Audit Attestation

Federal Office of Information Technology, Systems and Telecommunication (FOITT) CHE-221.032.573

Identification of the conformity assessment body (CAB):	KPMG AG, certification body SCESm 0071, Badenerstrasse 172, CH-8004 Zurich, Switzerland registered under CHE-106.084.881 Accredited by Schweizerische Akkreditierungsstelle SAS under registration SCESm 0071[2] for the certification of trust services according to "ISO/IEC 17021-1:2015" and "ETSI EN 319 403 V2.2.2 (2015-08)" according to ISO/IEC 17065:2013.
Identification of the trust service provider (TSP):	Federal Office of Information Technology, Systems and Telecommunication (FOITT) Monbijoustrasse 74 CH-3007 Bern Switzerland registered under CHE-221.032.573
Report Issuance	25th January 2022
Identification of the audited Root-CA:	**Swiss Government Root CA IV** **Distinguished Name:** CN=Swiss Government Root CA IV, OU= Swiss Government PKI, O= Bundesamt fuer Informatik und Telekommunikation (BIT), C=CH **SHA 256 Fingerprint:** 5a 0b af 55 88 e7 3f cc 33 6c 90 39 b8 59 81 18 92 96 67 0e fa 99 45 20 ff 00 8b 9a cf 4d 26 02 **Serial Number:** df b3 4d 9a 6a 2c cf 87 56 29 e9 ad af d2 8c 04 **Applied policy:** QCP-n-qscd, QCP-l-qscd, NCP+ of ETSI EN 319 411-1/2

Zurich, 26.01.2021

Reto Grubenmann
Director, Head of Certification Body

Reto Mathys
Senior Manager, Lead Auditor

[1] in the following termed shortly „*CAB*"

[2] https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas.html

This Audit Attestation Federal Office of Information Technology, Systems and Telecommunication (FOITT), CHE-221.032.573 consists of 3 pages.

Audit Attestation Federal Office of Information Technology, Systems and Telecommunication (FOITT), CHE-221.032.573

The certification for the control objectives and control framework was performed under the official accreditation against ISO/IEC 17021-1 and its PKI-framework based on the certification of the Swiss Trusted Service Provider (TSP), named Federal Office of Information Technology, Systems and Telecommunication (FOITT).

The audit was performed as full annual audit at the TSP's location in Berne. It took place from 4th May 2021 until 31st December 2021 and covered the period from 12th December 2020 until 18th November 2021.

The audit was performed according to the Swiss Standards "ZertES SR 943.03 (2016-3)", "VZertES SR 943.032 (2016-11)", "TAV SR 943.032.1 (2016-11)" as well as the European Standards "ETSI EN 319 411-1, V1.2.2 (2018-04)", "ETSI EN 319 411-2, V2.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)" considering the requirements of the "ETSI EN 319 403, V2.2.2 (2015-08)" for the Trust Service Provider Conformity Assessment.

This initial audit was based on the following policy and practice statement documents of the TSP:

1. Swiss Government PKI – Root CA IV: Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV, version 1.31, as of 5th January 2021

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

The audit was completed successfully without critical findings. In case of any question, please contact:

KPMG AG
Certification Body SCESm 0071
Badenerstrasse 172
CH-8045 Zurich
Switzerland
E-Mail: retogrubenmann@kpmg.com
Phone: +41 58 249 42 46

Identification of the Sub-CA	Distinguished Name	SHA-256 Fingerprint	Certificate Serial Number	Applied Policy	Procedure Number
Swiss Government Regulated CA 02	CN=Swiss Government Regulated CA 02 OU=Swiss Government PKI O=Bundesamt fuer Informatik und Telekommunikation (BIT) OID.2.5.4.97=VATCH-CHE-221.032.573 C=CH	8d 49 4a 34 9b 6e d3 6d cc ab cc e2 76 7c 8a 6d 52 7e 29 0d e0 79 7d ff 83 d5 8f 43 c2 d1 91 e9	03 6a 07 98 8f 3b 51 39 de f5 2b e5 a8 ea 75 5e	QCP-n-qscd, QCP-l-qscd, NCP+ of ETSI EN 319 411-1/2	Certificate Number: 184/2022

Table 1: Sub-CA’s issued by the Root-CA