Standard Audit Attestation for

Federal Office of Information Technology, Sytems and Telecommunication (FOITT), Campus Meielen, Eichenweg 3, 3003 Bern, Switzerland

Reference: 284/2026

Zurich, 2026-01-27

To whom it may concern,

This is to confirm that KPMG AG has audited the CAs of the Federal Office of Information Technology, Systems and Telecommunication (FOITT) without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “284/2026” covers multiple Root-CAs and consists of 8 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

KPMG AG
Certification Body SCESm 0071
Badenerstrasse 172
8004 Zurich, Switzerland
Internet: www.kpmg.ch
Phone: +41 58 249 30 48

With best regards,

Reto P. Grubenmann
Director, Head of Certification Body

Jonathan Peters
Manager

This attestation is based on the template version 3.4 as of 2025-07-08, that was approved for use by ACAB’c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• KPMG AG, certification body SCESm 0071, Badenerstrasse 172, 8004 Zurich, Switzerland, registered under CHE-106.084.881 • Accredited by Swiss Accreditation Service SAS under registration SCESm 0071 for the certification of trust services according to “ISO/IEC 17021-1:2015” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): Allianz Suisse Versicherungs-Gesellschaft AG • Third-party affiliate audit firms involved in the audit: None.
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: • 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, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • 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, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.
- Additional qualification and experience Lead Auditor:
  On top of what is required for team members (see above), the Lead Auditor
  a) has acted as auditor in at least three complete TSP audits;
  b) has adequate knowledge and attributes to manage the audit process; and
  c) has the competence to communicate effectively, both orally and in writing.
- 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:
  Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 2
- 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.

Identification of the CA / Trust Service Provider (TSP):	Federal Office of Information Technology, Sytems and Telecommunication (FOITT), Campus Meielen, Eichenweg 3, 3003 Bern, Switzerland registered under CHE-221.032.573

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:	2024-11-01 to 2025-10-31
Point in time date:	None, as audit was a period of time audit
Audit dates:	2025-06-03 to 2025-10-24 (on site)
Audit location:	Federal Office of Information Technology, Sytems and Telecommunication (FOITT), Campus Meielen, Eichenweg 3, 3003 Bern, Switzerland

Root 1: Swiss Government Root CA I

Standards considered:	European Standards: • ETSI EN 319 401 V2.3.1 (2021-05) • ETSI EN 319 411-1 V1.4.1 (2023-10) • 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) For the Trust Service Provider Conformity Assessment: • ISO/IEC 17021-1:2015 • ETSI EN 319 403 V2.3.1 (2020-06)

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

- Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I, version 3.5.2, as of 2025-06-06

In the following areas, non-conformities have been identified throughout the audit:

Findings regarding ETSI EN 319 401:

6.2 Terms and Conditions

NC #3: Not all information required is documented in the Terms and Conditions. [REQ-6.2-02]

7.2 Human resources

NC #2: The process for the appointment of trusted roles is not formalized and does not contain the explicit requirement, that senior management responsible for security is responsible for the appointment.

7.3 Asset management

NC #4: The asset management documentation has not been finalized and formally approved at the time of the audit, and an information asset register does not yet exist. [REQ-7.3-01, REQ-7.3.1-02]

7.6 Physical and environmental security

NC #5: The racks are in a server room of the FOITT and shared with other departments. The racks are physically locked but not monitored. As an interim measure, the racks are to be connected to the alarm system and electronically secured, but this has not yet been fully implemented. [REQ-7.6-03, REQ-7.6-04, REQ-7.6-05]

7.7 Operation security

NC #1: An Anti-Malware-System is not installed on Linux systems. [REQ-7.7-05]

7.8 Network security

NC #6: The network is provided as a service by FOITT and is not managed by the SG PKI department directly. The SG PKI department maintains and reviews their own list. The comparison between the list of the SG PKI to the export of the implemented rules by FOITT did not take place. [REQ-7.8-06]

7.9 Incident management

NC #7: The monitoring concept has not yet been finalized and formally approved. The monitoring of RHEL systems is not documented. System and application logs are not yet archived. [REQ-7.9-01, REQ-7.9-02, REQ-7.9-04, REQ-7.9-09]

NC #8: It is not formally documented that critical vulnerabilities are addressed within 48 hours. [REQ-7.9-10]

Findings with regard to ETSI EN 319 411-1:

6.2 Physical security controls

NC #13: As part of the Period of Time audit, the auditors found that not all names in certificates were correctly registered. [REG-6.2.2-02A – REG-6.4.5-04]

6.4 Facility, management, and operational controls

NC #5: The network is provided as a service by FOITT and is not managed by the SG PKI department directly. The SG PKI department maintains and reviews their own list. The comparison between the list of the SG PKI to the export of the implemented rules by FOITT did not take place. [OVR-6.4.2-02 – OVR-6.4.2-06]

NC #9: The Log Data Management Concept should be checked and updated if necessary. [OVR-6.4.5-06]

NC #5 No fire extinguishers were found in close proximity to the server racks. [OVR-6.4.7-07]

6.5 Technical security controls

NC #10: There is no description on how cryptographic devices should be stored. [OVR-6.5.2-11]

NC #11: The process for destroying cryptographic keys and devices is only available as a draft version. [OVR-6.5.2-13]

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN=Swiss Government Root CA I, OU=Services, O=The Federal Authorities of the Swiss Confederation, C=CH	SHA-256 fingerprint of the certificate: 6EC6614E9A8EFD47D6318FFDFD0BF65B493A141F77C38D0B319BE1BBBC053DD2	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, NCP+

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = Swiss Government Enhanced CA 01, OU = Certification Authorities, OU = Services, O = Admin, C = CH	SHA-256 fingerprint of the certificate: 7B8ABCDCBCBC696694D9C4993551E53C662A5EA2F12788F68E8F33C356847A66	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, NCP+
Complete subject DN: CN = Swiss Government Enhanced CA 02, OU = Certification Authorities, OU = Services, O = Admin, C = CH	SHA-256 fingerprint of the certificate: D506A0E9916076E6AFC8476DF9387FD07402D57CA4088873C99A41485BAEE944	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, NCP+

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Key pairs without a corresponding certificate (“parked keys”)

During the audit period there were no parked keys identified.

Modifications record

Version	Issuing Date	Changes
Version 1	2026-01-27	Initial attestation

End of the audit attestation letter.