



Standard Audit Attestation for

DigiCert Europe Netherlands B.V.

DigiCert Europe Belgium B.V.

This present Audit Attestation Letter is registered under the unique identifier number “PCEB-N 25/03/02” covers multiple Root-CAs and consists of 13 pages.

Kindly find here below the details accordingly.

This Attestation Letter is also available on the website <https://pceb.tayllorcox.cz/Documents.html>.

With best regards,

Prague, 2025-03-31

Martin Dudek

Lead Auditor

GENERAL AUDIT INFORMATION

On the request of DigiCert Europe Netherlands B.V. in the Netherlands and DigiCert Europe Belgium BV in Belgium, the annual certification audit on all areas and processes was performed by CAB TAYLLORCOX PCEB.

1.1 IDENTIFICATION DATA

Identification of the CA / Trust Service Provider (TSP):

Name of TSP / Name of company	DigiCert Europe Netherlands B.V.
Identification Number	30237459
Head or place of business / residence of TSP	Nevelgaarde 56 Noord 3436 ZZ Nieuwegein, Netherlands
Web address	https://www.quovadisglobal.com/nl-en/

Identification of the CA / Trust Service Provider (TSP):

Name of TSP / Name of company	DigiCert Europe Belgium B.V.
Identification Number	BE0537698318
Head or place of business / residence of TSP	Schaliënhoevedreef 20T 2800 Mechelen Belgium
Web address	https://www.quovadisglobal.com/be-en/

Identification data of CAB

Name of CAB / Name of company	Certification body TAYLLORCOX PCEB established by TAYLLORCOX s.r.o.
Identification Number	0027902587
Accreditation number	3239
Head or place of business / residence of CAB	Na Florenci 1055/35, 110 00 Praha 1
Electronic address	audit@tayllorcox.com
Web address	www.tayllorcox.com
Represented by	Ing. Radek Nedvěď, director
Scope of Accreditation	See Attachments on: https://www.cai.cz/?subjekt=3239-tayllorcox-s-r-o&lang=en
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 data of NAB which accredited CAB	
Name of National Accreditation Body (EN)	Český institut pro akreditaci, o.p.s. (Czech Accreditation Institute)
Identification Number	25677675
Head or place of business	Olšanská 54/3, 130 00 Praha 3
Electronic address	mail@cai.cz
Web address	www.cai.cz
Accreditation scheme	See document MPA: „K aplikaci ČSN EN ISO/IEC 17065:2013. Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby v akreditačním systému České republiky“, chapter 4, point 9 „Certifikace poskytovatelů služeb vytvářejících důvěru“. NAB MPA documents are on: https://www.cai.cz/?page_id=2961

1.2 IDENTIFICATION AND QUALIFICATION OF THE AUDIT TEAM

Number of team members	4
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	The competences of the audit team are specified by the contract and accreditation standards EN ISO/IEC 17065 and ETSI EN 319 403-1.
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, interviewing skills and effective communication; and the relevant knowledge and

	professional and personal attributes required and necessary to perform audits in defined roles.
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 through its internal procedures that its auditing staff maintain competence based on appropriate education, training or experience.
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	The Code of Conduct is implemented in accordance with Annex A, ETSI EN 319 403 or ETSI EN 319 403-1.

1.3 IDENTIFICATION AND QUALIFICATION OF THE REVIEWER PERFORMING AUDIT QUALITY MANAGEMENT

Number of Reviewers/Audit Quality Managers involved independent from the audit team	1
Note: 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.	

MAIN GOALS OF AUDIT

The full audit covered all relevant requirements from the audit criteria listed below (see "Information on the audit") as described in the eIDAS audit report No.: PCEB-N 24/12/02 dated 31.3.2025.

The scope of the assessment comprised the following Trust Service Provider component services:

- Registration Service;
- Certificate Generation Service;
- Dissemination Service;
- Revocation Management Service;
- Revocation Status Service;
- Subject Device Provision Service;

This includes operating a remote QSCD / SCDev, where electronic signature creation data is generated and managed on behalf of the signatory.

