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 Federal Office of Information Technology 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: AdminPKI Manager

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

Info Needed	**Data**	**Data**
Certificate Name	Admin-Root-CA	AdminCA-CD-T01
Cert summary / comments	This root has three internally-operated subordinate CAs, with two currently in operation. The sub-CAs issue certificates for hardware tokens to be used 1) for identification, digital signatures, encryption, and authentication of individuals 2) for qualified digital signatures. The hardware tokens are issued to employees of an administrative unit (federal, cantonal or municipal administration) who already have their information published in Swiss BIT's Admin-Directory.	This root does not have subordinate CAs, it issues end-entity certificates directly. The purpose of AdminCA-CD-T01 is to issue user/organisation certificates and device/server certificates of classes C/C-TrustCenter and 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. These certificates 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 BIT, such that their information is already in Swiss BIT's Admin-Directory.

URL of Root Cert	https://bugzilla.mozilla.org/attachment.cgi?id=377526	https://bugzilla.mozilla.org/attachment.cgi?id=377531
SHA-1 fingerprint	25:3f:77:5b:0e:77:97:ab:64:5f:15:91:55:97:c3:9e:26:36:31:d1	6b:81:44:6a:5c:dd:f4:74:a0:f8:00:ff:be:69:fd:0d:b6:28:75:16
Valid from	11/15/2001	1/25/2006
Valid to	11/10/2021	1/25/2016
Cert Version	3	3
Modulus length	2048	2048
Test website(s) or cert(s)	End-entity certs under this root get generated on hard tokens.	https://www.medreg.admin.ch/
CRL URL	ARL: http://www.pki.admin.ch/crl/Admin-Root-CA.crl	http://www.pki.admin.ch/crl/AdminCA-CD-T01.crl NextUpdate: 8 days
CRL update frequency	CPS sections 4.9.7 and 4.9.8: The Certification Authority updates its CRL: • after each certificate revocation • every 7 (seven) days if no certificate has been revoked during this period. • Within 24 hours after receiving a revocation request.	
OCSP Responder URL	None	None
CA Hierarchy Diagram	http://www.bit.admin.ch/adminpki/00247/index.html	
CA Hierarchy Description	Admin-Root-CA issues the following 3 sub-CAs: -> AdminCA-A-T01 issues Class A certificates – HW Token Personal Identification - Legally binding signature -> Admin-CA2 -> Admin-CA3 Admin-CA2 and Admin-CA3 issue Class B certificates – HW Token Personal Identification – Signature, Encryption, Authentication	Admin-CA-CD-T01 issues end-entity certificates directly: Class D Certificates – Soft-Token – Administrative Identification – Authentication Maschinen (Machine) Certificate – Soft-Token – Administrative Identification – Authentication of webserver, application server, etc. CodeSigning Certificate – HW or SW Token – Personal Identification – Only Signatures
Externally Operated subCAs	None	None
Cross-Signing	None	None
Requested Trust Bits	Email	Websites Email Code Signing
SSL Verification Type	No SSL Certificates chain to this root. The certs chaining up to this root are for digital signatures and encryption.	OV
EV policy OID	Not Applicable	Not Applicable

CP/CPS	Admin PKI Repository: http://www.pki.admin.ch/ Hierarchy Diagram: http://www.bit.admin.ch/adminpki/00247/index.html Admin-Root-CA Documents (email, digital signature) CP/CPS for AdminPKI - Class A (English Translation): https://bugzilla.mozilla.org/attachment.cgi?id=374130 CP/CPS for AdminPKI - Class A (AdminCA-A-T01 sub-CA): http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf CP/CPS for AdminPKI-Class B (Admin-CA2 and Admin-CA3 sub-CAs): http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_3_FR.pdf AdminCA-CD-T01 Documents (SSL, code signing) CP/CPS Class CD-T01 (English): https://bugzilla.mozilla.org/attachment.cgi?id=376403 Process Description for Provisioning Server certificates (German): https://bugzilla.mozilla.org/attachment.cgi?id=382263
AUDIT	Audit Type: ETSI 101 456 Auditor: KPMG SA (Klynveld Peat Marwick Goerdeler SA) Auditor Website: http://www.kpmg.ch Audit Statement: https://bug435026.bugzilla.mozilla.org/attachment.cgi?id=385981 (2009.02.28) Email confirmation of audit statement from Auditor: > From: Grubenmann, Reto <retogrubenmann@kpmg.com> > Subject: RE: Confirmation of new Audit Statement for BIT > To: "Kathleen Wilson" <kathleen95014@yahoo.com> > Date: Thursday, July 9, 2009, 11:04 PM > Dear Mrs. Wilson > I do confirm that the content of this KPMG letter is right and all the surveillance audits have been performed by KPMG > AG (Switzerland). > With kind regards, > Reto Grubenmann > Leader of certification body, KPMG AG (Switzerland)
Admin-Root-CA Verification of Subscriber Identity	CPS Section 3.2.3 Verification of the identity of the certificate applicant The tasks of identifying the certificate applicants and gathering all the information required for issuing a certificate is delegated to the Local Registration Authority. The Local Registration Authority must: • verify the content of the certificate application form • verify that the applicant is registered in the *Admin-Directory* • ensure that the applicant’s name in the directory is the same as that on the ID presented • scan the identification documents presented.

