Bugzilla ID: 435026
Bugzilla Summary: Add Swiss BIT Root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Name	Swiss BIT
Website URL	http://www.bit.admin.ch/
Organizational type	Government Agency
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 (one of the biggest employers in Switzerland) and third parties. The FOITT also operates a carrier network for the Federal administration and organisations close to the administration. Various, partly encrypted, virtual private networks (VPN) are operated on this carrier network. 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.
CA Contact Information	CA Email Alias: pki-info@bit.admin.ch CA Phone Number: +41 31 325 90 11 Title / Department: Swiss Government's PKI Manager

Technical information about each root certificate

Certificate Name	Swiss Government Root CA II
Issuer	CN = Swiss Government Root CA II OU = Certification Authorities OU = Services O = The Federal Authorities of the Swiss Confederation C = CH
Cert summary	This root cert is offline and signs internally-operated intermediate certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=549069 http://www.bit.admin.ch/adminpki/00247/index.html?lang=de&download
SHA-1 fingerprint	C7:F7:CB:E2:02:36:66:F9:86:02:5D:4A:3E:31:3F:29:EB:0C:5B:38
Valid from	2011-02-16
Valid to	2035-02-16

Cert Version	3
Cert Signature Algorithm	SHA-256
Modulus length	4096
Test website	https://www.regular.pki.admin.ch/
CRL URLs	http://www.pki.admin.ch/crl/RootCAII.crl http://www.pki.admin.ch/crl/RegularCA01.crl (Next update 7 days) CP/CPS section 4.9.7: every 7 (seven) days
OCSP Responder URL	http://www.pki.admin.ch/aia/ocsp No OCSP URI in AIA in end-entity cert CP/CPS section 7.3: OCSP profile: Swiss Government's PKI does not offer any online service (OCSP) OCSP is required now by CA/Browser Forum's Baseline Requirements
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Verification Type	OV
EV policy OID	Not Applicable, not requesting EV treatement

CA Hierarchy Information for each root certificate

CA Hierarchy	CP/CPS section 1.3.1: Certification authorities • 'Machine certificates' issued for Web-servers, servers and network components operated by administrative bodies to support SSL (including SAN- and wildcard-certificates). • 'Group mailbox certificates' – certificates for signing and en-cryption, issued for shared mailboxes used by administra-tive bodies. The certified key pairs are distributed to all us-ers entitled to access the individual mailboxes. • 'Organization certificates' – certificates for authentication, signing and encryption issued to administrative bodies (fed-eral, cantonal or communal) as well as to external organiza-tions to support Sedex (primarily intended for ensuring traceability). • 'e-Dec certificates' – authentication certificates issued to employees of companies/organizations using the electronic goods declaration in their transactions with the Federal Cus-toms Administration. • 'Code signing certificates' – certificates for signing pieces of code, e.g. applets, issued to employees of the administra-tion responsible for web services and/or applications which must be able to prove their authenticity.
Externally Operated subCAs	All SubCAs of this root are internally operated.
Cross-Signing	No Cross-Signing used

Verification Policies and Practices

CP/CPS	Document Repository: http://www.bit.admin.ch/adminpki/00243/index.html?lang=de Swiss Government Root CA II CP/CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=758550
Audit	Need link to actual audit statement. For your next audit, please make sure it meets the requirements of version 2.1 of Mozilla's CA Certificate Policy https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Audit_Criteria https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Baseline_Requirements Audit Type: • ETSI 101 456, ETSI TS 102 042 • ISO 27001 Auditor: • In&Out (internal audits) • KPMG Switzerland (external audits) Auditor Website: • http://www.inout.ch • http://www.kpmg.com Audit Statement: • CP/CPS section 8 Compliance Audit and other Assessments. • Swiss Government's PKI Root CA II and the subordinated Swiss Government Regular CA 01 are subject to a verification of their compliance with the requirements of this CP/CPS at least yearly. These audits are done by the Auditor (see 5.2.1). • Additionally, as Root CA II and Regular CA 01 are operated in the identical environment and subject to the identical security requirements as Root CA I and its subordinated qualified/enhanced Cas, the yearly recertification of the qualified Cas by the Swiss Certification Body essentially covers opera-tion of Root CA II and Regular CA 01 as well.
Baseline Requirements	The CA/Browser Forum's Baseline Requirements are required for all root certs with the Websites (SSL/TLS) trust bit enabled. https://www.cabforum.org/documents.html Please carefully review the Baseline Requirements document, and update your CA practices and policies accordingly. Please also respond to https://wiki.mozilla.org/CA:Communications#January_10.2C_2013 Version 2.1 of Mozilla's CA Certificate Policy was published in February, and is available here: http://www.mozilla.org/projects/security/certs/policy/
SSL Verification Procedures	CP/CPS section 3.2.3 Authentication of individual identity • In order to guarantee the correctness of the link between a pair of cryptographic keys, or more accurately between a public key and a certificate owner, the registration agents must satisfy themselves as to the identity of the certificate applicant. The task of identifying the certificate applicant and compiling the information required to issue a certificate is delegated to the registration agents.

