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 Bundesamt für Informatik und Telekommunikation (BIT) Federal Office of Information Technology and Telecommunica-tion (FOITT)
Website URL	www.bit.admin.ch
Organizational type	Government Agency
Primary market / customer base	Swiss 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.

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.

The root CA certificate URL	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	http://www.pki.admin.ch/crl/Admin-Root-CA.crl	http://www.pki.admin.ch/crl/AdminCA-CD-T01.crl Error Code:ffffe095 Comment #15: We have this critical extension Flag at "issuing distribution point" only in our CD-T CA. This will be corrected by the end of June, as this is not a necessary flag an can be omitted, by our guidelines.
CRL update frequency for end-entity certificates	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
List or description of subordinate CAs operated by the CA organization associated with the root CA.	Hierarchy Diagram: http://www.bit.admin.ch/adminpki/00247/index.html Admin-Root-CA issues the following 3 internally operated 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	Hierarchy Diagram: http://www.bit.admin.ch/adminpki/00247/index.html 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
subordinate CAs operated by third parties	None	None

List any other root CAs that have issued cross-signing certificates for this root CA	None	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Email No SSL Certificates chaining to this root.	Websites Email Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	IV The certs chaining up to this root are for digital signatures and encryption. Subscriber ID is confirmed according to section 3.2.3 of the CPS.	OV
EV policy OID	Not Applicable	Not Applicable
CP/CPS	English translation provided: https://bugzilla.mozilla.org/attachment.cgi?id=374130 Information Service: www.pki.admin.ch CP/CPS AdminPKI - ClassA (AdminCA-A-T01 sub-CA) http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf 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	AdminPKI – CP/CPS Class CD-T01 (English) https://bugzilla.mozilla.org/attachment.cgi?id=376403 New Version of CP/CPS Klasse CD-T01 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://bugzilla.mozilla.org/attachment.cgi?id=362013 2008.03.31 Next Surveillance Audit planned for second quarter 2009	

	Email confirmation of audit statement from Auditor: > From: Grubenmann, Reto <retogrubenmann@kpmg.com> > Subject: RE: Confirmation of Audit Statement for BIT > To: kathleen95014@yahoo.com > Date: Monday, March 2, 2009, 7:57 AM > Dear Mrs. Kathleen > I am the Swiss practice leader of the certification body of KPMG (Switzerland). > It is correct that the evidence based on the attachment (KPMG letter of the certification body) was issued by KPMG > (Zurich, Switzerland). BIT, our client has fullfilled all mandatory surveillance audits for the European and Swiss PKI standardization. > I confirm the authorization for this configuration. > Kind regards, > Reto Grubenmann

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - Admin-Root-CA – Not applicable
    - AdminCA-CD-T01
        - 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.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Admin-Root-CA
        - Section 4 of the CPS: Only the following people may apply for certs chaining up to this root. "Any employee of an administrative unit (federal, cantonal or municipal administration) that has signed a framework contract and concluded a Service Level Agreement with the Admin PKI may submit a certificate application (cf. 1.3.3). The personal details of the certificate applicant (last and first names, distinctive hash code, e-mail address) are published in the Admin-Directory."
        - The Registration Authority should also verify the authenticity of the application (by checking the application form and checking the data in the *Admin-Directory*).
    - AdminCA-CD-T01
        - CP/CPS section 4.1.1: 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 AdminPKI.
            - Note: This means that their (last and first names, distinctive hash code, e-mail address) are in the Admin-Directory.
        - 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.

- Verify identity info in code signing certs is that of subscriber
    - Admin-Root-CA – Not applicable
    - AdminCA-CD-T01
        - "Any employee of an administrative unit (federal, cantonal or municipal administration) that has signed a framework contract and concluded a Service Level Agreement with the Admin PKI may submit a certificate application (cf. 1.3.3). The personal details of the certificate applicant (last and first names, distinctive hash code, e-mail address) are published in the Admin-Directory."
        - CP/CPS section 3.2.3: 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
    - CP/CPS section 4.2.2: 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.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - Admin-Root-CA – Not applicable
    - 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
    - Admin-Root-CA – Not applicable
    - 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
    - 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
    - Admin-Root-CA – No. End entity certs are issued from the internally operated sub-CA.
    - 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.

- Allowing external entities to operate unconstrained subordinate CAs
  - Admin-Root-CA – The sub-CAs for this root are internally operated.
  - AdminCA-CD-T01 – This root has no subordinate CAs.
- Distributing generated private keys in PKCS#12 files
  - Admin-Root-CA – No.
  - 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
  - Admin-Root-CA – Not applicable
  - AdminCA-CD-T01 – Not found
- OCSP Responses signed by a certificate under a different root
  - Admin-Root-CA – Not applicable; OCSP not provided.
  - AdminCA-CD-T01 – Not applicable; OCSP not provided.
- CRL with critical CIDP Extension
  - Admin-Root-CA – No
  - AdminCA-CD-T01 – **Yes. Plan to remove by end of June.**

Verify Audits

(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Confirmed authenticity via email exchange with auditor at KPMG.
- For EV CA's, verify current WebTrust EV Audit done.
  - Not EV
- Review Audit to flag any issues noted in the report
  - No issues noted in auditor statement