ATTESTIC CERTIFICATION IS PLEASED TO AWARD THIS CONFORMITY CERTIFICATE TO:

Digidentity B.V.

Schenkkade 50
2595 AR The Hague
The Netherlands

FOR DELIVERING THE QUALIFIED TRUST SERVICE(S)

Issuance of qualified certificates for electronic signatures
Issuance of qualified certificates for electronic seals

In accordance with all relevant requirements outlined in:

- **Regulation (EU) No. 910/2014 (eIDAS)**
- **ETSI EN 319 411-2 v2.5.1 (2023-10)**

Electronic Signatures and Infrastructures (ESI) -
Policy and security requirements for Trust Service Providers issuing certificates –
Part 2: Requirements for trust service providers issuing EU qualified certificates

Further details on the scope covered by the certification are outlined on the subsequent pages.

Our certification was based on the accredited certification scheme "Scheme for Trust Services and Trust Service Provider Conformity Assessment based on Regulation 910/2014 (eIDAS)", version 1.1 as of 6 June 2025.
The evaluation documentation for this conformity certificate is registered under our reference 2500701.

On behalf of Attestic Certification:

Certification granted: 2025-10-02

Attestic B.V. has issued this conformity certificate to Digidentity B.V. ('Digidentity') based on a full certification audit performed on all areas and processes.

The audit covered the audit criteria listed below (see "Audit Information"). Digidentity has determined the requirements which were applicable for this audit in its Overview of Applicability. Digidentity has asserted compliance to all applicable requirements in its Statement of Applicability, dated 19 November 2024. This assertion was independently reviewed by Attestic Certification.

AUDIT CONCLUSION

The result of the certification audit is that based on the objective evidence collected for the period from 1 November 2023 through 31 October 2024, the areas assessed were generally found to be effective.

We confirm that the following identification method(s) provide equivalent assurance in terms of reliability to physical presence, pursuant to Regulation (EU) 910/2014 (eIDAS) article 24, paragraph 1a, sub d, for the trust services (and Identity Proofing Context) covered by this Certificate of Conformity:
Digidentity Remote Identity Proofing Level of Assurance 4 – EU Qualified or eIDAS High", supporting the ETSI TS 119461 Use Case for Unattended remote identity proofing (9.2.3): "Hybrid manual and automated operation" (9.2.3.3)", and (where applicable) "Identity proofing of Legal Person" (9.3); and "Identity proofing of Natural Person representing Legal Person" (9.4).

STATEMENT ON THE ISSUANCE OF S/MIME CERTIFICATES:

Issuing CAs in scope of certification are technically capable of issuing S/MIME certificates. On the request of Digidentity, we performed audit procedures to confirm that ETSI TS 119 411-6 V1.1.1 (2023-08) is not applicable. This is because from the CAs in scope of certification:
- We have not observed that S/MIME certificates have been issued in the audit period
- Controls are in place to prevent the issuance of S/MIME certificates

SCOPE: COMPONENT SERVICES

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

Service	Subcontractor	Certificate No.	QR code
Registration Service	-	-	
Certificate Generation Service	-	-	
Dissemination Service	-	-	
Revocation Management Service	-	-	
Certificate Status Service	-	-	
Subject Device Provision Service	-	-	

These TSP component services are being provided for the following qualified trust services as defined in Regulation (EU) 910/2014 (eIDAS):
- Issuance of qualified certificates for electronic signatures (qualified trust service), in accordance with the policy: QCP-n-qscd.
- Issuance of qualified certificates for electronic seals (qualified trust service), in accordance with the policy: QCP-l-qscd.

SCOPE: CERTIFICATE AUTHORITIES

The certificates are issued through the issuing Certification Authorities, as specified below:

Root CA: Staat der Nederlanden Root CA - G3 (not in scope)
Domain CA: Staat der Nederlanden Organisatie Persoon CA - G3 (not in scope)
Issuing CA: Digidentity BV PKIoverheid Organisatie Persoon CA - G3 (OID 2.16.528.1.1003.1.3.5.8.2)
Sha256 Fingerprint:
533FE97EB45FCED24049E41EFE9DB254A5DD9D90DFD53C9512C6207EDB21D82C
- Non-Repudiation (OID 2.16.528.1.1003.1.2.5.2), in accordance with policy: QCP-n-qscd