The TSP component services are performed, partly or completely by subcontractors under the final responsibility of QuoVadis.

These TSP component services are being provided for the following qualified trust service(s) as defined in Regulation (EU) 910/2014 (eIDAS):

- Issuance of qualified certificates for electronic signatures (qualified trust service), in accordance with the policies: QCP-n, QCP-n-qscd
- Issuance of qualified certificates for electronic seals (qualified trust service), in accordance with the policy: QCP-I, QCP-I-qscd
- Issuance of qualified certificates for website authentication (qualified trust service), in accordance with policies QEVCP-w, QCP-w-psd2;

1.4 POLICY AND PRACTICE STATEMENT

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

- digicert-europe-cpcps-v-6-0-en.pdf (DigiCert Europe CP/CPS)
- digicert-europe-pki-disclosure-statement-v2-0-en.pdf (DigiCert Europe / DigiCert PKI Disclosure Statement)
- DigiCert-pkio-disclosure-statement-v1-13-en.pdf (DigiCert + DigiCert PKI Disclosure Statement for PKIoverheid)
- digicert-pkioverheid-cps-v-2-0-en.pdf (DigiCert Certification Practice Statement for PKIoverheid Certificates)

1.5 AUDIT CRITERIA

The following standards and metrics were determined to assess the individual service requirements.

Identification of Standards	Definition of Standards (description)
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS), to the extent of the service requirements specified in Chapter 1.1 of this report and in the ETSI EN 319 403-1 V2.3.1 in conjunction with document DKP v.4 and ETSI standards
Standards	Standards to which the eIDAS Regulation refers or is recommended as a guide to meet its requirements, in current versions: ETSI EN 319 401 V2.3.1 (2021-05) / ETSI EN 319 401 V3.1.1 (2024-06) ETSI EN 319 411-1 V1.4.1 (2023-10) ETSI EN 319 411-2 V2.5.1 (2023-10) ETSI EN 319 412-1 V1.5.1 (2023-09) ETSI EN 319 412-2 V2.3.1 (2023-09) ETSI EN 319 412-3 V1.3.1 (2023-09) ETSI EN 319 412-4 V1.3.1 (2023-09) ETSI EN 319 412-5 V2.4.1 (2023-09) ETSI TS 119 495 V1.6.1 (2022-11) / ETSI TS 119 495 V1.7.1 (2024-07) ETSI TS 119 461 V1.1.1 (2021-07) ETSI TS 119 312 V1.4.2 (2022-02) CA/Browser Forum – Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates 2.0.2 (8 January 2024) CA/Browser Forum – Guidelines for the Issuance and Management of Extended Validation Certificates v1.8.0 (30 November 2022) CA/Browser Forum - Network and Certificate System Security Requirements v1.7 (5 April 2021) PKIoverheid - Programma van Eisen v4.12 / v5.0 (https://www.logius.nl/english/pkioverheid)

HIERARCHICAL STRUCTURE OF CERTIFYING AUTHORITIES FOR THE SERVICES

The certificates are issued through the issuing certification authorities, as specified below:

1.6 PKIOVERHEID

1.6.1 DIGICERT QUOVADIS PKIOVERHEID ORGANISATIE PERSOON CA - 2023

Root CA: Staat der Nederlanden Root CA – G3 (not in scope)

Domein: Staat der Nederlanden Organisatie Persoon CA – G3 (not in scope)

Issuing CA	SHA-256 fingerprint
DigiCert QuoVadis PKIoverheid Organisatie Persoon CA - 2023	C8C77ECF368D73214D50D88384464339E6F8E59F34B47E39E7965F4E5787CF1D

Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Personal Organisation Non-Repudiation	QCP-n-qscd	2.16.528.1.1003.1.2.5.2

