ATTESTIC CERTIFICATION IS PLEASED TO AWARD THIS CONFORMITY CERTIFICATE TO:

CIBG

Uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport

Rijnstraat 50
2515 XP Den Haag
The Netherlands

FOR DELIVERING THE TRUST SERVICE(S)

Issuance of certificates for electronic signatures

In accordance with all relevant requirements outlined in:

ETSI EN 319 411-1 v1.5.1 (2025-04)
Electronic Signatures and Trust Infrastructures (ESI);
Policy and security requirements for Trust Service Providers issuing certificates;
Part 1: General requirements

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 2600802.

On behalf of Attestic Certification:

Certification granted: 2026-02-02

Certificate ID	CT-029
Valid from	2025-11-22
Expiry date	2027-11-21
First issued	2014-12-18, Before 2026-02-02 certification was awarded by another CAB

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

The audit covered the audit criteria listed below (see "Audit Information"). CIBG has determined the requirements which were applicable for this audit in its Overview of Applicability, dated September 2025. CIBG has asserted compliance to all applicable requirements in its Statement of Applicability, dated 15 September 2025.
This assertion was independently reviewed by Attestic Certification.

AUDIT CONCLUSION

The result of the certification audit is that, based on the objective evidence collected during the certification audit for the period from 1 September 2024 through 31 August 2025, the areas assessed were generally found to be effective.

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 CIBG, 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, performed completely/partly by subcontractors under the responsibility of CIBG:

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

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

- Issuance of certificates for electronic signatures, in accordance with the policies: NCP, NCP+

SCOPE: CERTIFICATE AUTHORITIES

The end-entity certificates are issued through its issuing certification authorities, as specified below:

Root CA: Staat der Nederlanden Private Root CA - G1 (not in scope)
Domain CA: Staat der Nederlanden Private Services CA - G1 (not in scope)
Issuing CA: UZI-register Private Server CA G1
Sha256 Fingerprint:
`BDD860EF8E87E2B2C7EBB34DD6E9E1771A3A3C5DEC850BA7080E3E2904DBD897`

- Services - Server (2.16.528.1.1003.1.2.8.6), in accordance with policy: NCP

Issuing CA: Issuing CA: ZOVAR Private Server CA G1

Sha256 Fingerprint:
FE54263BC96C2DFBAC5BE5F449CFF7F5B12B6255A7BBCF761BA979E5986E1598

- Services - Server (2.16.528.1.1003.1.2.8.6), in accordance with policy: NCP

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: Issuing CA: UZI-register Zorgverlener CA G3
Sha256 Fingerprint (2017):
3EAD4F72F06F1054881D2728DE033A8E13FADE6BD165084018EB943C17378DAA
Sha256 Fingerprint (2019):
507DB60D263D3D09D283DE2E3AA435DFD8775E52BC335702E3832BBB57EC1CBD

- Authentication (2.16.528.1.1003.1.2.5.1), in accordance with policy: NCP+
- Confidentiality (2.16.528.1.1003.1.2.5.3), in accordance with policy: NCP+

Issuing CA: UZI-register Medewerker op naam CA G3
Sha256 Fingerprint (2017):
D8553A2880E96B7AA4C7413DD903AFD3D580504695DD26A168FD48CCE7B1474A
Sha256 Fingerprint (2019):
D28DB435E31212A3BDCCF87620F6544B99A9C02328BF983E882FD0627A1D130F

- Authentication (2.16.528.1.1003.1.2.5.1), in accordance with policy: NCP+
- Confidentiality (2.16.528.1.1003.1.2.5.3), in accordance with policy: NCP+

Domein CA: Staat der Nederlanden Organisatie Services CA - G3 (not in scope)
Issuing CA: UZI-register Medewerker niet op naam CA G3
Sha256 Fingerprint (2017):
38DED3FF6827579008AF4887EB9698A3CFA927FA8ED59F06BA090FB9A63E2D77
Sha256 Fingerprint (2019):
972957304031234ED17679FDCB97556D6173D5F2BF0E6E66D612680CA6E77685

- Authentication (2.16.528.1.1003.1.2.5.4), in accordance with policy: NCP+
- Confidentiality (2.16.528.1.1003.1.2.5.5), in accordance with policy: NCP+

DOCUMENTED PRACTICES

The Certification Authority processes and services are documented in the following documents:

- Certification Practice Statement (CPS) UZI-register, versie 2.1, 22-04-2025 (OID: 2.16.528.1.1007.1.1)
- Certification Practice Statement (CPS) ZOVAR, versie 2.1, 22-04-2025 (OID: 2.16.528.1.1007.5.1.1)

AUDIT INFORMATION

Audit criteria

- Regulation (EU) 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) Electronic Signatures and Trust Infrastructures (ESI) - General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 v1.5.1 (2025-04) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, for the policies: NCP, NCP+

Subordinate to ETSI EN 319411-1:

- CA/Browser Forum – Network and Certificate System Security Requirements v2.0.5 (9 July 2025)
- PKIoverheid Programme of Requirements, version 5.2, 8 July 2025, parts:
  - G3 Legacy Organization Person certificates (previously PoR part 3a)
  - G3 Legacy Organization Services certificates (previously PoR part 3b)
  - Private Server certificates (previously PoR part 3h)

Audit Period of Time
1 September 2024 through 31 August 2025

Audit performed
September 2025

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