Bugzilla ID: 759732
Bugzilla Summary: Add new Swisscom root certs to trusted root CA cert list

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Swisscom Solutions AG
Website URL	http://www.swissdigicert.ch
Organizational type	Swisscom AG is a commercial CSP that provides certification services for individual and corporate customers. Swisscom operates a certificate authority and registration authority. Customers may choose to use the registration services of Swisscom and purchase single certificates. Customers may also choose to operate their own registration authority (managed PKI).
Primark Market / Customer Base	Swisscom operates Issuing CA for national (Switzerland) and internatinal purpose. Swisscom AG focuses for national (Switzerland) and international purpose to provide managed PKI services. Registration Services may be used for national (Switzerland) and international purpose.
CA Contact Information	CA Email Alias: sdcs.spoc@swisscom.com CA Phone Number: 41 44 294 71 24 Title / Department: ICT Security Consulting

Technical information about each root certificate

Cert Name	Swisscom Root CA 2	Swisscom Root EV CA 2
Certificate Issuer Field	CN = Swisscom Root CA 2 OU = Digital Certificate Services O = Swisscom C = ch	CN = Swisscom Root EV CA 2 OU = Digital Certificate Services O = Swisscom C = ch
Cert Summary	This "Swisscom Root CA 2" root cert will eventually replace the "Swisscom Root CA 1" root cert that was included in NSS as per bug #342470.	This is a new EV cert with one internally-operated subCA.
Root Cert URL	http://aia.swissdigicert.ch/sdcs-root2.crt	http://www.swissdigicert.ch/download/sdcs-root2-ev.crt
SHA1	77:47:4F:C6:30:E4:0F:4C:47:64:3F:84:BA:B8:C6:95:4A:8A:41:EC	E7:A1:90:29:D3:D5:52:DC:0D:0F:C6:92:D3:EA:88:0D:15:2E:1A:6B
Valid From	2011-06-24	2011-06-24
Valid To	2031-06-25	2031-06-25
Cert Version	3	3
Signature Algo	PKCS #1 SHA-256 With RSA Encryption	PKCS #1 SHA-256 With RSA Encryption
Key length	4096	4096
Test Website	Please provide the url to a website with an SSL cert chaining up to this root.	Please provide the url to a website with an EV SSL cert chaining up to this root.

CRL URL	http://crl.swissdigicert.ch/sdcs-root2.crl http://crl.swissdigicert.ch/sdcs-diamant2.crl http://crl.swissdigicert.ch/sdcs-diamant2-suisseid.crl http://crl.swissdigicert.ch/sdcs-saphir2.crl http://crl.swissdigicert.ch/sdcs-saphir2-suisseid.crl http://crl.swissdigicert.ch/sdcs-rubin2.crl http://crl.swissdigicert.ch/sdcs-smaragd2.crl	http://www.swissdigicert.ch/download/sdcs-root2-ev.crl http://crl.swissdigicert.ch/sdcs-root2-ev.crl
OCSP URL	http://ocsp.swissdigicert.ch/sdcs-diamant2 http://ocsp.swissdigicert.ch/sdcs-diamant2-suisseid http://ocsp.swissdigicert.ch/sdcs-saphir2 http://ocsp.swissdigicert.ch/sdcs-saphir2-suisseid http://ocsp.swissdigicert.ch/sdcs-rubin2 http://ocsp.swissdigicert.ch/sdcs-smaragd2	http://ocsp.swissdigicert.ch/root2-ev http://ocsp.swissdigicert.ch/quartz2
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS)
SSL Validation Type	DV, OV	EV
EV Policy OID(s)	Not applicable	Need EV Policy OID

CA Hierarchy information for each root certificate

CA Hierarchy	The "Swisscom Root CA 2" currently has eight internally-operated subordinate CAs: - Swisscom Diamant CA 2 - Swisscom Diamant SuisseID CA 2 - Swisscom Sahir CA 2 - Swisscom Saphir SuisseID CA 2 - Swisscom Rubin CA 2 - Swisscom Smaragd CA 2 - Swisscom TSS CA 2 - Swisscom Customer Root CA 2	The "Swisscom Root EV CA 2" currently has one internally-operated subordinate CAs: - Swisscom Quarz EV CA 2
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	None
Cross-Signing	List all cross-signing relationships.	None
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	Not applicable