	• The process to authenticate the certificate applicant is part of the following issuing procedure: • Only members of the restricted user group DomainSSL can apply for certificates. • To become member of the restricted user group DomainSSL, an applicant needs to hand in a written request form, signed by a duly registration agents of the applicants organization unit. • Request forms are validated by Swiss Government PKI Security Officers - identifying both applicant and registration agents in the official directory of Swiss Government. • After approval by a Swiss Government PKI Security Officers, a Swiss Government PKI Operator authorizes the applicant in the DomainSSL provisioning application. • As a member of the restricted user group DomainSSL an applicant can post a certificate request via the web-based provisioning application (https). The provisioning application enforces strong client-authentication on the basis of a enhanced certificate of Swiss Government PKI (personal Smartcard). • Contained in the request are domain name and optional subject alternative names. The content may also detail hostnames, IP addresses, e-mail or additional domains controlled or owned by the applicant. No private key is submitted, only CSR. • All posted requests are verified individually within 1-3 working days by Swiss Government PKI: o On the basis of the registration process of the restricted user group DomainSSL Swiss Government PKI deems valid all requests for DomainSSL matching the applicants organizational unit (limited to Swiss Government Domains). o If the request contains a hostname or additional domain not identifying the organizational unit of the applicant, Swiss Government PKI requests additional evidence (Swiss Official Gazette of Commerce "SHAB", WHOIS combined with personal contact (telephone/e-mail) to the owner of the domain). o If an e-mail address is included in the CSR, the address is validated (challenge response procedure). • If a request is verified positively, Swiss Government PKI signs the CSR and submits the certificate to the applicant.
Organization Verification Procedures	CP/CPS section 3.2.5: Validation of authority CP/CPS section 4.1.1 Who may submit a certificate application. CP/CPS section 1.3 PKI participants CP/CPS section 4.1.2 Enrollment process and responsibilities • Describes the enrollment processes for the different types of certificates issued by Swiss Government Regular CA 01 together with the responsible parties. • The registration agents (see section 1.3.2) makes a request to Swiss Government's PKI for himself and a deputy to be admitted to the registration application for the relevant domain (e.g. sedex, group mailboxes, e-dec etc.). These persons must be authorized by the director of their administrative unit and must have passed the "personal security check" of the federal department of defence ("Personensicherheitspruefung"). Registration agents get an individual introduction to their new task by Swiss Government's PKI staff, and have to pass regular quality checks and external auditing. They may apply for certificates for any persons/organizations and download them. They are responsible for their publication and installation and are obliged to revoke the certificates through the registration application on suspicion of violation of the CP/CPS. The Swiss Government's PKI Security Officers observe the system and check regularly the databases for wrongly or illegally issued certificates and entries. • Swiss Government's PKI examines requests to authorize registration agents for using the registration application. It grants

	access if all the required documents have been submitted. The registration application is operated by the responsible administrative unit (federal, cantonal or municipal administration). A framework agreement and an SLA govern the relationship be-tween Swiss Government's PKI and the registration agents. • Any certificate applicant addresses the responsible registration agent with the requirement to obtain a certificate, who does the necessary verification (e.g. identification of the per-son/organization) as the first step in the certificate issuance process.. • The registration agent then prepares an entry for the person organization of the relevant certificate applicant in the federal administration's directory, Admin-Directory. • The registration agent uses a Swiss Government's PKI enhanced certificate (strong authentication) to log in to the registration application. After entering data identifying the certificate applicant in sufficient detail, the registration agent proceeds per the instructions of the registration application and finally approves the request. The application generates the cryptographic keys and submits the request(s) for the corresponding certifi-cate(s) to the CA, which in turn generates the certificate(s) and returns it/them to the registration application. • The registration agent must inform the certificate applicant about his obligations and responsibility with regard to using the certificates. 4.2 Certificate application processing • Additional information is included in the registration directives of Swiss Government's PKI for registration agents. 4.2.1 Performing identification and authentication functions • Swiss Government's PKI identifies registration agents authorized by the management of the administrative units having a need for certificates just initially and authorizes them to access its registration application for requesting and downloading certificates (Server administrators acting as registration agents for machine certificates must be identified face-to-face on the basis of a formal identity document). The registration application then authenticate the agents with each certificate request they issue. Registration agents authorized to approve requests autonomously are authenticated by the RA application on the ba-sis of enhanced certificates. 4.2.2 Approval or rejection of certificate applications • The registration agent must verify that the application is genuine (checking the application form, checking the data in Admin-Directory, checking the identity of the applicant). If the data is incomplete and/or the certificate applicant is not identifiable, the registration agent stops processing the application.
Email Address Verification Procedures	CP/CPS section 3.2.4: Non-verified subscriber information • All the information required to identify the applicant is verified. For example if the request for a Server Certificate contains an e-mail address, it is checked before the issuance of the certificate. CP/CPS section 4.3.2: Notification to subscriber by the CA of issuance of certificate • Issuance of the certificate is notified to the applicant by means of an e-mail. The e-mail address indicated in the certificate is used for this purpose. • The e-mail addresses written to the certificates and used for notification are explicitly (machine certificates) or implicitly (personal certificates) verified in the course of registration (see CP/CPS section 3.2.3)
Code Signing Subscriber Verification Procedures	CP/CPS 4.1.2

