

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 Telecommunication (FOITT)
Website URL (English version)	www.bit.admin.ch
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Government Agency
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	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 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.
The root CA certificate URL	http://www.bit.admin.ch/adminpki/00247/00792/index.html	http://www.bit.admin.ch/adminpki/00247/00796/index.html
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
CRL <ul style="list-style-type: none"> URL update frequency for end-entity certificates 	http://www.pki.admin.ch/crl/Admin-Root-CA.crl CPS sections 4.9.7 and 4.9.8: The secondary Certification Authority updates its CRL: <ul style="list-style-type: none"> 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. 	http://www.pki.admin.ch/crl/AdminCA-CD-T01.crl CPS sections 4.9.7 and 4.9.8: The Certification Authority updates its CRL: <ul style="list-style-type: none"> 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 -> Admin-CA3 -> Admin-CA2 AdminCA-A-T01 issues Class A certificates – HW (Token) – Personal Identification - Legally binding signature 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 Maschinen Certificates CodeSigning Certificates Class D – 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: <ul style="list-style-type: none"> Websites (SSL/TLS) Email (S/MIME) Code (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
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. <ul style="list-style-type: none"> For SSL certificates this should also include URLs of one or more web servers using the certificate(s). 	Need sample cert.	Need url to website whose cert chains up to this root.
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	English translation provided: https://bugzilla.mozilla.org/attachment.cgi?id=374131 Email from March 6: I will inform you as soon as we have the new version and all the responses to your questions!

	<p>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</p>	
<p>AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the “audit report and management assertions” document available from the webtrust.org site or elsewhere.)</p>	<p>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</p> <p>“Our company’s PKI Trust Centre was certified on July the 4th 2007 by KPMG SA Switzerland (Klynveld Peat Marwick Goerdeler SA).”</p> <p>From Audit Statement: Surveillance Audit 2008 completed 3/31/2008 Next Surveillance Audit planned for second quarter 2009</p> <p>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 fulfilled all mandatory surveillance > audits for the European and Swiss PKI standardization. > I confirm the authorization for this configuration. > Kind regards, > > Reto Grubenmann > KPMG AG</p>	

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
 - 4) --MetB: "I will check all these points with the SecOf an get back to you again asap"
 - METB: We ensure it with our internal processes: We need to have the delegation signature of the superior on a formulary witch confirms that the requester has been authorized.
- 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
 - METB: Same process: moreover: we enforce it by the issuing process, as the certificate is delivered to the mail address referenced in the certificate.
 - 4) --MetB: "I will check all these points with the SecOf an get back to you again asap"
I was not able to find the information in the AdminCA-CD-T01 CPS that satisfies section 7 of <http://www.mozilla.org/projects/security/certs/policy/>.
- Verify identity info in code signing certs is that of subscriber
 - Admin-Root-CA – Not applicable
 - AdminCA-CD-T01
 - METB: Yes, we ensure it and check it by our internal issuing process
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices

(http://wiki.mozilla.org/CA:Problematic_Practices)

- [1.1 Long-lived DV certificates](#)
 - Admin-Root-CA – Not applicable

- AdminCA-CD-T01 –
- [1.2 Wildcard DV SSL certificates](#)
 - Admin-Root-CA – Not applicable
 - AdminCA-CD-T01 –
 -
- [1.3 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 –
 -
- [1.4 Allowing external entities to operate unconstrained subordinate CAs](#)
 - Admin-Root-CA – The sub-CAs for this root are internally operated.
 - AdminCA-CD-T01 –
 -
- [1.5 Distributing generated private keys in PKCS#12 files](#)
 - Admin-Root-CA – No.
 - AdminCA-CD-T01 –
 -
- [1.6 Certificates referencing hostnames or private IP addresses](#)
 - Admin-Root-CA – Not applicable
 - AdminCA-CD-T01 –
 -
- [1.7 OCSP Responses signed by a certificate under a different root](#)
 - Admin-Root-CA –
 - AdminCA-CD-T01 –
 -
- [1.8 CRL with critical CIDP Extension](#)
 - Admin-Root-CA –
 - AdminCA-CD-T01 –
 -

Verify Audits (COMPLETE)

(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