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 about the CA's associated organization

CA Name	Swiss Government Root II
Website URL	www.pki.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 / FOITT

Technical information about each root certificate

Certificate Name	Swiss Government Root CA II
Certificate Issuer Field	CN = Swiss Government Root CA II OU = Certification Authorities OU = Services O = The Federal Authorities of the Swiss Confederation C = CH
Certificate Summary	Swiss Government Root CA II operating at first – root – level acts as the common trust reference for all regular CAs and end-user certificates. It issues CA certificates to the CAs operating at second level exclusively, while these CAs in turn issue certificates to the end-users. The two-level CA-hierarchy enables Swiss Government's PKI to easily add additional subordinated CAs to an existing Root CA when needed and thus avoid the comparably large effort to establish new Root CAs among all interested parties (requires incorporation of Root CA certificate in all relevant browsers, installation by trusted personnel, etc.).
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=549069

	http://www.bit.admin.ch/adminpki/00247/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDen53fGym162epYbg2c_JjKbNoKSn6A--
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
Certificate Version	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	RSA modulus length: 4096
Test website	https://www.regular.pki.admin.ch/
CRL URLs	URL: • ldap://admindir.admin.ch:389/cn=Swiss%20Government%20Root%20CA%20II,ou=Certification%20Authorities,ou=Services,o=Admin,c=CH • URL=http://www.bit.admin.ch/adminpki/03603/index.html?lang=de CRL update frequency: • CP/CPS section 4.9.7 CRL import Firefox Browser Test: • Successfully imported. No errors
OCSP URL	CP/CPS section 7.3: OCSP profile • Swiss Government's PKI does not offer any online service (OCSP)
Requested Trust Bits	• Websites (SSL/TLS) • Email (S/MIME) • Code Signing
SSL Verification Type	OV: • CP/CPS section 4.1.2 Enrollment process and responsibilities
EV policy OID	Not Applicable

CA Hierarchy information for each root certificate

CA Hierarchy	CP/CPS section 1.1: Overview • Swiss Government Root CA II operating at first – root – level acts as the common trust reference for all regular CAs and end-user certificates. It issues CA certificates to the CAs operating at second level exclusively, while these CAs in turn issue certificates to the end-users. • Figure 1.1 - CA hierarchy 'Swiss Government Root CA II' 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 encryption, issued for shared mailboxes used by administrative bodies. The certified key pairs are distributed to all users entitled to access the individual mailboxes. • 'Organization certificates' – certificates for authentication, signing and encryption issued to administrative bodies (federal, cantonal or communal) as well as to external organizations 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 Customs Administration. • 'Code signing certificates' – certificates for signing pieces of code, e.g. applets, issued to employees of the administration responsible for web services and/or applications which must be able to prove their authenticity.
Externally Operated SubCAs	All SubCAs of this root are operated solely by the FOITT.
Cross-Signing	No Cross-Signing used
Technical Constraints on Third-party Issuers	No Third-party issuers

Verification Policies and Practices

Policy Documents	URL: • http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf
Audit	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 operation of Root CA II and Regular CA 01 as well.

Baseline Requirements	Not applicable (no WebTrust audit, EV)

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 Ga-

	zette 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 • Swiss Government’s PKI validates the authority of Registration Agents before enabling them to use any of the applications necessary for requesting certificates and approving requests. For that purpose either consults with the management of the administrative unit concerned or verifies the function has been formally assigned in the appropriate directory (see section 4.1.2). CP/CPS section 4.1.1 Who may submit a certificate application. • Requests for regular certificates may be submitted exclusively by server administrators and Registration Agents formally authorized for the task (see section 1.3.2). CP/CPS section 1.3 PKI participants • The Certification Authority „ *Swiss Government Root CA II* is the first level CA constituting the basis of trust for all regular certificates. … The Swiss Government Root CA II certificate is formally distributed as ‘trust anchor’ to all participants in the Swiss administration.. „ (see section 1.3.1 Certification authorities) … 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 organizational units that own certificates from a Certification Authority subordinated to „Swiss Government Root CA II“. 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”). Registra-