Verification Policies and Practices

Policy Documentation	Documents are in German and some older versions are available in English. Document Repository: http://www.swissdigicert.ch/sdcs/portal/page?node=download_docs CPS (German): http://www.swissdigicert.ch/sdcs/portal/open_pdf?file=deutsch%2F002_CPS_Swisscom_Digital_Certificate_Services_2_16_756_83_2_1_V2_1_de.pdf CPS (English): http://www.swissdigicert.ch/sdcs/portal/download_file?file=english%2F002_CPS_SDCS_2_16_756_83_2_1_V2_0_en.pdf CP: http://www.swissdigicert.ch/sdcs/portal/open_pdf?file=deutsch%2F007_CP_Smaragd_SDCS_2_16_756_1_83_3_V2_2_de.pdf There is a CP for each subCA, the documents are available on the Swisscom website. This CP is for the Emerald CA: For issuing Emerald-class user and device/server certificates. Certificate requests of this type are submitted to the RA as signed PKCS#10 requests. EV CPS: http://www.swissdigicert.ch/sdcs/portal/download_file?file=deutsch%2F102_CPS_SDCS_EV_2_16_756_1_83_2_2_V2_0_de.pdf EV CP: http://www.swissdigicert.ch/sdcs/portal/download_file?file=deutsch%2F008_CP_Quartz_EV_SDCS_2_16_756_1_83_4_V2_0_de.pdf
Audits	Audit Type: ETSI 101.456 Auditor: KPMG Auditor Website: www.kpmg.ch Audit Result: http://www.seco.admin.ch/sas/00229/00251/index.html?lang=en ZertES is granted by the Swiss Accreditation Service (SAS) and the Swiss Federal Office of Communications (BAKOM) based on an audit by KPMG. It is based on Swiss law and on ETSI standards for Qualified Certification Service Providers (CSP) and Time Stamping Authorities. It requires an annual audit. I see that this type of audit is for qualified certificates (electronic signatures). Where is the audit related to SSL certificates? Where is the EV audit statement?
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Organization Verification Procedures	CPS (English) section 3.1.1: Ruby/Emerald (Sec. e-mail / server / device) Required: • At least one person per organisation (field O= in DN) or domain (SSL server, e-mail) must be registered as in the case of Sapphire and guarantee that the details in the certificate are correct • For each domain entered in the certificate there must be one proxy of the legal person to which the domain refers

	Sapphire level verification requires proof of identity.
Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	See above.
Audit Criteria	?
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	?

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	?
Wildcard DV SSL certificates	?
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	CPS (English) section 1.3.2 Registration Authorities (RAs): The Swisscom (Schweiz) AG business model is based on a registration authorities (hereinafter RA) contractual partner model. Contractual partners of Swisscom (Schweiz) AG assume the role of RA. **The RA partner is free to choose whether to issue certificates within its organisation only or to also act as a "public" RA.** RA partners are obliged by the terms of a Service Level Agreement (SLA) to comply with the processes defined by Swisscom for the registration, issuance and revocation of certificates. If the RA

	partner also wishes to issue qualified certificates it is incorporated in the authorisation process by a certification authority accredited by the Swiss Accreditation Service (SAS). If the RA partner only issues advanced certificates, it is audited by Swisscom at least one a year. The Swisscom (Schweiz) AG business model differentiates the following types of RA: - Swisscom RA: For issuing certificates for own use and downstream RAs (E-RA) - E-RA: (Enterprise Registration Authority) is an RA partner authorised to create and issue SSCDs and certificates directly. Copyright Swisscom (Schweiz) AG Certification Practice Statement (CPS) of Swisscom Digital Certificate Services Version 1.3 12/62 - TPS: (Trusted Point of Sale) is an RA partner which, as a registration authority, receives and checks the details of certificate applications. SSCDs for the "Diamond" and "Sapphire" certificate classes are personalised and distributed by an E-RA or a central distribution point. A complete list of all public registration authorities is published on the web server referred to in section 2.2. The identity check of subscribers is performed by employees of the registration authorities. Who does the domain-name and email address verification? RAs? What sorts of checks are in place by SwissCom?
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	?
Distributing generated private keys in PKCS#12 files	Not for SSL certs. Email and code signing?
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	?
CRL with critical CIDP Extension	No. CRLs import into Firefox without error.
Generic names for CAs	CN includes CA name.
Lack of Communication With End Users	?