Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Management Assertion Logius 2017

Date   13 December 2019

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from 1 January 2017 through 31 December 2017

13 December 2019

The Dutch Governmental Shared Service Organisation for ICT "Logius" provides its SSL Certification Authority (CA) services through the central infrastructure of the Dutch Government. For the issuance of SSL – CA services, the central infrastructure of the Dutch Government consists:

Certificate Authority	SHA2-fingerprint
Root Certification Authority – G2 ("Staat der Nederlanden Root CA – G2")	66:8C:83:94:7D:A6:3B:72:4B:EC:E1:74: 3C:31:A0:E6:AE:D0:DB:8E:C5:B3:1B: E3:77:BB:78:4F:91:B6:71:6F
Subordinate Domain-CA for Organisations – G2 ("Staat der Nederlanden Organisatie CA – G2")	85:A8:F5:86:6D:D7:8D:F1:73:B0:66:73: 17:C5:9B:2D:62:42:DE:59:EB:01:BB:2F: 2E:8B:9D:B7:14:B4:CA:27
Root Certification Authority – G3 ("Staat der Nederlanden Root CA – G3")	3C:4F:B0:B9:5A:B8:B3:00:32:F4:32:B8: 6F:53:5F:E1:72:C1:85:D0:FD:39:86:58: 37:CF:36:18:7F:A6:F4:28
Subordinate Domain-CA for Organisations-Services – G3 ("Staat der Nederlanden Organisatie Services CA – G3")	D9:58:1D:BD:E9:9B:39:EE:FF:6C:E5:C8: 0D:E1:65:0D:A0:C1:C8:A1:09:70:5E:D2: 86:C5:3B:C9:5E:66:55:E4
Root Certificate Authority – EV ("Staat der Nederlanden EV Root CA")	4D:24:91:41:4C:FE:95:67:46:EC:4C:EF: A6:CF:6F:72:E2:8A:13:29:43:2F:9D:8A: 90:7A:C4:CB:5D:AD:C1:5A
Subordinate Intermediate-CA for EV certificates ("Staat der Nederlanden EV Intermediair CA")	DC:86:2A:3F:02:5E:F7:F2:52:FA:94:13: CB:60:DE:25:E5:7E:6A:A7:E1:FB:1D:CA: 7B:59:D2:C2:21:71:06:EA
Subordinate Domain-CA for Organisations-Persons – G3 ("Staat der Nederlanden Organisatie Persoon CA – G3")	82:22:BC:4F:E7:A3:DD:CA:9E:F0:BF: 0D:68:2A:C8:88:79:9F:87:82:2D:15:33: 2A:54:C0:BF:DF:C6:85:4F:7B
Subordinate Domain-CA for Government-Citizen – G3 ("Staat der Nederlanden Burger CA – G3")	2E:7A:0A:3B:0C:52:7E:B2:0C:52:25:3C: 8D:22:78:CA:10:81:36:A8:CA:3A:4E:A2: 2D:A7:B5:9B:AC:90:65:0A
Subordinate Domain-CA for Autonomous Devices – G3 ("Staat der Nederlanden Autonome Apparaten CA – G3")	AD:49:3D:6E:85:EC:60:8A:B8:13:A8:87: BD:C4:D4:19:6A:0B:C9:B3:3D:25:65:A7: FA:8A:C4:30:F0:8A:99:A5
Subordinate Domain-CA for Government-Citizen – G2 ("Staat der Nederlanden Burger CA – G2")	2F:2F:0C:84:4F:B3:36:A9:42:1A:B6:FA: 36:DC:DA:C3:BB:84:E0:38:4C:FF:5D: AD:51:11:3C:8C:A4:24:E6:A4
Subordinate Domain-CA for Autonomous Devices – G2 ("Staat der Nederlanden Autonome Apparaten CA – G2")	1B:17:10:02:64:24:7D:70:90:03:61:16: 23:8C:93:F4:58:53:ED:E5:AE:A6:F9:F1: A4:52:4F:69:78:DD:89:54

The management of Logius has assessed the disclosure of its certificate practices and its controls over its SSL CA services. Based on that assessment, in Management's opinion, in providing its SSL CA services in the Netherlands, during the period from 1 January 2017 through 31 December 2017, Logius has:

- Disclosed its Certificate practices and procedures in its Certification Practice Statement, version 4.1, dated December 2017, including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines and

- Maintained effective controls to provide reasonable assurance that:

    - subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;

    - the integrity of keys and certificates it manages was established and protected throughout their life cycles;

    - logical and physical access to CA systems and data was restricted to authorized individuals;

    - the continuity of key and certificate management operations was maintained; and

    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.2, including the following:

CA BUSINESS PRACTICES DISCLOSURE

CA SERVICE INTEGRITY
      Key Generation Ceremony
      Certificate Content And Profile
      Certificate Request Requirements
      Verification Practices
      Certificate Revocation And Status Checking
      Employee And Third Parties
      Data Records
      Audit

CA ENVIRONMENTAL SECURITY

Within the G2 hierarchy Logius does not operate an OCSP responder to serve status information on the subordinate CAs. The rationale for this decision is that the inception of this environment predates the effective date of the Baseline Requirements by four years. Logius has incorporated OCSP functionality in the G3 CA, which is the successor of the G2 Root. In both environments status information is made available by means of Certificate Revocation Lists.

<u>This management assertion has been re-issued because of an omission in earlier management assertions regarding the scope of the WTBR audit. Some of our intermediate CAs were omitted in the management assertion by accident although they have been audited against the relevant WTBR criteria and principles.</u>

For approval:

Y.L (Yvonne) van der Brugge-Wolring EM
The general director Logius