	tion 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 between 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 person/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 certificate(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 • Issueance 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	Done, see CP/CPS 4.1.2
Multi-factor Authentication	CP/CPS 4.2.1 Performing identification and authentication functions • 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. • Swiss Government's PKI's certification infrastructure is operated in a specific network-segment separated from the federal administration's intranet by a gateway acting as a firewall. This blocks all protocols which are not absolutely necessary with Swiss Government's PKI's operations. CP/CPS section 5.4 Audit Logging Procedures • All relevant events related to the issuance and maintenance of Swiss Government's PKI certificates are logged automatically or manually (journals, e.g. for recording entries to/exits from a protected room) for checking purposes, together with date/time, type, reason for and result of action, name of requestor, name(s) of person(s) approving (where applicable). CP/CPS section 5.4.8 Vulnerability assessments • A dedicated application analyzes Swiss Government's PKI's certification infrastructure at least once a week, identifying vulnerabilities and potential attempts at breaching the security of the system. • There is a Host Based Intrusion Detection System (OSSEC) in use as well as a NESSUS-Scanner.

	• The PKI Security Officer is warned in case there are critical anomalies detected. CP/CPS 4.2.1 Performing identification and authentication functions • Registration Agents authorized to approve requests autonomously are authenticated by the RA application on the basis of enhanced certificates (on Smartcard).

Response to Mozilla's CA Recommended Practices

Publicly Available CP and CPS	CP/CPS section 2 Publication and Repository Responsibilities • FOITT makes information related to Swiss Government Root CA II and its subordinated CAs publicly available through Swiss Government's PKI's web site (www.pki.admin.ch) and/or the Admin-Directory, a directory service compliant with ITU-T recommendation X.500. CP/CPS 2.2 Publication of certification information • FOITT publishes information related to certificates issued by Swiss Government Root CA II and its subordinated certification authorities: the current version of the CP/CPS for the Swiss Government Root CA II and its subordinated certification authorities. CP/CPS section 9.10 Term and termination • This CP/CPS becomes valid the day it is published on Swiss Government's PKI's website (see section 2.2).
CA Hierarchy	See "CA Hierarchy information for each root certificate"
Audit Criteria	See "Verification Policies and Practices"
Document Handling of IDNs in CP/CPS	(see below)
Revocation of Compromised Certificates	CP/CPS section 4.9: Certificate revocation and suspension Regular certificates must be revoked under the following circumstances: • A compromise of private key or password of a soft-token is suspected or has actually happened. • A certificate token has been erased. • Parts of the data in a certificate are obsolete. • A certificate has been acquired illegitimately. • A subscriber has been dismissed or suspended by his employer. • The contract with a subscriber has expired. • A subscriber or a Registration Agent has violated the rules set out in this CP/CPS. • Swiss Government Regular CA 01 ceases its operation. CP/CPS section 4.9.2 Who can request revocation • Requests for revoking certificates can be requested by: o Subscribers.

