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	https://test-emerald-ca-2.pre.swissdigicert.ch	https://test-quarz-ev-ca-2.pre.swissdigicert.ch

		Please perform the EV testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Post a screen-shot in the bug when you have successfully done this.
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 http://crl.swissdigicert.ch/sdcs-quarz2-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	Swisscom Root EV CA 2 - EV Policy OID: 2.16.756.1.83.2.2 Swisscom Quarz EV CA 2 - EV Policy OID: 2.16.756.1.83.21.0 Which EV Policy OID do you want added to http://mxr.mozilla.org/mozilla-central/source/security/manager/ssl/src/nsIdentityChecking.cpp ?

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	None	None
Cross-Signing	None	None
Technical Constraints on Third-party Issuers	Comment #6: Contract between Swisscom (Schweiz) AG and the contract taking organisation, NDA and background check of RA officer of the contract taking organisation, workflow system for certificate issuance with personal accont based on strong authentication account (smart card), control and monitoring of the issuance activities, audit of the contract taking organisation and RA officer by internal and external audit.	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 Emerald 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. Ruby CP: http://www.swissdigicert.ch/sdcs/portal/open_pdf?file=deutsch%2F009_CP_Rubin_SDCS_2_16_756_1_83_4_V2_0_de.pdf 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_2_de.pdf
Baseline Requirements	What is your status in regards to complying with the CAB Forum Baseline Requirements? (https://www.cabforum.org/Baseline_Requirements_V1.pdf)
Audits	Audit Type: ETSI 101.456 Auditor: KPMG, www.kpmg.ch

	Audit Result: http://www.seco.admin.ch/sas/00229/00251/index.html?lang=en -- **This audit is for qualified certificates (electronic signatures).** 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. Where is the audit related to SSL certificates chaining up to the "Swisscom Root CA 2" root (e.g. non-EV SSL cert issuance)? WebTrust KPMG EV Cert Audit Cover Page https://bugzilla.mozilla.org/attachment.cgi?id=656885 There is a WebTrust seal audit cover page, so did you get a WebTrust seal? Is there a url on the webtrust.org website that has the audit report and management assertions?
Verification Levels	CPS (English) section 1 Associated with this document are the respective Certificate Policies (CP) of the certificate classes "Diamond" (qualified), "Sapphire" (advanced), "Ruby" and "Emerald", in addition to Time Stamp Services. The present CPS describes with two different CA generations. The first generation ends with CA 1 and uses SHA-1 as hashing algorithm. The second CA generation ends with CA 2 and uses SHA-256 as hashing algorithm. The numbering within a CA hierarchy is kept constant, this means all CA 1 issuing CAs are issued by Root CA 1 and all CA 2 issuing CAs are issued by Root CA 2. If not otherwise specified all specifications in this document refer to both CA generations. When the term "qualified" is used in connection with electronic signatures and certificates it means that a service provider meets the requirements of the Signatures Act (ZertES [1]), the Ordinance on Electronic Signatures (VZertES [2]) and the technical and administrative guidelines for certification services in the field of electronic signatures (TAV [3]). Compliance with these provisions is assessed by a certification authority accredited by the Swiss Accreditation Service (SAS). Accredited certificate service providers (hereinafter referred to as CSP) are authorised to offer certificates for the creation and verification of "qualified" electronic signatures. The qualified signature can also be used for verifying origin (authenticity) and protecting against unauthorised modifications (integrity). CPS section 1.3.1.2 The following Swisscom Digital Certificate Services certification authorities are operated downstream from the Root CA: **Diamond CA (qualified):** For issuing Diamond-class **user certificates**. Meets the requirements of ZertES. The certificate owner or subscriber uses a secure signature creation device (SSCD). The key is used for creating legally binding signatures. This level of certificate is only issued to natural persons, who nevertheless can represent legal entities. The certificate can only be used for signing purposes. **Diamond SuisseID CA (qualified):** For issuing Diamond-SuisseID-class **user certificates**. Meets the requirements of ZertES) and conforms the specification of SuisseID. The certificate owner or subscriber uses a secure signature creation device (SSCD). The key is used for creating legally binding signatures. This level of certificate is only issued to natural persons, who nevertheless can represent legal entities. The certificate can only be used for signing purposes.