AdminCA-CD-T01 Organization Verification	CPS Section 1.3.2 Registration Authority The Certification Authority AdminCA-CD-T01 operates a central Registration Authority (RA), which is accessible to authorised persons at all times through a Web-based registration application. 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. The authorised person makes a request to AdminPKI for himself and a deputy to be admitted to the registration application for the relevant domain. AdminPKI examines requests to register authorisations for the registration application. It grants the authorisations if all the required documents have been submitted. The duties of the Registration Authority or authorised persons include: • Identification and authentication of certificate applicants … The registration application is operated by an administrative unit (federal, cantonal or municipal administration). A framework agreement and a SLA govern the relationship between AdminPKI and the authorised person/administrative unit. 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 form
Email Address Ownership / Control	The same process is used for both Admin-Root-CA and AdminCA-CD-T01. Relevant sections of each CPS: Section 4.1.1 to 4.3.2 Summary: The Federal Administration maintains a meta-directory called the Admin-Directory. Employees of an administrative unit (federal, cantonal or municipal administration) are registered in the Admin-Directory. Anyone whose personal data are published in the Admin-Directory may complete the certificate application form. The Registration Authority compares the information in the certificate application with the data in the Admin-Directory, including the subscriber's last and first names, distinctive hash code, and e-mail address. The consent of the administrative unit employing the subscriber is required for publishing the certificate in the public version of the Admin-Directory. The applicant is notified by e-mail of the issuance of the certificate. The e-mail address in the certificate is used for this purpose.
Domain Name Ownership / Control	Only applies to AdminCA-CD-T01, for which the SSL trust bit is requested. CP/CPS Class CD-T01 translated into English: https://bugzilla.mozilla.org/attachment.cgi?id=376403

	There is a self-service, web-based registration application for issuing SSL certificates. Only authorised persons as defined in section 4.1.2 of the CP/CPS Class CD-T01 can issue/revoke certificates in this registration application. The user manual for this application has been attached to the bug: https://bugzilla.mozilla.org/attachment.cgi?id=382263 This user manual is intended for employees of an administrative unit who are authorized to issue certificates for servers and manage them. Comment #28: These authorised persons are specially selected by the chief of their departements/organizations (AdminPKI issues certificates only for the federal government and canton departments in Switzerland) . They get an education and have to pass security audits. Even if they can issue Certificates from any Domain, they are not allowed to do so. They are only authorized to issue Certificates for their Department/Organization and they are aware of the consequences of misuse. From CPS section 4.1.2: AdminPKI 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 AdminPKI 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 (“Personensicherheitsprüfung”). Registration officer get a private course from the AdminPKI 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 AdminPKI Security Officers observe the system and check regularly the databases for wrong or not legally issued certificates and entries. To avoid misuse, the security officer has to observe the system once per week for wrong or illegally issued certificates. In Detail, the security officers receive reports. In these reports is declared, which authorized person has issued each specific domain, including organization/department name, address, Issuing Date, and so on... The security officer now checks these reports for suspicious elements (if domain is not a subdomain of admin.ch, it is suspicious because AdminPKI only issues Certificate for federal government and cantonal departments). If such elements were found, he checks if domain and authorized person matches with different WHOIS queries. If not, he has to revoke the certificate and send a notice to the specific chief of department, respective his office. With all the other elements, which are not suspicious, the security officer makes random checks with the same methods as described before. This whole process is described in the internal security officer process (only in German). If you wish i can upload the file. In the current Release of the Provisioning Platform, the AdminPKI handles these security issues reactive. In further release, it will be most likely proactive.

Identity of Code Signing Subscriber	The code signing trust bit is being requested only for the AdminCA-CD-T01 root. Only authorised persons as defined in section 4.1.2 of the CP/CPS Class CD-T01 can request CodeSigning Certificates. After the personal identification of this person, the AdminPKI issues the requested CodeSigning Certificate and delivers it personally to the requester.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o Admin-Root-CA – Not applicable o AdminCA-CD-T01 – SSL certs are OV ▪ CP/CPS section 6.3.2: three (3) years, or as the case may be, (2) years, depending on the intended purpose • Wildcard DV SSL certificates o Admin-Root-CA – Not applicable o AdminCA-CD-T01 – SSL certs are OV. ▪ CP/CPS section 4.2: Wildcard and SAN (Subject Alternative Name) machine certificates are only issued manually and only by the AdminPKI, 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 1.3.2: The Certification Authority AdminCA-CD-T01 operates a central Registration Authority (RA), which is accessible to authorised persons at all times through a Web-based registration application. • Issuing end entity certificates directly from roots o Admin-Root-CA – No. End entity certs are issued from the internally operated sub-CA. o AdminCA-CD-T01 – **This root does not have subordinate CAs. It issues end-entity certificates directly** for users/organizations and devices/servers for identification, digital signatures, encryption, code/document signing, webserver authentication (SSL), and application server authentication. These certificates 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 BIT. o As noted in our problematic practices document, we think that issuing end-entity certificates directly from a root is not a good practice, and that a better practice would be to issue EE certificates from a subordinate CA that can act as the issuing CA. However there is nothing in our current CA policy that prohibits issuing EE certificates directly from a root. • Allowing external entities to operate unconstrained subordinate CAs o Admin-Root-CA – The sub-CAs for this root are internally operated. o AdminCA-CD-T01 – This root has no subordinate CAs. • Distributing generated private keys in PKCS#12 files o Admin-Root-CA – No.

	o AdminCA-CD-T01 ▪ CP/CPS section 3.2.1: 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. ▪ CP/CPS section 4.1.2: The authorised person uses an AdminPKI 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. • Certificates referencing hostnames or private IP addresses o Admin-Root-CA – Not applicable o AdminCA-CD-T01 – Not found • OCSP Responses signed by a certificate under a different root o Admin-Root-CA – Not applicable; OCSP not provided. o AdminCA-CD-T01 – Not applicable; OCSP not provided. • CRL with critical CIDP Extension o Admin-Root-CA – No o AdminCA-CD-T01 - No