	o The Registration Agent having done the registration for the certificate in question. o The administrative unit employing the subscriber. o The PKI Security Officer. o The PKI Manager. Certificates may also be revoked on the basis of a judicial decision. The ensuing request in writing and founded must be addressed to the PKI Manager as per 1.5.2. CP/CPS section 4.9.3: Procedure for revocation request • The procedure for revoking regular certificates is as follows: o The actual requestor (see 4.9.2) initiates the process and authenticates with a Registration Agent (as detailed in 3.4). o The Registration Agent verifies requestor's entitlement for launching the request. Provided the result is positive the Registration Agent approves the request and forwards it to Swiss Government Regular CA 01. o The CA processes the revocation request automatically and instantaneously. It then informs the Registration Agent on the completed revocation.
Verifying Domain Name Ownership	CP/CPS section 3.2.3: With applications for machine certificate Swiss Government's PKI ensures the requests and the data therein are authentic in the following way: – Machine certificates are issued exclusively for domains owned by the federal, or a cantonal or communal administration. – As a prerequisite, signatories of the departments owning domains need to formally authorize selected system administrators to act as Registration Agents for requesting machine certificates identifying the respective domains. Swiss Government's PKI maintains a list of these particular Registration Agents (which form the 'DomainSSL' group) together with the domains they are responsible for. – With each request for a machine certificate, the authorization of the requester and the validity of the domain(s) to be identified are verified per the above list. – E-mail addresses to be added to machine certificates are validated by Swiss Government's PKI staff through a challenge/response procedure. – Requests for domains not supported by the list or not in compliance with the established guidelines for SAN-certificates undergo an exceptional process wherein the requester is required to give further evidence supporting the request, e.g. on the basis of the Swiss Official Gazette of Commerce 'SHAB' or 'WHOIS' supported by an oral or e-mail statement of the domain owner identified.
Verifying Email Address Control	Applicants for regular personal certificates are authenticated by means of the corresponding entries in Admin-Directory. As Admin-Directory is a trusted database, subscriber identifying data such as e-mail addresses etc. may be retrieved from it without additional

	verification. Representatives of private companies requiring a certificate first need to get an formal entry established in Admin-Directory, upon which the corresponding data may be trusted in the same way as with federal employees.
Verifying Identity of Code Signing Certificate Subscriber	(see CPS 4.1.2, table 4.5)
DNS names go in SAN	CP/CPS section 3.2.3: • Requests for domains not supported by the list or not in compliance with the established guidelines for SAN-certificates undergo an exceptional process wherein the requester is required to give further evidence supporting the request, e.g. on the basis of the Swiss Official Gazette of Commerce 'SHAB' or 'WHOIS' supported by an oral or e-mail statement of the domain owner identified.
Domain owned by a Natural Person	Swiss Government's PKI SSL certificates can only be purchased by organizations (within the administration). CP/CPS section 4.1.1: Who may submit a certificate application • Requests for regular certificates may be submitted exclusively by server administrators and Registration Agents formally authorized for the task (see section 1.3.2).
OCSP	See "Technical information about each root certificate"
Network Security Controls	See "Verification Policies and Practices"

Response to Mozilla's list of Potentially Problematic Practices

Long-lived DV certificates	CP/CPS section 6.3.2: Certificate operational periods and key pair usage period
	• Swiss Government's PKI certificate validity periods are:
	  • 24 years with Swiss Government Root CA II.
	  • 14 years with the subordinated CA.
	  • 2 years with end-user certificates.

Wildcard DV SSL certificates	(see CP/CPS --> 4.2.2)
Email Address Prefixes for DV Certs	E-Mail addresses are retrieved from requestors' entries in Admin Directory (trusted, see CP/CPS 3.2.3)
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	CP/CPS section 1.1: Overview • Swiss Government Root CA II operating at first – root – level acts as the common trust reference for all regular CAs and end-user certificates. It issues CA certificates to the CAs operating at second level exclusively, while these CAs in turn issue certificates to the end-users.
Allowing external entities to operate subordinate CAs	All SubCAs of this root are operated solely by the FOITT.
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 remains 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): • Swiss Government'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
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 “Technical information about each root certificate”
CRL with critical CIDP Extension	CRL import Firefox Browser Test: • Successfully imported. No errors
Generic names for CAs	CN = Swiss Government Root CA II OU = Certification Authorities OU = Services O = The Federal Authorities of the Swiss Confederation C = CH
Lack of Communication With End Users	CP/CPS section 1.5.2 : Contact person • Contact person is the PKI Manager: *Swiss Government* *Federal Office of Information Technology, Systems and Telecommunication FOITT* *PKI Manager* *PKI* *74, Monbijoustrasse* *3003 Berne* *Switzerland*