Multi-factor Authentication	CP/CPS 4.2.1: Registration Agents authorized to approve requests autonomously are authenticated by the RA application on the basis of enhanced certificates (on Smartcard).
Network Security	CP/CPS section 6.7 Network security controls CP/CPS section 5.4 Audit Logging Procedures CP/CPS section 5.4 Audit Logging Procedures CP/CPS 4.2.1 Performing identification and authentication func-tions

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	Yes
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	See below
Revocation of Compromised Certificates	CP/CPS section 4.9
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	CP/CPS section 3.2.3
Domain owned by a Natural Person	CP/CPS section 4.1.1
OCSP	See above
Network Security Controls	See above

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV CP/CPS section 6.3.2: 2 years with end-user certificates
Wildcard DV SSL certificates	CP/CPS section 4.2.3: Wildcard and SAN (Subject Alternative Name) machine certificates are only issued manually and only by the Swiss Government‟s PKI, after having identified the owner face to face with an official identity document (Passport/ Identity card).
Email Address Prefixes for DV Certs	SSL certs are OV
Delegation of Domain / Email validation to third parties	CP/CPS section 1.3.2: Registration authorities • To cope with the variety of certificates issued by Swiss Government Regular CA 01, the submission of requests as well as the registration of applicants and requests is typically done by ‘Registration Agents’ of the different departments employing certificates. These agents are formally identified by the respective department’s management and communicated to Swiss Government’s PKI either directly or through entries

	in suitable directories operated by the Federal Administration. Swiss Gov-ernment's PKI personnel is involved in registration tasks only with requests for specific certificates where the entries in the certificates are of crucial importance (e.g. domain names identified in SSL, SAN or wildcard certificates).Persons authorized to create certificates include, for example, for organization certificates, the Chief Officer or a person to whom he has delegated the duty, for certificates for shared mailboxes, the person responsible for the e-mail address or his deputy, or for e-Dec certificates, the person responsible for the application or deputies appointed by him. o The registration agent makes a request to Swiss Government's PKI for himself and a deputy to be granted access to the registration application for the relevant domain. o The registration application is operated by the responsible administrative unit (federal, cantonal or municipal administration)
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	CP/CPS section 3.2.1: Method to prove possession of private key • The private key for Server Certificates (also known as Machine-Certificates) is typically generated by the Operator of the Server. As only a CSR is submitted to the CA, the private key re-mains in possession of the Operator. In other cases, the private key and the certificate are downloaded by the registration agent (see section 1.3.2) of the registration application in a PKCS#12 file, and forwarded for installation to certificate applicants or technicians (for organization certificates) by encrypted e-mail or on diskette/CD, via a software distribution system, or through private shares. The activation password is notified to the certificate applicant/technician by other means (e.g. new e-mail, phone, fax, in writing, etc.).
Certificates referencing hostnames or private IP addresses	Private IP addresses are not allowed (see CP/CPS 3.2.3)
Issuing SSL Certificates for Internal Domains	.int domains are not allowed (see CP/CPS 3.2.3): • Swiss Govnerment's Regular CA 01 does explicitly not issue certificates for identifying servers not visible to Internets' DNS i.e. using the following identifiers: o host names o private IP addresses o internal domain names
OCSP Responses signed by a certificate under a different root	See above
CRL with critical CIDP Extension	CLR imported into Firefox without error
Generic names for CAs	CN and Issuer field are not generic. See above.
Lack of Communication With End Users	Contact information provided in CP/CPS.