1.6.2 DIGICERT QUOVADIS PKIOVERHEID ORGANISATIE SERVICES CA - 2023

Root CA: Staat der Nederlanden Root CA – G3 (not in scope)

Domein: Staat der Nederlanden Organisatie Services CA - G3 (not in scope)

Issuing CA	SHA-256 fingerprint
DigiCert QuoVadis PKIoverheid Organisatie Services CA - 2023	6E25C0044C7EBB30D01A4CC3D5733D734D06CD296A6823E63527F4182D528351

Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Organisation Service Seal	QCP-l-qscd	2.16.528.1.1003.1.2.5.7

1.6.3 DIGICERT QUOVADIS PKIOVERHEID BURGER CA - 2023

Root CA: Staat der Nederlanden Root CA – G3 (not in scope)

Domein: Staat der Nederlanden Burger CA - G3 (not in scope)

Issuing CA	SHA-256 fingerprint
DigiCert QuoVadis PKIoverheid Burger CA - 2023	66388EE649CBE920FD949FA9B77E2AA45B5DEC4120B8FFAB371B0C9C5E38C1C1

Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Personal Citizen Non-Repudiation	QCP-n-qscd	2.16.528.1.1003.1.2.3.2

1.6.4 DIGICERT QUOVADIS PKIOVERHEID PRIVATE PERSONEN CA - 2023

Root CA: Staat der Nederlanden Private Root CA - G1 (not in scope)

Domein: Staat der Nederlanden Private Personen CA - G1 (not in scope)

Issuing CA	SHA-256 fingerprint
DigiCert QuoVadis PKIoverheid Private Personen CA - 2023	C3FB1A9E37B754E6FE2E313D8D33838E96211087958F70616F49B812FFFF6A8D

Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Private Personal Non-Repudiation	QCP-n-qscd	2.16.528.1.1003.1.2.8.2

1.7 DIGICERT QUOVADIS

Certificates are issued through the Certification Authorities as specified below.

1.7.1 ROOT QUOVADIS ROOT CA 1 G3

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

1.7.1.1 QUALIFIED NATURAL PERSON CERTIFICATES

Issuing CA	SHA-256 fingerprint		
DigiCert QuoVadis G3 Qualified Europe RSA4096 SHA256 2023 CA1	B36425F1491B2EE08EC87B69C23EA6A76EBF769C4C34FE3798A4CB9A1990E070		
Certificates		Applicable Policy	Applicable Policy OID
eIDAS Qualified Natural Person		QCP-n	0.4.0.194112.1.0
eIDAS Qualified Natural Person		QCP-n-qscd	0.4.0.194112.1.2

Issuing CA	SHA-256 fingerprint		
DigiCert QuoVadis G3 Qualified BE RSA4096 SHA256 2023 CA1	2CB07880B4E584F366E083791511BB48812FF5164C5BA3BBB3C1688AA456B13C		
Certificates		Applicable Policy	Applicable Policy OID
eIDAS Qualified Natural Person		QCP-n	0.4.0.194112.1.0
eIDAS Qualified Natural Person		QCP-n-qscd	0.4.0.194112.1.2

1.7.1.2 QUALIFIED LEGAL PERSON CERTIFICATES

Issuing CA	SHA-256 fingerprint		
DigiCert QuoVadis G3 Qualified Europe RSA4096 SHA256 2023 CA1	B36425F1491B2EE08EC87B69C23EA6A76EBF769C4C34FE3798A4CB9A1990E070		
Certificates	Applicable Policy	Applicable Policy OID	
eIDAS Qualified eIDAS Qualified Legal Person	QCP-I	0.4.0.194112.1.1	
eIDAS Qualified eIDAS Qualified Legal Person	QCP-I-qscd	0.4.0.194112.1.3	
eIDAS Qualified: PSD2 Legal Person	QCP-I	0.4.0.194112.1.1 0.4.0.19495.2	
eIDAS Qualified: PSD2 Legal Person	QCP-I-qscd	0.4.0.194112.1.3 0.4.0.19495.2	

