



Deutsche  
Akkreditierungsstelle  
D-ZE-20924-01-00

# Audit Attestation

## *Bundesamt für Informatik und Telekommunikation (BIT)*

### **CHE-221.032.573**

Identification of the conformity assessment body (CAB):	KPMG AG, certification body SCESm 0071, Räfelstrasse 28, CH-8036 Zurich, Switzerland registered under CHE-106.084.881 Accredited by Schweizerische Akkreditierungsstelle SAS under registration SCESm 0071 <sup>2</sup> for the certification of trust services according to "DIN EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)".
Identification of the trust service provider (TSP):	Bundesamt für Informatik und Telekommunikation (BIT) Monbijoustrasse 74 CH-3007 Bern Switzerland  registered under CHE-221.032.573
Report Issuance	22th May 2019
Identification of the audited Root-CA:	<p><b>Swiss Government Root CA IV</b></p> <p><b>Distinguished Name:</b> CN=Swiss Government Root CA IV, OU= Swiss Government PKI, O= Bundesamt fuer Informatik und Telekommunikation (BIT), C=CH</p> <p><b>SHA 256 Fingerprint:</b> 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</p> <p><b>Serial Number:</b> df b3 4d 9a 6a 2c cf 87 56 29 e9 ad af d2 8c 04</p> <p><b>Applied policy:</b> QCP-n-qscd, QCP-l-qscd, NCP+ of ETSI EN 319 411-1/2</p>

Zurich, 22.05.2019

Reto Grubenmann  
Director, Head of Certification Body

Reto Mathys  
Manager, Lead Auditor

<sup>1</sup> in the following termed shortly „CAB“

<sup>2</sup>[https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrestellensuchesa/\\_icr\\_content/par/externalcontent\\_1828266334.external.exturl.pdf/aH/R0cHM6Ly9zYXNkYi5jbGllbnRzLmtpaXAUy2qvbWVkaWEvcG/RmL1NDRVNtLTAwNzEtZGUucGRm.pdf](https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrestellensuchesa/_icr_content/par/externalcontent_1828266334.external.exturl.pdf/aH/R0cHM6Ly9zYXNkYi5jbGllbnRzLmtpaXAUy2qvbWVkaWEvcG/RmL1NDRVNtLTAwNzEtZGUucGRm.pdf)

This Audit Attestation Bundesamt für Informatik und Telekommunikation (BIT), CHE-221.032.573 consists of 3 pages.



Audit Attestation Bundesamt für Informatik und Telekommunikation (BIT), CHE-221.032.573

The audit was performed as point in time audit at the TSP's location in Berne. It took place from 11<sup>th</sup> February 2019 until 20<sup>th</sup> May 2019.

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 (2018-4)", "ETSI EN 319 411-2, V2.2.1 (2018-4)", "ETSI EN 319 401, V2.2.1 (2018-4)", "ETSI EN 319 421, V1.1.1 (2016-03), and "ETSI EN 319 422 V1.1.1 (2016-03)" 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 1.1, as of 10<sup>th</sup> May 2019

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  
Räffelstrasse 28  
CH-8036 Zurich  
Switzerland  
E-Mail: [retogrubenmann@kpmg.com](mailto:retogrubenmann@kpmg.com)  
Phone: +41 58 249 42 46



Audit Attestation Bundesamt für Informatik und Telekommunikation (BIT), CHE-221.032.573

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-I-qscd, NCP+ of ETSI EN 319 411-1/2	Certificate Number: 137/2019

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