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**	Ready for Public Discussion

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?**	Not Applicable
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

Required and 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	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes 3) Audit Criteria: KPMG, see http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx 4) Document Handling of IDNs in CP/CPS: in CP/CPS section 3.2.2 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: Not applicable 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: Compliant: DNS Names go in SAN 10) Domain owned by a Natural Person: No DV certificates are issued, see CP/CPS, Chapter 1.4.1. 11) OCSP: Yes 12) Network Security Controls: in CP/CPS section 6.7	**Verified?**	Verified

Forbidden and 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	1) Long-lived DV certificates: No DV certificates are issued, see CP/CPS, Chapter 1.4.1. 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: No DV certificates are issued, see CP/CPS, Chapter 1.4.1. 4) Delegation of Domain / Email validation to third parties: CA does not delegate Domain / Email validation to third parties, see CP/CPS, Chapter 3.2. 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: CA does not distribute generated private keys in PKCS#12 files, see CP/CPS, Chapter 6.1.2 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: CA does not issue certificates for internal domains, see CP/CPS chapter 7.1.2.4 10) OCSP Responses signed by a certificate under a different root: No 11) SHA-1 Certificates: CA does not issue SHA-1 certificates, see CP/CPS chapter 7.1.3. 12) Generic names for CAs: No 13) Lack of Communication With End Users: See CP/CPS 5.2.1, “PKI Order Management”. 14) Backdating the notBefore date: Backdating the notBefore date is not performed by the CA.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Swiss Government Root CA III	**Root Case No**	R00000115
Request Status	Ready for Public Discussion	**Case Number**	00000042

Certificate Data

Certificate Issuer Common Name	Swiss Government Root CA III
O From Issuer Field	Swiss Government PKI
OU From Issuer Field	www.pki.admin.ch
Valid From	2016 Apr 15
Valid To	2041 Apr 15
Certificate Serial Number	00fb1f0b422ba8413e57d1ee2a6e5a4fbb
Subject	CN=Swiss Government Root CA III, OU=www.pki.admin.ch, O=Swiss Government PKI, C=CH
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	CC:EA:E3:24:45:CD:42:18:DD:18:8E:AD:CE:B3:13:3C:7F:B3:40:AD
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
Certificate Fingerprint	84:53:9C:5F:F1:3F:09:B4:75:D9:7D:B4:E6:EC:30:F8:68:D9:70:B3:59:84:AF:35:23:48:75:47:4C:9A:31:15
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	The 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
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
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.16.756.1.17.3.61.2	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	Name constrains are not considered by the CA.	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://www.valid-ev.pki.admin.ch	**Verified?**	Verified
Test Website - Expired	https://www.expired-ev.pki.admin.ch		
Test Website -	https://www.revoked-ev.pki.admin.ch		

Revoked	
Example Cert	
Test Notes	

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

Revocation Tested	No Errors	**Verified?**	Verified
CA/Browser Forum Lint Test	Certificate not found.	**Verified?**	Verified
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	ev-checker exited successfully: Success!	**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	The “Swiss Government Public Trust Standard CA 02” subCA has been cross-signed by QuoVadis Enterprise Trust CA 2 G3. The cross-signed certificate is technically constrained to the domains listed in Annex B (section 9.19) of the CPS.	**Verified?**	Verified
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 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.	**Verified?**	Verified

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	http://www.pki.admin.ch/public/83823_Checkliste-Genehm-SSL-TLS-ZertifAntr-CAs-SwissGov-PKI-160513-e_pub.pdf	**Verified?**	Verified
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	https://home.kpmg.com/xx/en/home.html	**Verified?**	Verified
Auditor Qualifications	KPMG is accredited according to X9.79 (Webtrust).	**Verified?**	Verified
Standard Audit	http://www.pki.admin.ch/public/25-01-2017-BIT-ZertES-Certification-Confirmation-2017_Final.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	1/25/2017	**Verified?**	Verified
BR Audit	http://www.pki.admin.ch/public/25-01-2017-BIT-ZertES-Certification-Confirmation-2017_Final.pdf	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	1/25/2017	**Verified?**	Verified
EV SSL Audit	http://www.pki.admin.ch/public/25-01-2017-BIT-ZertES-Certification-Confirmation-2017_Final.pdf	**Verified?**	Verified
EV SSL Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV SSL Audit Statement Date	1/25/2017	**Verified?**	Verified
BR Commitment to Comply	in CP/CPS, Chapter 1.1.2 and 8.4	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8859143	**Verified?**	Verified
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 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.	**Verified?**	Verified
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	Not requesting Email trust bit.	**Verified?**	Not Applicable

Procedures			
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Smart card authentication is required for all accounts capable of directly causing certificate issuance For system operation and maintenance segregation of duties is used (4 eyes principles), i.e. operator actions can only be performed with the security credentials of security officers	**Verified?**	Verified
Network Security	See CP/CPS, Chapter 6.7. We confirm that we have done the following, and will do the following on a regular basis: - Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements. - Check for mis-issuance of certificates, especially for high-profile domains. - Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. - Ensure Intrusion Detection System and other monitoring software is up-to-date. - Ensure that we are able to shut down certificate issuance quickly if we are alerted of intrusion.	**Verified?**	Verified