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 25/03/03” covers a single Root-CA and consists of 9 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	QuoVadis TrustLink 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 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 Nedvěd, 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:

The QuoVadis Time-stamping Authority (QV-TSA) uses Public Key Infrastructure and trusted time sources to provide reliable, standards-based Electronic Timestamps. The QuoVadis Time-stamp Policy/Practice Statement (QV-TSP/PS) defines the operational and management practices of the QV-TSA such that Subscribers and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

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

- Issuing qualified electronic time stamps (qualified trust service), in accordance with the policies: QTSA

Permissible time-stamp request digests include those generated through SHA-256, SHA-384, and SHA-512 algorithms. The corresponding signature methods allowed are sha256WithRSAEncryption, requiring a minimum 3072-bit key, or sha256WithECDSA with a p-256 key.

1.4 POLICY AND PRACTICE STATEMENT

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

- QuoVadis Timestamp Policy/Practice Statement v2.13 dated 9 October 2023

1.5 AUDIT STANDARDS

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 319 412-3 V1.3.1 (2023-09) ETSI EN 319 412-5 V2.4.1 (2023-09) ETSI EN 319 421 V1.2.1 (2023-05) ETSI EN 319 422 V1.1.1 (2016-03) ETSI TS 119 312 V1.4.2 (2022-02)

HIERARCHICAL STRUCTURE OF CERTIFYING AUTHORITIES FOR THE SERVICES

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

1.6 ICA

1.6.1 ROOT QUOVADIS ROOT CA 1 G3

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = QuoVadis Root CA 1 G3, O = QuoVadis Limited, C = BM	8A866FD1B276B57E578E921C65828A2BED58E9F2F288054134B7F1F4BFC9CC74	Any policy (not in scope)

1.6.1.1 INTERMEDIATE CA (ECC)

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = DigiCert QuoVadis G3 TS Europe ECC P256 SHA256 2023 CA1, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	CE49790DCEB21562949C5270BB02C0F34C7B3861D85F98D1069E20453C426BC5	1.3.6.1.4.1.8024.0.2000.6

Time Stamp Unit (TSU) Certificates (ECC)

Distinguished Name	SHA-256 fingerprint	Issuer
CN = tsaeuecc1.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	4F5E4A5CB90714C9C2FD003D15E6559032D839255536A5FBFBE8A40CDFCE459A	DigiCert QuoVadis G3 TS Europe ECC P256 SHA256 2023 CA1
CN = tsaeuecc2.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	B377E92AEFEA0680E7DB074EC83EADF842663DDB866E653FC5EC9DC23972DF08	DigiCert QuoVadis G3 TS Europe ECC P256 SHA256 2023 CA1
CN = tsaeuecc3.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	2C11031A0ABD08FB4D755DFC2E5FC94EFC3AC5D981893946F9116C61A9495125	DigiCert QuoVadis G3 TS Europe ECC P256 SHA256 2023 CA1

1.6.1.2 INTERMEDIATE CA (RSA)

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = DigiCert QuoVadis G3 TS Europe RSA4096 SHA256 2023 CA1, 2.5.4.97 = NTRNL-30237459, O = QuoVadis Trustlink B.V., C = NL	8CD1E1AFA9F976519AA252A0C4568B22092A5773D7E2B4631D19DE2B39ABFA3B	1.3.6.1.4.1.8024.0.2000.6

Time Stamp Unit (TSU) Certificates (RSA)

Distinguished Name	SHA-256 fingerprint	Issuer
CN = tsaeursa1.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	5EA9856907868C43C32DF58791416E738528AC49F00E1C8B3D4BFA62148612FB	DigiCert QuoVadis G3 TS Europe RSA4096 SHA256 2023 CA1
CN = tsaeursa2.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	84029D662EF5F6750DE73D5782C9D3DF6300A7D656C223C2ACBD938F76FC4915	DigiCert QuoVadis G3 TS Europe RSA4096 SHA256 2023 CA1
CN = tsaeursa3.digicert.eu O = QuoVadis Trustlink B.V. 2.5.4.97 = NTRNL-30237459 C = NL	9D2B152525B9137AE15A4EB180374478D17603DA2B24009150EFD7FA751DA6E8	DigiCert QuoVadis G3 TS Europe RSA4096 SHA256 2023 CA1

AUDIT SUMMARY

1.7 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

1.8 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.

1.9 FINDINGS

Findings with regard to ETSI EN 319 401:

No nonconformity found.

Findings with regard to ETSI EN 319 421:

No nonconformity found.

1.10 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.