Issuing CA	SHA-256 fingerprint		
DigiCert QuoVadis G3 Qualified BE RSA4096 SHA256 2023 CA1	2CB07880B4E584F366E083791511BB48812FF5164C5BA3BBB3C1688AA456B13C		
Certificates	Applicable Policy	Applicable Policy OID	
eIDAS Qualified eIDAS Qualified Legal Person	QCP-I	0.4.0.194112.1.1	
eIDAS Qualified eIDAS Qualified Legal Person	QCP-I-qscd	0.4.0.194112.1.3	

1.7.2 ROOT QUOVADIS ROOT CA 2 G3

Distinguished Name	SHA-256 fingerprint
CN = QuoVadis Root CA 2 G3, O = QuoVadis Limited, C = BM	8FE4FB0AF93A4D0D67DB0EBB23E37C71BF325DCBCDD240EA04DAF58B47E1840

1.7.2.1 QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION (PSD2)

Issuing CA	SHA-256 fingerprint		
DigiCert QuoVadis G3 Qualified TLS RSA4096 SHA256 2023 CA1	FE3CBED838D30BAB900184C1F21A4B27D3211CB5C9257D7E985C2AE43AC6A89F		
Certificates	Applicable Policy	Applicable Policy OID	
Qualified Certificate for Website Authentication	QEVCP-w	0.4.0.194112.1.4	
PSD2 Qualified certificate for website authentication	QEVCP-w and QCP-w-psd2	0.4.0.194112.1.4 and 0.4.0.19495.3.1	

1.7.3 COMPONENT SERVICES

The Registration Service was assessed, and we were able to confirm that the Registration Service (Remote Identity Proofing), based on objective evidence collected during the audit, provides equivalent assurance in terms of reliability as physical presence, according to Regulation (EU) 910/2014 (eIDAS, version 2014) Art. 24.1 sub d) or Regulation (EU) 910/2014 (eIDAS, version 2024) Art. 24.1a sub c), for trusted services (and identity verification context) covered by this certificate of conformity:

- DigiCert Remote ID Validation RIV2, supporting ETSI TS 119 461 Use Case for Unattended Remote Identity Proofing (9.2.3), Hybrid Manual and Automated Operation (9.2.3.3); and
- DigiCert Remote ID Validation RIV4, supporting ETSI TS 119 461 Use Case for Unattended Remote Identity Proofing (9.2.3), Hybrid Manual and Automated Operation (9.2.3.3).



AUDIT SUMMARY

1.8 AUDIT INFORMATION

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 / Point in time date	1 January 2024 - 31 December 2024

1.9 RESULT OF AUDIT

The result of the full audit is that, based on the objective evidence gathered during the certification audit from 21 October 2024 to 31 December 2024, we conclude that the areas assessed during the audit were generally found to be effective, as evidenced by the records of findings contained in Audit Report No. PCEB-N 24/12/02.

1.10 FINDINGS

Findings with regard to ETSI EN 319 401:

No nonconformity found

Findings with regard to ETSI EN 319 411-2:

One minor nonconformity found

Chapter 6.6.1 Certificate Profile:

Documentation of the PKI TSP certificate structure shall be improved [GEN-6.6.1-02]

1.11 SCOPE OF AUDIT / AUDIT LOCATIONS

1) DigiCert Europe Netherlands B.V.

Nevelgaarde 56 Noord
3436 ZZ Nieuwegein
The Netherlands

2) DigiCert Europe Belgium B.V.

Schaliënhoevedreef 20T
Mechelen
2800
Belgium

HISTORY

Date of issue	Comments
March 31, 2025	First version
April 3, 2025	Reclassification of findings for ETSI EN 319 401. The identified requirement for compliance with Commission Implementing Regulation (EU) 2024/2690 is not a direct requirement of the relevant standard.