	Sapphire CA (advanced): For issuing Sapphire-class user and **device/server certificates.** Conforms to the definitions set out in ZertES (article 2, clause B) for advanced certificates and EIDI-V [8] and uses a secure signature creation device (SSCD). This type of certificate is used for creating signatures in cases where there is no provision for documents in paper form or for purposes which have been agreed by the parties. This level of certificate is issued for natural persons and organisations and can be used for signing, encrypting and authenticating purposes. **Sapphire SuisseID CA (advanced):** For issuing Sapphire-SuisseID-class user and **device/server certificates**. Conforms to the definitions set out in ZertES (article 2, clause B) for advanced certificates and EIDI-V [8] and to the SuisseID specification. A secure signature creation device (SSCD) is used. This type of certificate is used for signatures in cases where there is no legal requirement for written form or for purposes which have been agreed by the parties. This level of certificate is issued for natural persons and legal entities and can be used for signing, encrypting and authenticating purposes. **Emerald CA:** For issuing Emerald-class user and **device/server certificates**. These are soft certificates and do not use a secure signature creation device (SSCD). Certificates from the Emerald CA are signed with a ValiCert Class 3 key by means of "RSA KEON ROOT SIGNING SERVICE" so that certificates issued from it are considered as "trusted" in the latest browsers and e-mail clients. Device certificates (SSL server/client) and certificates for e-mail security (sign and encrypt) are issued. **Ruby CA**: For issuing Ruby-class user and **device/server certificates**. These are soft certificates and do not use a secure signature creation device (SSCD). This level of certificate is issued for natural persons and organisations and can be used for signing, encrypting, authenticating, etc. **Customer CA:** For issuing digital CA certificates to create customer own Issuing CAs and to issue digital CA certificates to create a subordinate customer Root CA (). The private key to prepare a customer own Issuing CA is generated by SDCS through a HSM. The private key from the customer Root CA was generated and stored either in SSCD or in software. **TimeStamp CA:** For issuing certificates for the TimeStamp Service. Each TimeStamp Server has its own certificate. **Test CA:** For test purposes **E-RA-CA:** For issuing certificates for creating the SSL link between the Enterprise Registration Authority and the Trust Center. These certificates are only issued for E-RA officers and are bound to an SSCD. The certification authorities issue certificates for users, organisations and devices. No other certification authorities are certified.
External Registration Authorities	CPS 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.
Organization Verification Procedures	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.
SSL Verification Procedures	Under which levels can SSL certificates by issued? Where is this stated? Emerald (Smaragd) SubCA CP (Google Translations) – Please provide improved translation of these two sections. 3.2.3 Authentication of a person natürlichen For the Identitätsprüfung natürlichen a person or legal entity for which the applicant carries out a role for an advanced certificate following steps apply: First The applicant sends a certificate of one or more RA bestätigende his identity documents. Second An RA staff leads the Identitätsprüfung basis of the applicant's disposal for documents made and documented the process. Third For use with all certificate in the data processing system noted attributes must be made evidence. Grouted the requester available via one gültiges certificate, applying for additional allowances made for that person, even by one Übersendung verschlüsselten and signed application, provided that the identity of the person has not changed. 3.2.4 Überprüfung the domain name of the applicant Swisscom Digital Certificate Services überprüft the domain name of the applicant available via a Whois query. The applicant shall provide for the application for a certificate to submit a Bestätigungsschreiben, signed by the technical contact of the Whois statement or by authorized signatory of the company representatives ACCORDING of registration. A confirmation is valid period not exceeding two years.
EV SSL Verification Procedures	EV CP (Google Translation): 3.2.3 economic agents in the Commercial Register For companies that are listed in the Register, which is based on check the details of company registration, stating that the organization actually exists and which persons are authorized to sign for the organization. The document submitted must be certified and must not be older than one year. For obtaining an EV certificate, a company must be in the following countries listed in the Register: - Switzerland Not registered in Switzerland Things must teach documents which allow a similar identification of business entities.

