KPMG AG
Information Risk Management
Certification Body SCESm 0071
Badenerstrasse 172
CH-8004 Zurich

P.O. Box
CH-8036 Zurich

Telephone +41 58 249 49 32
Fax +41 58 249 48 68
Internet www.kpmg.ch

Bundesamt für Informatik und
Telekommunikation (BIT)
Mr. Michael von Niederhäusern
Head of PKI
Monbijoustrasse 74
3003 Bern

Contact
Reto Grubenmann
+41 58 249 42 46

Zurich, 25 January 2017

To the Certification Authority staff and Management of BIT

Dear Mr. von Niederhäusern

We have performed the procedures enumerated below, which were agreed to by the Managements of Client, solely to conduct BIT’s (Federal Office of Information Technology, Systems and Telecommunication) Compliance Audits. This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants.

KPMG has executed the Compliance Audits in year 2016 against the mandatory standardizations listed in the following section (specified information/procedure/results).

FOITT operates the following three Root Certification Authorities:

- Swiss Government Root CA I
  sha-1: A1 58 51 87 15 65 86 CE F9 C4 54 E2 2A B1 5C 58 74 56 07 B4

- Swiss Government Root CA II
  sha-1: C7 F7 CB E2 02 36 66 F9 86 02 5D 4A 3E 31 3F 29 EB 0C 5B 38

- Swiss Government Root CA III
  sha-1: CC EA E3 24 45 CD 42 18 DD 18 8E AD CE B3 13 3C 7F B3 40 AD

We especially confirm that we have used the following standards and policies:

Standard	Policies
ETSI TS 101 456 V1.4.3 or later - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates	QCP public + SSCD
ETSI TS 102 042 V2.4.1 or later - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates	OVCP, PTC-BR, EVCP, EVCP+, LCP, NCP

The sufficiency of the procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purposes.

Specified Information:	Procedure:	Results:
	KPMG has completed the Certification Audit Process in accordance with the CSP requirements: - ETSI TS 101.456 (qualified environment) - ETSI TS 102.042 V2.4.1 (PKI standard for Europe), CAB/Forum Baseline and CAB/Forum EV Guideline with ETSI EN 319.403 and referenced PKI standards for the PKI Trust Center of BIT.	KPMG herewith confirms that the CSP audit certification process: - ETSI TS 101.456 and - ETSI TS 102.042 with EV requirements) also covers all aspects of a Web Trust certification and is therefore fit to be included in web browser root certificate stores.
Legal Name: **Bundesamt für Informatik and Telekommunikation (BIT)**	BIT is a Government entity and not listed in the Commercial Register	Government Entity
Monbijoustrasse 74 **3003 Bern**	KPMG has performed several site visits at **BIT's** head office.	The site visit has shown that **BIT** operates at the indicated address.
Business Phone Number: **+41 58 465 90 11**	We have called the indicated central phone number and additionally phone numbers of individual **BIT** employees.	Phoned Business Number and noted that it was answered with the Doing Business As name. A receptionist has answered the phone.
Bank Account – "Bank Name", "Account Number"	This is not applicable in Switzerland.	N/A
The corporate officers are "NAMED" (verified officer)	We personally know and have spoken to in person to several corporate officers.	The corporate officers who KPMG knows are: **Mr. Michael von Niederhäusern** **Mr. Jürgen Weber** **many others**
Name of application signer and approver	Obtain letter from verified Officer, confirming the names of the application signer and approver.	**Mr. Michael von Niederhäusern** serves as Head of PKI infrastructure. KPMG knows Michael von Niederhäusern in person.

We were engaged to conduct the annual examinations, with the objective of which would be the expression of an opinion on the compliance to the standards mentioned above.
The Compliance Audit evaluated the Certificate Authority and Directory Server components associated with these three CAs mentioned above.

Accordingly, we do express our positive opinion and provide you confirmation that the requirements were fulfilled during the annual certification audits based on the control objectives and standards. If we would perform additional procedures with deviations in the audit result, we shall inform you about these matters and give close attention to you.

We have prepared this confirmation report with reference to the various PKI standarizations and international norms concerning the infrastructure and processes described above to the best of our knowledge based upon review procedures, walk through, technical console testings, the documentation made available to us and the explanations received. We trust this confirmation report as a management summary, which accurately reflects the situation at BIT in the year 2016.

This confirmation report is intended solely for the information and use of the Certification Authority (CA) and managements of client, and is not intended to be and should not be used by anyone other than these specified parties.

Please do not hesitate to contact Mr. Reto Grubenmann (+41 58 249 42 46), leader of the KPMG's certification body SCESm 0071 of KPMG AG in Zurich (Switzerland), should you have any queries.

Yours sincerely

KPMG AG

U. Würgler

Reto Grubenmann
Director

Urs Würgler
Manager

Copy to:
Certification Body SCESm 0071, KPMG AG in Switzerland