Bugzilla ID: 453460
Bugzilla Summary: Add "SwissSign Gold CA - G2" as EV 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	SwissSign
Website URL (English version)	http://www.swisssign.com/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Public Corporation
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?)	SwissSign AG is a commercial CSP that provides certification services for individual and corporate customers. SwissSign operates the certificate authority for the Swiss Post and is mostly focused on Switzerland but Registration Services may be used internationally.

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

Info Needed	Data
Certificate Name	SwissSign Gold CA - G2
Cert summary / comments	This request is to EV-enable this root, which is already in the NSS store. This root has three internally-operated subordinate CAs: the SwissSign Personal Gold CA issues certificates for natural persons and organizations, the SwissSign Server Gold CA issues certificates for systems, and the SwissSign EV Gold CA issues EV certificates.
The root CA certificate URL	Already in NSS.
SHA-1 fingerprint.	d8:c5:38:8a:b7:30:1b:1b:6e:d4:7a:e6:45:25:3a:6f:9f:1a:27:61
Valid from	2006-10-25
Valid to	2036-10-25
Cert Version	3
Modulus length / key length	4096
CRL	http://crl.swisssign.net/0E414F33ED1FEE8DAF6A1916B706D286B253008A

• URL • update frequency for end-entity certificates	From CP/CPS: At least once every 24 hours. At most, 24 hours may pass from the time a certificate is revoked until the revocation is reported on the CRL.
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."	http://ocsp.swisssign.net/0E414F33ED1FEE8DAF6A1916B706D286B253008A From CP/CPS: Real-time. The OCSP responder will report a certificate revoked immediately after the revocation has been completed. Comment #8: => There is no expiration time for OCSP as this is done in Real-time. The OCSP responder will report a certificate revoked immediately after the revocation has been completed. (Refer to the CP/CPS attachments, section 4.9.7) => In the answer itself from the OCSP side the nextUpdate is set to thisUpdate + 25 hours
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	Hierarchy diagram provided in section 1.1. of the CPS. From CP/CPS: The "SwissSign Gold CA" is one of the certification authorities operated by SwissSign AG. The "SwissSign Gold CA" has three subordinate CAs: the "SwissSign Personal Gold CA", the "SwissSign Server Gold CA" and the "SwissSign EV Gold CA". The "SwissSign Personal Gold CA" issues certificates that support digital signing and/or encryption for individuals. The SwissSign Server Gold CA issues certificates for servers. The SwissSign EV Gold CA issues Extended Validation SSL certificates. For the issuance of Extended Validation SSL certificates, SwissSign fully complies with all the rules and regulations published by the CA/Browser Forum (http://www.cabforum.org/): The "SwissSign Personal Gold CA", the "SwissSign Server Gold CA" and the "SwissSign EV Gold CA" are issuing CAs for certificates that meet the stipulations of the European Technical Specification ETSI TS 102 042 - "Normalized" Certificate Policy (NCP).
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which	None This root CA may also operate other customer-specific Issuing CAs if and only if they fully comply with all the stipulations of the "Gold G2" CP/CPS.

those subordinates are authorized, controlled, and audited.	Comment #8: 3) Does this root have any sub-CAs that are operated by third parties? => No
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV, EV
EV policy OID	2.16.756.1.89.1.2.1.1
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.	https://testevg2.swisssign.net/
CP/CPS	CP/CPS: https://bugzilla.mozilla.org/attachment.cgi?id=360528 End User Agreement: http://repository.swisssign.com/SwissSign-Gold-EUA-R3.pdf SwissSign Document Repository http://repository.swisssign.com/
AUDIT	Audit Type: WebTrust for EV Auditor: KPMG Statement of completed point in time audit:

	https://bugzilla.mozilla.org/attachment.cgi?id=346440 October, 2008 Audit Type: ETSI TS 101.456 Auditor: KPMG Letter from KPMG confirming audit https://bugzilla.mozilla.org/attachment.cgi?id=336659 June, 2008 SwissSign is listed in the Directory of the certified bodies conform to the Bundesgesetz über die elektronische Signatur (ZertES): Swiss Accreditation Service Certified Bodies List, SAS details for SwissSign The criteria include ETSI TS 101.456 EV audit statement attached to bugzilla has been confirmed by KPMG via email. Friday, November 7, 2008.

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - In section 3.2.2 of the CP/CPS
- 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.
    - In section 3.2.3 of the CP/CPS.
- Verify identity info in code signing certs is that of subscriber
    - In section 3.2 of the CP/CPS
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)
Comment #8: "I looked at your comments in the Information Gathering Document and those are correct: no one is relevant for SwissSign"

- 1.1 Long-lived DV certificates
    - Not found
- 1.2 Wildcard DV SSL certificates
    - Not found
- 1.3 Issuing end entity certificates directly from roots
    - Root is offline, with subordinates to issue certs.

- 1.4 Allowing external entities to operate unconstrained subordinate CAs
  - No
- 1.5 Distributing generated private keys in PKCS#12 files
  - CPS Section 6.1.2 Private key delivery to subscriber
    Subscribers of the SwissSign RA have the choice, where the keys will be generated. SwissSign AG recommends to generate the keys for a signing certificate on a secure crypto device and the keys for an encryption certificate on the SwissSign web site. Private keys generated on a secure crypto device or browser-generated keys do not need to be delivered. **The delivery of private keys generated on the SwissSign web site will be delivered through a passphrase-protected download mechanism (PKCS#12).** Other RAs may manage the key generation and the delivery differently.
- 1.6 Certificates referencing hostnames or private IP addresses
  - Not found
- 1.7 OCSP Responses signed by a certificate under a different root
  - Not found
- 1.8 CRL with critical CIDP Extension
  - CRL download works

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.
  - Independent verification of authenticity of the audit report was completed.
- For EV CA's, verify current WebTrust EV Audit done.
  - Yes
- Review Audit to flag any issues noted in the report
  - No issues noted