Print this page

Mozilla - CA Program

Case Information

Case Number	00000042	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Swiss BIT, Swiss Federal Office of Information Technology, Systems and Telecommunication (FOITT)	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include Swiss Government roots	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=435026

General information about CA's associated organization

CA Email Alias 1	pki-info@bit.admin.ch		
CA Email Alias 2			
Company Website	http://www.bit.admin.ch /index.html?lang=en	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Need Response From CA
Geographic Focus	Switzerland	**Verified?**	Verified
Primary Market / Customer Base	Swiss Bundesamt für Informatik und Telekommunikation (BIT) is also known as the Swiss Federal Office of Information Technology, Systems and Telecommunication (FOITT) which operates servers and software applications for the Confederation and third parties.	**Verified?**	Verified
Impact to Mozilla Users	Overall the FOITT serves 1200 locations in Switzerland and 200 locations worldwide. The FOITT is also responsible for networking the Swiss cantons and the Principality of Liechtenstein.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes 3) Audit Criteria: ??? 4) Document Handling of IDNs in CP/CPS: ??? 5) Revocation of Compromised Certificates: CPS section 4.9.1 6) Verifying Domain Name Ownership: CPS section 3.2.2.4 7) Verifying Email Address Control: ??? 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: ??? 10) Domain owned by a Natural Person: ??? 11) OCSP: Yes 12) Network Security Controls: ???	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: ??? 2) Wildcard DV SSL certificates: CPS section 3.2.2.6: SG PKi Root III and its subordinate CAs do not issue Wildcard DV certs 3) Email Address Prefixes for DV Certs: ??? 4) Delegation of Domain / Email validation to third parties: ??? 5) Issuing end entity certificates directly from roots: No. CPS section 1.3. 6) Allowing external entities to operate subordinate CAs: No. CPS section 1.3. 7) Distributing generated private keys in PKCS#12 files: ??? 8) Certificates referencing hostnames or private IP addresses: CPS section 3.2.2.5: SG PKI Root III and its subCAs do not issue certs for IP addresses. 9) Issuing SSL Certificates for Internal Domains: ??? 10) OCSP Responses signed by a certificate under a different root: No 11) SHA-1 Certificates: ??? 12) Generic names for CAs: No 13) Lack of Communication With End Users: ??? 14) Backdating the notBefore date: ???	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Swiss Government Root CA III	**Root Case No**	R00000115
Request Status	Need Information from CA	**Case Number**	00000042

Additional Root Case Information

Subject	Include Swiss Government Root CA III

Technical Information about Root Certificate

O From Issuer Field	Swiss Government PKI	**Verified?**	Verified
OU From Issuer Field	www.pki.admin.ch	**Verified?**	Verified
Certificate Summary	Include Swiss Government Root CA III (SG Root CA III) hierarchy supports certificates of high, medium, and low assurance level for Publicly-Trusted Authentication and Code Signing Certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8752168	**Verified?**	Verified
Valid From	2016 Apr 15	**Verified?**	Verified
Valid To	2041 Apr 15	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www.valid-dv.pki.admin.ch/ https://www.valid-ov.pki.admin.ch/ https://www.valid-ev.pki.admin.ch/	**Verified?**	Verified
CRL URL(s)	http://www.pki.admin.ch/crl/RootCAIII.crl http://www.pki.admin.ch /crl/PTSTCA02.crl http://www.pki.admin.ch /crl/PTEVCA02.crl CPS section 4.9.7.1: The value of the nextUpdate field is never more than ten days beyond the value of the thisUpdate field.	**Verified?**	Verified
OCSP URL(s)	http://www.pki.admin.ch/aia/ocsp CPS section 4.9.9: certificate status database, used by the OCSP service, is updated every 4 hours during office hours.	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.756.1.17.3.62.4	**Verified?**	Verified
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central /source/security/nss/lib/certdb /genname.c#1551	**Verified?**	Need Response From CA

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/	**Verified?**	Need Response From CA

	make sure there aren't any errors.		
CA/Browser Forum Lint Test	OK. Certificate not found.	**Verified?**	Verified
Test Website Lint Test	NEED: test https://www.valid-ev.pki.admin.ch/ in http://cert-checker.allizom.org/ ERRORS: Failure ASN.1 Error in X520countryName ASN.1 Error in X520SerialNumber	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	CC:EA:E3:24:45:CD:42:18:DD:18:8E:AD:CE:B3:13:3C:7F:B3:40:AD	**Verified?**	Verified
SHA-256 Fingerprint	95:8A:BB:AE:FF:76:0F:4F:BF:66:FF:0F:2C:27:08:F4:73:9B:2C:68:61:27:23:9A:2C:4E:C8:7A:68:A9:84:C8	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CPS section 1.3.1: SG Root CA III signs subordinated CAs that are operated exclusively by Swiss Government PKI staff appointed to the task. CPS section 1.3.1.2: SG Root CA III currently has the following internally-operated subordinate CAs: - Swiss Government Public Trust Standard CA 02 - Swiss Government Public Trust EV CA 02 - Swiss Government Public Trust Codesign CA 02 - Swiss Government Public Trust EV Codesign CA 02	**Verified?**	Verified
Externally Operated SubCAs	CPS section 1.3.1: There are no externally-operated subCAs chaining up to this root cert.	**Verified?**	Verified
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	CPS section 1.3.2 External Registration Agents are allowed. CPS section 1.3.2.3: SG PKI requires RA by contract to ... - fully comply with SG PKI Root III	**Verified?**	Verified

	CP/CPS - Agree to accept regular audits to validate compliance with SG PKI Root III CP/CPS - Supply appropriate information for the requested Fully-Qualified Domain Name(s) as specified in Section 3.2.2.4 (Domain Authorization Letter) SG PKI is keeping record of all contracts and annually verifies the Registration Agents audit and domain authorization status.

Verification Policies and Practices

Policy Documentation	The CP/CPS is provided in English	**Verified?**	Verified
CA Document Repository	https://www.bit.admin.ch/adminpki/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.bit.admin.ch/adminpki/00243/06257/index.html	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.pki.admin.ch /cps/CPS_2_16_756_1_17_3_61_0.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org /CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED only if requesting EV treatment	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	CPS section 3.2.2.4: For each Fully-Qualified Domain Name listed in a Certificate, SG PKI confirms that, as of the date the Certificate was issued, the Applicant ... either is the Domain Name Registrant or has control over the FQDN by: - communicating direction with the Domain Name Registrant	**Verified?**	Verified

	using the contact information listed in the WHOIS records "registrant', "technical", or "administrative" field. - Relying upon a Domain Authorization Document approved by the Domain Name Registrant. The document must be dated on or after the certificate request date or used by SG PKI to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate issuance.		
EV SSL Verification Procedures	CPS section 4.1.2.3: Prior to the issuance of a EV Server Certificate, SG PKI obtains and approves the following documentation from the Applicant: - a signed Organization Authorization Letter for the requested Organization entry. - a valid Domain Authorization Letter for the requested FQDN - a signed Terms & Conditions Agreement - a certificate request in the form of a PKCS#10	**Verified?**	Verified
Organization Verification Procedures	CPS section 4.2.1 - verifying org existence and identity, and authority of cert requester	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.bit.admin.ch/adminpki/	**Verified?**	Verified