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

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Swiss BIT
Website URL	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

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
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 / comments	
URL of Root Cert	https://bugzilla.mozilla.org/attachment.cgi?id=549069
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	If requesting the Website (SSL/TLS) trust bit, then please provide a url to a test website whose SSL cert chains up to this root.
CRL URLs	ARL, sub CA CRL DP, end-entity cert CRL DP.
CRL update frequency	CP/CPS section 4.9.7: Swiss Government's PKI updates its ARL once a year if none of the Certification Authority's certificates were cancelled during this period. The Certification Authority updates its CRL: □ after every certificate revocation □ every 7 (seven) days if no certificate has been revoked in this period.
OCSP Responder URL	None. CP/CPS section 2.3: Swiss Government's PKI does not offer any online service (OCSP)
CA Hierarchy	List, description, and/or diagram of all intermediate CAs (current and planned) signed by this root. Identify which subCAs are (or will be) internally-operated and which are (or will be) externally operated.
Externally Operated subCAs	If this root has or will have subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List all other roots for which this root CA has issued cross-signing certificates. List all other root CAs that have issued cross-signing certificates for this root CA. Note whether the roots in question are already included in the Mozilla root store or not.
Requested Trust Bits	One or more of: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Verification Type	e.g. DV, OV, and/or EV
EV policy OID	Not Applicable
CP/CPS	Admin PKI Repository: http://www.pki.admin.ch/ Swiss Government Root CA II CP/CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=549071
Audit	Audit Type: one of ETSI 101 456, ETSI TS 102 042, or WebTrust CA (or equivalent) Auditor: Auditor Website: Audit Statement: Government CAs -- According to section 7 of Mozilla's CA Certificate Inclusion Policy, the audit must be performed according to criteria that is equivalent to one (or more) of ETSI TS 101 456, ETSI TS 102 042, or WebTrust CA. The government's auditing agency should provide a statement about which of these their government criteria is equivalent to. -- According to sections 10 and 11 of Mozilla's CA Certificate Inclusion Policy, it is acceptable for a government auditing organization to perform the audit of the government's CA organization. It must be clear that the CA organization does not audit itself.

Identity / Organization Verification	CP/CPS section 3.2.3 Authentication of the certificate applicant 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 authorised persons 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 authorised person. The authorised persons must: check the content of the Web form for applying for a certificate check whether the applicant is subject to registration in the Directory Service Admin-Directory satisfy themselves that the name of the applicant in the Directory is identical with the name in the certificate application form5 In case of certificate requests containing a Domain Name (Server Certificates), the applicant's authorization for this domain is checked before the issuance. CP/CPS section 3.2.4: 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 4.1.1 Who can apply for a certificate? Certificates of class C/C-Trustcenter and D may be applied for by members of an administrative unit (federal, cantonal or municipal administration) that have concluded a framework agreement and SLA with Swiss Government's PKI. CP/CPS section 1.3 The Certification Authority „Swiss Government Root CA II" is part of Swiss Government's PKI and issues digital certificates of class C/C-TrustCenter and class D. „ … These are soft certificates and do not use any Secure Signature Creation Device (SSCD). A certificate of class C/C-Trustcenter is issued for natural persons and organisations and can be used for signing purposes, encryption, and authentication. Class D certificates are only for authentication. … Certificate owners act on behalf of an administrative unit (federal, cantonal or municipal administration) within the context of the relevant application. Certificate owners are any natural persons or legal entities or organisational units that own certificates from the Certification Authority „Swiss Government Root CA II". CP/CPS section 4.1.2 Registration process Swiss Government's PKI provides a modular Web-based registration application for the registration process, depending on the intended purpose. The authorised person (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, class D 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 ("Personensicherheitspru□fung"). Registration officer get a private course from the Swiss Government's PKI for their new task, and have to pass to regular quality checks and external auditings. They may apply for certificates for any persons/organisations 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 wrong or not legally issued certificates and entries. Swiss Government's PKI examines requests to register authorisations for the registration application. It grants the authorisations if all the required documents have been submitted. The registration application is operated by an administrative unit (federal, cantonal or municipal administration). A framework agreement and an SLA govern the relationship between Swiss Government's PKI and the authorised person. The certificate applicant refers to the authorised person with the requirement to obtain a certificate. The formalities are dealt with at this stage (e.g. identification of the person/organisation). The authorised person then prepares an entry for the person /organisation of the relevant certificate applicant in the federal administration's directory, Admin-Directory. The authorised person uses an Swiss Government's PKI class B certificate (strong authentication) to log in to the registration application. After identification/authentication of the certificate applicant, the authorised person carries out the instructions in the registration application. The application generates the cryptographic keys and applies for the certificates from the CA, which generates the certificate and returns it to the registration application. The authorised person must inform the certificate applicant about his obligations and responsibility with regard to using the certificates. 4.2 Handling the application for a certificate Additional information is included in the registration directives of Swiss Government's PKI for authorised persons. 4.2.1 Identification and authentication of the applicant The task of identifying/authenticating the certificate applicant is performed by authorised persons. The authorised persons must be satisfied as to the identity of the applicant. 4.2.2 Approval/rejection of the application for a certificate The authorised person 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 authorised person stops processing the application.
Domain Name Ownership / Control	CP/CPS section 3.2.3: In case of certificate requests containing a Domain Name (Server Certificates), the applicant's authorization for this domain is checked before the issuance. This is not sufficient, there needs to be information in the CP/CPS about the actual procedure to confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership

Email Address Ownership / Control	CP/CPS section 3.2.4: 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: Issue 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. This is not sufficient, there needs to be information in the CP/CPS about the actual procedure to confirm that the certificate subscriber owns/controls the email address to be included in the certificate, before the certificate is issued. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control
Identity of Code Signing Subscriber	Not Applicable – Not requesting code signing trust bit. I didn't see reference to Code Signing certs in the CP/CPS, so I'm assuming this is not applicable.
Potentially Problematic Practices	Please review and comment on Mozilla's list of potentially problematic practices http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o CP/CPS section 6.3.2: public key of the subscriber: three (3) years, or as the case may be, two (2) years, depending on the intended purpose • Wildcard DV SSL certificates o 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). • Delegation of Domain / Email validation to third parties o CP/CPS section 1.6: Registration Authority: Person or organisation responsible for identifying/authenticating a subscriber before certificates are issued to him, but which does not sign or issue any certificates. o CP/CPS section 1.3.2: o The Certification Authority „Swiss Government Root CA II" operates a central Registration Authority (RA), which is accessible to authorised persons at all times through a Web-based registration application. o Persons authorised to create certificates include, for example, for C-Trustcenter certificates, the Chief Officer or a person to whom he has delegated the duty, for C-group mailbox certificates, the person responsible for the e-mail address or his deputy, or for class D certificates, the person responsible for the application or deputies appointed by him. o The authorised person makes a request to Swiss Government's PKI for himself and a deputy to be admitted to the registration application for the relevant domain. o The registration application is operated by an administrative unit (federal, cantonal or municipal

	administration).
	• Issuing end entity certificates directly from roots
	  ○
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○
	• Distributing generated private keys in PKCS#12 files
	  ○ CP/CPS section 3.2.1: 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 remains in possession of the Operator. In other cases, the private key and the certificate are downloaded by the authorised person (see section 1.3.2) of the registration application in a PKCS#12 file, and forwarded for installation to certificate applicants or technicians (for organisation 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.). The PKCS#12 file is installed on the local machine. As a consequence the private keys are in the possession of the certificate owner.
	• Certificates referencing hostnames or private IP addresses
	  ○
	• OCSP Responses signed by a certificate under a different root
	  ○ Not applicable.
	• CRL with critical CIDP Extension
	  ○