Domain CA: Staat der Nederlanden Burger CA - G3 (not in scope)
Issuing CA: Digidentity BV PKIoverheid Burger CA – 2021 (OID 2.16.528.1.1003.1.3.3.2.1)
Sha256 Fingerprint:
9C64E24D2CAAA8DD45EF99BA62277CEEE6005C663624514B8C770E2D075BB611
- Non-Repudiation (OID 2.16.528.1.1003.1.2.3.2), in accordance with policy: QCP-n-qscd

Domain CA: Staat der Nederlanden Organisatie Services CA - G3 (not in scope)
Issuing CA: Digidentity BV PKIoverheid Organisatie Services CA - 2021 (OID 2.16.528.1.1003.1.3.5.8.3)
Sha256 Fingerprint:
827A6B205D2E73FF379286DD0B2DED5AEC7239EFE6BC8CACB03ABCCD84B95750
- Non-Repudiation (OID 2.16.528.1.1003.1.2.5.7) in accordance with policy: QCP-l-qscd

Root CA: Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024 (not in scope)
Intermediate CA: Staat der Nederlanden - G4 Intm EUTL G-Sigs NP - 2024 (not in scope)
Issuing CA: Digidentity - G4 PKIo EUTL G-Sigs NP - 2024
Sha256 Fingerprint:
28DB5E6187462835A50960FC56F3C0FE163A0759036047DD6588E71D3DEA1302
- Personal non-repudiation (QCP-n-qscd) - 2.16.528.1.1003.1.2.44.14.11.5
- Professional non-repudiation (QCP-n-qscd) - OID 2.16.528.1.1003.1.2.44.14.12.5

Intermediate CA: Staat der Nederlanden - G4 Intm EUTL G-Sigs LP - 2024 (not in scope)
Issuing CA: Digidentity - G4 PKIo EUTL G-Sigs LP - 2024
Sha256 Fingerprint:
6D705D05D2DD8010A974716D8B190CA591CA2781DFFFA61936A59EC617649463
- Non-Repudiation (QCP-l-qscd) - OID 2.16.528.1.1003.1.2.5.2

Root CA: Digidentity SSCD Root CA
Sha256 Fingerprint:
C20451BD93D8FD6D0C43CD5CE832877FD5614055875126D170910E1209C9B77D
Issuing CA: Digidentity Personal Qualified CA
Sha256 Fingerprint:
03E1AAEF72329B4DA1FCF0BA75FCB7B2F2F34B25AADE701AAAEACC0F65A3B4C4
- Non-Repudiation (OID 1.3.6.1.4.1.34471.3.1.3), in accordance with policy QCP-n-qscd

Issuing CA: Digidentity Business Qualified CA
Sha256 Fingerprint:
21E5D8CFBC2430AA45AD86D38394AE97B359C0E88835E4DE5E0AD1CE92A8201D
- Non-Repudiation (OID 1.3.6.1.4.1.34471.3.2.3), in accordance with policy QCP-l-qscd

DOCUMENTED PRACTICES

The Certification Authority processes and services are documented in the following documents:
- Certificate Practice Statement – PKIoverheid certificates, 2024v3, 21 November 2024, valid from: 28 November 2024
- PKI Disclosure Statement – PKIoverheid certificates, 2024v3, 21 November 2024, valid from: 28 November 2024

- Certificate Policy & Certificate Practice Statement Digidentity Certificates, 2024v3, 21 November 2024, valid from: 28 November 2024
- PKI Disclosure Statement – Digidentity Certificates, 2024v3, 21 November 2024, valid from: 28 November 2024

AUDIT INFORMATION

Audit criteria

- Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Chapter III – Trust Services
- ETSI EN 319 401 v3.1.1 (2024-06) General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 v1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements, for the policies: NCP, NCP+
- ETSI EN 319 411-2 v2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates; - Part 2: Requirements for trust service providers issuing EU qualified certificates, for the policies: QCP-n-qscd and QCP-l-qscd

Subordinate to EN 319411-2:

- ETSI TR 119 461 v1.1.1 (2021-07): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- CA/Browser Forum – Network and Certificate System Security Requirements v2.0 (5 June 2024)
- PKIoverheid Programme of Requirements, version 5.0, 1 June 2024, parts: G3 Legacy Organization Person certificates (previously 3a), G3 Legacy Organization Services certificates (previously 3b), G3 Legacy Citizen certificates (previously 3c)

Audit Period of Time
1 November 2023 through 31 October 2024

Audit performed
October and November 2024

Attestic B.V.
Zeestraat 70, 2518 AC The Hague | P.O. Box 9185, 3301 AD Dordrecht, The Netherlands
info@attestic.eu | www.attestic.eu

Raad voor Accreditatie (Dutch Accreditation Council), registration nr. C710