	EV CP: (English Translation provided in section 10.1) 3.2.3 Economic Subject with excerpt from the commercial register Companies listed in the commercial register are checked based on the excerpt from the commercial register that the organization actually exists and which persons are authorized to sign for that organization. The document submitted must be certified and must not be older than one year. To obtain an EV certificate a company has to be in one of the following countries in the Commercial Register: · Switzerland Companies not registered in Switzerland must submit documentations that allow comparable identification of the company. EV CP (Google Translation): 3.2.8 check the details of the domain name of the applicant Swisscom Digital Certificate Services überprüft the domain name of the applicant available via a Whois query. Applicants must for Requesting an EV certificate submit a confirmation letter, signed by the technical contact of the Whois statement. Is the domain name of the applicant is not listed, but quite like the name of a known domain, created by the Anti-Phishing Workgroup name lists überprüft with potential phishing attack targets. There are only issued certificates, for which a legitimation or control exists - especially are no man-in-the-middle-issued certificates. EV CP (English Translation provided in Section 10.2) 3.2.8 Checking the domain name of the applicant Swisscom Digital Certificate Services checks the domain name of the applicant via a Whois query. The applicant must submit for an EV certificate request a written confirmation signed by the technical contact of the Whois statement. In case the domain name of the applicant is not listed, but looks similar to the name of a known domain then the name lists of potential phishing attack targets maintained by the Anti-Phishing Workgroup are tested.
Email Address Verification Procedures	EV CP (Google Translation) 3.2.9 check the details of the e-mail address of the applicant The applicant must demonstrate that he has access to the mailbox, and that he can use it to receive emails. According to my notes (see above), for the “Swisscom Root EV CA 2” root cert you are only requesting the websites trust bit. Is that correct? You are requesting the email trust bit for the “Swisscom Root CA 2” root cert, so I’ll need to see information in the related CP/CPS documentation about how it is proved that the certificate subscriber owns/controls the email address to be included in the certificate.
Code Signing Subscriber Verification Procedures	You are requesting the code signing trust bit for the “Swisscom Root CA 2” root cert, so I’ll need to see information in the related CP/CPS documentation about how authentication is done for the certificate subscriber for **Code Signing Certificates**.

Multi-factor Authentication	CPS section 5.2.3: The identification and authentication of roles is based on the role models described in the previous sections. Technical access to the individual IT systems is implemented using high-level authentication (SSCD) or user names and passwords. Cryptographic devices such as HSM and CA servers are subject to special authentication procedures. The password for "Admin" access to these components is split between the Root CA Administrator and the ISO. All access is based on the "4-eyes-principle". Physical access to the individual IT systems is regulated by access control mechanisms.
Network Security	CPS section 5.1, Infrastructural security controls

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	See above.
Document Handling of IDNs in CP/CPS	Do you allow the use of internationalize domain names (IDNs) in SSL (both non-EV and EV) certificates?
Revocation of Compromised Certificates	Yes
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	Yes
Domain owned by a Natural Person	SSL certs are issued to organizations.
OCSP	

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

Long-lived DV certificates	CPS section 6.3.2 Validity of certificates and key pairs • "Emerald" class CA certificates signed by RSA, up to 2 years • "Diamond", "Sapphire" and "Ruby" class certificates, up to three (3) years • "Emerald" class certificates, up to 1 year
Wildcard DV SSL certificates	N/A
Email Address Prefixes for DV Certs	N/A
Delegation of Domain / Email validation to third parties	**Yes. Enterprise RAs. – Which levels of verification (e.g. Diamond, Sapphire, etc.) can the E-RAs issue certs for? What types of certs can they issue?** 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. CPS section 5.2.1 Registrationauthority(RA) Although Digital Certificate Services outsources the registration of subscribers to an RA partner (ERA/TPS) it does operate its own RA for the registration of LRA Officers and internal Swisscom requirements. As a superordinate registration authority, the Swisscom RA is able to view all entries of the various E-RAs and if necessary can also revoke certificates issued by E-RAs. The Swisscom RA is operated by the RA Administrator. RAPartner(E-RA) Digital Certificate Services outsources the registration of subscribers to RA partners (E-RA). The E-RAs assume responsibility for the correct registration and vetting of the subscriber's personal identification details and attributes required for the creation and issuing of certificates, and the personalisation of secure signature creation device (SSCD). The RAs transfer this information to the Trust Center, where the certificate is issued. The RAs are responsible for the organisational structure and role concept. Basic roles (administrators, vettors, auditors) are filled at all RAs, although the composition of the roles may vary.
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	CPS section 4.12 Key escrow and recovery In accordance with ZertES, key escrow and key recovery is not permitted for qualified signature keys and is not supported by Swisscom Digital Certificate Services for signature keys. The same applies for "Sapphire" class certificates based on the regulatory requirements of EIDI-V.

	Swisscom Digital Certificate Services offers RA partners a procedure for generating encryption keys for the Ruby and Emerald certificate classes outside
Certificates referencing hostnames or private IP addresses	No
Issuing SSL Certificates for Internal Domains	No
OCSP Responses signed by a certificate under a different root	No
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	http://www.swissdigicert.ch/sdcs/contact/send