Certificate No.: PCEB 26/03/01-1

taylorcox.com
ensure your certification

Certificate

Certification body TAYLLORCOX PCEB
established by TAYLLORCOX s.r.o. auditing, inspection and testing institute hereby awards this certificate to the company

DigiCert Europe Netherlands B.V.

Identification No.: 30237459
Nevelgaarde 56 Noord
3436 ZZ Nieuwegein, Netherlands

DigiCert Europe Belgium B.V.

Identification No.: BE0537698318
Schaliënhoevedreef 20T
Mechelen
2800 Belgium

to confirm that its trust services for services specified (see page with detailed scope) is in accordance with:
Regulation (EU) No 910/2014 of the European Parliament and of the Council, revised by Regulation (EU) 2024/1183, ETSI EN 319 411-1 V1.5.1 (2025-04) - Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

This certificate is issued based on a conformity assessment conducted in accordance with ČSN ETSI EN 319 403-1 v2.3.1 and DKP Version 4 under the eIDAS CZ Certification Scheme administered by the Digital and Information Agency (dia.gov.cz), meeting the requirements of Commission Implementing Regulation (EU) 2025/2162.

Date of the certification: 2026-01-01
This certification is valid until: 2026-12-31

Ing. Radek Nedvěd
Head of Certification Body

Place and date of issue of the certificate: Prague, 2026-03-31

The certificate was issued by TAYLLORCOX s.r.o., TAYLLORCOX PCEB
Křižíkova 2136/2a, Karlín, Praha 8, CZ 186 00, audit@tayllorcox.com, www.tayllorcox.com
To check this certificate validity please call the phone number: +420 222 553 101 or on the website pceb.tayllorcox.cz
Member of: TAYLLORCOX UK Ltd., 75 King William St., EC4N, London, United Kingdom, audit@tayllorcox.com

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.digicert.com/

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.digicert.com/

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 26/03/01 dated 31.3.2026.

The conformity assessment report identifier is PCEB-N 26/03/01, version 1.1, issued on 16 April 2026. The audit statement is unqualified.

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;

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

These TSP component services are for public key certificates (non-qualified trust service) in accordance with policies NCP, NCP+, OVCP and PTC.

1.4 POLICY AND PRACTICE STATEMENT

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

- digicert-europe-cp-cps-v6-08.pdf (DigiCert Europe CP/CPS)
- digicert-europe-pki-disclosure-statement-v2-02-en.pdf (DigiCert Europe / DigiCert PKI Disclosure Statement)
- qv-pkio-disclosure-statement-v2-1-en.pdf (DigiCert + DigiCert PKI Disclosure Statement for PKIoverheid)
- digicert-pkioverheid-cps-v2-02-en.pdf (DigiCert Certification Practice Statement for PKIoverheid Certificates)

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, revised by Regulation (EU) 2024/1183 (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 used as audit criteria for this certificate: ETSI EN 319 401 V3.1.1 (2024-06) ETSI EN 319 411-1 V1.5.1 (2025-04) ETSI EN 319 411-2 V2.6.1 (2025-06) 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 V1.7.1 (2024-07) ETSI TS 119 461 V2.1.1 (2025-02) 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 2.1.16 (2025-08-25) CA/Browser Forum – Guidelines for the Issuance and Management of Extended Validation Certificates v2.0.1 (2024-05) CA/Browser Forum - Network and Certificate System Security Requirements v1.7 (2021-04-05) / v2.0.5 (2025-11-12) PKIoverheid - Programma van Eisen v4.12 / v5.0 (https://www.logius.nl/english/pkioverheid)

HIERARCHICAL STRUCTURE OF CERTIFYING AUTHORITIES FOR THE SERVICES

1.6 COMPONENT SERVICES

1.6.1 DIGICERT QUOVADIS PKIOVERHEID ORGANISATIE PERSOON CA - 2023

Issuing CA	SHA-256 fingerprint	
DigiCert QuoVadis PKIoverheid Organisatie Persoon CA - 2023	C8C77ECF368D73214D50D88384464339E6F8E59F34B47E39E7965F4E5787CF1D	
Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Personal Organisation Authenticity	NCP+	2.16.528.1.1003.1.2.5.1
PKIOverheid Personal Organisation Encryption	NCP+	2.16.528.1.1003.1.2.5.3

1.6.2 DIGICERT QUOVADIS PKIOVERHEID ORGANISATIE SERVICES CA - 2023

Issuing CA	SHA-256 fingerprint	
DigiCert QuoVadis PKIoverheid Organisatie Services CA - 2023	6E25C0044C7EBB30D01A4CC3D5733D734D06CD296A6823E63527F4182D528351	
Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Organisation Service Authenticity	NCP+	2.16.528.1.1003.1.2.5.4
PKIOverheid Organisation Service Encryption	NCP+	2.16.528.1.1003.1.2.5.5

