVadis PKIoverheid PKI Disclosure Statement v1.13 (30 May 2025)

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

Findings with regard to ETSI EN 319 401:
None.

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

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

During the audit period, no S/MIME certificates (as defined in the S/MIME Baseline Requirements) were issued by the audited PKI infrastructure mentioned in the report.

All 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 audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = Staat der Nederlanden Root CA - G3, O = Staat der Nederlanden, C = NL	3C4FB0B95AB8B30032F432B86F535FE172C185D0FD39865837CF36187FA6F428	Not in scope

Table 5: Root-CA 2 (not in scope but relevant to ICAs 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	Comment
CN = Staat der Nederlanden Organisatie Services CA - G3, O = Staat der Nederlanden, C = NL	D9581DBDE99B39EEFF6CE5C80DE1650DA0C1C8A109705ED286C53BC95E6655E4	Not in scope	Domain CA not in scope but relevant to ICAs in scope of audit.
CN = DigiCert QuoVadis PKIoverheid Organisatie Services CA – 2023, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	6E25C0044C7EBB30D01A4CC3D5733D734D06CD296A6823E63527F4182D528351	PKIoverheid Programme of Requirements 5 PKIOverheid Organisation Service Authenticity (OID 2.16.528.1.1003.1.2.5.4), NCP+ PKIOverheid Organisation Service Encryption (OID 2.16.528.1.1003.1.2.5.5), NCP+ PKIOverheid Organisation Service Seal (OID 2.16.528.1.1003.1.2.5.7), QCP-l-QSCD	

Table 6: Sub-CA's issued by the Root-CA 2 or its Sub-CA's

Distinguished Name	SHA-256 fingerprint	Applied policy	Comment
CN = Staat der Nederlanden Burger CA - G3, O = Staat der Nederlanden, C = NL	2E7A0A3B0C527EB20C52253C8D2278CA108136A8CA3A4EA22DA7B59BAC90650A	Not in scope	Domain CA not in scope but relevant to ICAs in scope of audit.
CN = DigiCert QuoVadis PKIoverheid Burger CA – 2023, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	66388EE649CBE920FD949FA9B77E2AA45B5DEC4120B8FFAB371B0C9C5E38C1C1	PKIoverheid Programme of Requirements 5 PKIOverheid Personal Citizen Authenticity (OID 2.16.528.1.1003.1.2.3.1), NCP+ PKIOverheid Personal Citizen Non-Repudiation (OID 2.16.528.1.1003.1.2.3.2), QCP-n-qscd PKIOverheid Personal Citizen Encryption (OID 2.16.528.1.1003.1.2.3.3), NCP+	

Table 7: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s

Distinguished Name	SHA-256 fingerprint	Applied policy	Comment
CN = Staat der Nederlanden Organisatie Persoon CA - G3, O = Staat der Nederlanden, C = NL	8222BC4FE7A3DDCA9EF0BF0D682AC888799F87822D15332A54C0BFDFC6854F7B	Not Applicable (not in scope)	Domain CA not in scope but relevant to ICAs in scope of audit.
CN = DigiCert QuoVadis PKIoverheid Organisatie Persoon CA – 2023, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	C8C77ECF368D73214D50D88384464339E6F8E59F34B47E39E7965F4E5787CF1D	PKIoverheid Programme of Requirements 5 PKIOverheid Personal Organisation Authenticity (OID 2.16.528.1.1003.1.2.5.1), NCP+ PKIOverheid Personal Organisation Non-Repudiation (OID 2.16.528.1.1003.1.2.5.2), QCP-n-qscd PKIOverheid Personal Organisation Encryption (OID 2.16.528.1.1003.1.2.5.3), NCP+	

Table 8: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s

Distinguished Name	SHA-256 fingerprint	Applied policy	Comment
CN = Staat der Nederlanden Root CA – G1, O = Staat der Nederlanden, C = NL	0257CE27B52408E24EE2C0945640B723C5BC66DDBDA4ADA58C60357604F0E675	Not Applicable (not in scope)	Domain CA not in scope but relevant to ICAs in scope of audit.

Table 9: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s

Distinguished Name	SHA-256 fingerprint	Applied policy	Comment
CN = Staat der Nederlanden Private Personen CA - G1, O = Staat der Nederlanden, C = NL	DC49949882D6ACE7EC23520BB2A625C6F0B08F41602449E42AD7F5CE8B5D4659	Not applicable (not in scope)	Domain CA not in scope but relevant to ICAs in scope of audit.
CN = DigiCert QuoVadis PKIoverheid Private Personen CA – 2023, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	C3FB1A9E37B754E6FE2E313D8D33838E96211087958F70616F49B812FFFF6A8D	PKIoverheid PoR v5, PKIOverheid Private Personal Authenticity (OID 2.16.528.1.1003.1.2.8.1), NCP+ PKIOverheid Private Personal Non-Repudiation (OID 2.16.528.1.1003.1.2.8.2), QCP-n-qscd PKIOverheid Private Personal Encryption (OID 2.16.528.1.1003.1.2.8.3), NCP+	

Table 10: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s

Distinguished Name	SHA-256 fingerprint	Applied policy	Comment
CN = Staat der Nederlanden Private Services CA - G1 O = Staat der Nederlanden C = NL	2EAAF678E645DC26EA82C016EF3960935659CF81B4C44D9B2D0FB1A142666C98	Not applicable (not in scope)	Domain CA not in scope but relevant to ICAs in scope of audit.
CN = DigiCert QuoVadis PKIoverheid Private Services CA – 2023, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	B63A82CE98E9FE704DC42B7CB4B63D4BF0646B1D0754F9A4C696A4AFB39436BC	PKIoverheid Programme of Requirements 5 , PKIOverheid Private Services – Authenticity (OID 2.16.528.1.1003.1.2.8.4), OVCP PKIOverheid Private Services – Encryption (OID 2.16.528.1.1003.1.2.8.5), OVCP PKIOverheid Private Services – Server (OID 2.16.528.1.1003.1.2.8.6), OVCP	

Table 11: Sub-CA’s issued by the Root-CA 2 or its Sub-CA’s

Modifications record

Version	Issuing Date	Changes
Version 1	2026-03-31	Initial attestation
…	…	…

End of the audit attestation letter.