1.6.3 DIGICERT QUOVADIS PKIOVERHEID BURGER CA - 2023

Issuing CA	SHA-256 fingerprint	
DigiCert QuoVadis PKIoverheid Burger CA - 2023	66388EE649CBE920FD949FA9B77E2AA45B5DEC4120B8FFAB371B0C9C5E38C1C1	
Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Personal Citizen Authenticity	NCP+	2.16.528.1.1003.1.2.3.1
PKIOverheid Personal Citizen Encryption	NCP+	2.16.528.1.1003.1.2.3.3

1.6.4 DIGICERT QUOVADIS PKIOVERHEID PRIVATE PERSONEN CA - 2023

Issuing CA	SHA-256 fingerprint	
DigiCert QuoVadis PKIoverheid Private Personen CA - 2023	C3FB1A9E37B754E6FE2E313D8D33838E96211087958F70616F49B812FFFF6A8D	
Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Private Personal Authenticity	NCP+	2.16.528.1.1003.1.2.8.1
PKIOverheid Private Personal Encryption	NCP+	2.16.528.1.1003.1.2.8.3

1.6.5 DIGICERT QUOVADIS PKIOVERHEID PRIVATE SERVICES CA - 2023

Issuing CA	SHA-256 fingerprint	
DigiCert QuoVadis PKIoverheid Private Services CA - 2023	B63A82CE98E9FE704DC42B7CB4B63D4BF0646B1D0754F9A4C696A4AFB39436BC	
Certificates	Applicable Policy	Applicable Policy OID
PKIOverheid Private Services - Server	NCP	2.16.528.1.1003.1.2.8.6

1.6.6 DIGICERT - G4 PKIO EUTL G-SIGS NP - 2025

Issuing CA	SHA-256 fingerprint	
DigiCert - G4 PKIo EUTL G-Sigs NP - 2025	D1EDAF0A7F51175C6C1D3B3B8802A6DC0F19D9E6D5E616471D8DC4BB9A052DFE	
Certificates	Applicable Policy	Applicable Policy OID
G4 EUTL Individual Validated eSignature	NCP+	2.16.528.1.1003.1.2.44.14.11.5

1.6.7 DIGICERT - G4 PKIO EUTL G-SIGS LP - 2025

Issuing CA	SHA-256 fingerprint	
DigiCert - G4 PKIo EUTL G-Sigs LP - 2025	A190491567D9869CE0CAC5D39319AA63435BB9DB7AA5563BA2A19FDDB3EB9A25	
Certificates	Applicable Policy	Applicable Policy OID
G4 EUTL Organization Validated eSeal	NCP+	2.16.528.1.1003.1.2.44.14.25.5

1.6.8 DIGICERT - G4 PKIO PRIV G-TLS SYS - 2025

Issuing CA	SHA-256 fingerprint	
DigiCert - G4 PKIo Priv G-TLS SYS - 2025	A3234374CE91C000C929C66DAADE6C85457D61850E6FB388E349FD710A9BB305	
Certificates	Applicable Policy	Applicable Policy OID
G4 Private Organization Validated Server	NCP	2.16.528.1.1003.1.2.44.15.35.11

1.6.9 DIGICERT - G4 PKIO PRIV G-OTHER NP - 2025

Issuing CA	SHA-256 fingerprint	
DigiCert - G4 PKIo Priv G-Other NP - 2025	0A0C91666E2A090D750ED7C25944A760FA8A2A68CFA3A524D209F9C0D1F6061D	
Certificates	Applicable Policy	Applicable Policy OID
G4 Private certificate profiles	NCP, NCP+	See applicable profile OIDs in report PCEB-N 26/03/01

1.6.10 QUOVADIS EU ISSUING CERTIFICATION AUTHORITY G4

Issuing CA	SHA-256 fingerprint	
QuoVadis EU Issuing Certification Authority G4	1D24222B5EEC71FE99BE9D700FA5FF72312DB3EB0FCB4A4F3BCC135DA36C1355	
Certificates	Applicable Policy	Applicable Policy OID
QV Advanced	NCP	0.4.0.2042.1.1
QV Advanced +	NCP+	0.4.0.2042.1.2

1.7 COMPONENT SERVICES

The Registration Service was assessed for public key certificates issued as non-qualified trust services under NCP, NCP+, OVCP and PTC.

The assessed methods include RIV2, RIV4 and Web RIV. Within this certificate, Web RIV applies only to non-qualified certificates and seals and to non-qualified PKIoverheid certificates. ITSME qualified certificate issuance is outside this certificate scope.

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 2025 - 31 December 2025

1.9 RESULT OF AUDIT

The result of the full audit is that, based on the objective evidence gathered during the certification audit from 31 October 2025 to 31 December 2025, 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 26/03/01.

1.10 FINDINGS

The audit identified 0 minor nonconformities and 11 observations. The observations do not affect certification status and are intended to support continuous improvement.

Findings with regard to ETSI EN 319 401:

No nonconformity found.

Findings with regard to ETSI EN 319 411-1:

No nonconformity found.

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