Print this page

Mozilla - CA Program

Case Information

Case Number	00000060	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	SwissSign AG	**Request Status**	Need Information from CA

Additional Case Information

Subject	Include SwissSign SHA2 root certificates	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1142323

General information about CA's associated organization

CA Email Alias 1	rootcert@swisssign.com		
CA Email Alias 2			
Company Website	http://www.swisssign.com/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Switzerland	**Verified?**	Verified
Primary Market / Customer Base	SwissSign operates an Issuing CA for the Swiss Post. SwissSign also provides managed PKI services. Registration Services may be used internationally.	**Verified?**	Verified
Impact to Mozilla Users	This request is to include the SHA-256 versions of the SHA-1 root certificates that were included via Bugzilla #343756.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Chapter 1.1 of CP/CPS 3) Audit Criteria: Yes 4) Document Handling of IDNs in CP/CPS: Chapter 3.1 of CP/CPS 5) Revocation of Compromised Certificates: Chapter 4.9 of CP/CPS 6) Verifying Domain Name Ownership: CP/CPS section 3.2.2 7) Verifying Email Address Control: CP/CPS section 3.2.3 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: Chapter 7.1.2 of CP/CPS 10) Domain owned by a Natural Person: Chapter 3.2.3 of CP/CPS 11) OCSP: Chapter 4.10 and 7.3 of CP/CPS 12) Network Security Controls: Chapter 6.7 and 8 of CP/CPS	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and

			clarifications noted in the text box below.
CA's Response to Problematic Practices	1) Long-lived DV certificates: the validity is 36 month max 2) Wildcard DV SSL certificates: Yes 3) Email Address Prefixes for DV Certs: No 4) Delegation of Domain / Email validation to third parties: No 5) Issuing end entity certificates directly from roots: No 6) Allowing external entities to operate subordinate CAs: No 7) Distributing generated private keys in PKCS#12 files: Yes, P12 is deleted after a defined time frame, when customer has downoaded the certificate 8) Certificates referencing hostnames or private IP addresses: No 9) Issuing SSL Certificates for Internal Domains: No 10) OCSP Responses signed by a certificate under a different root: No 11) SHA-1 Certificates: yes, only for certificates for individuals used für authentication 12) Generic names for CAs: No 13) Lack of Communication With End Users: No 14) Backdating the notBefore date: No	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	SwissSign Gold Root CA - G3	**Root Case No**	R00000076
Request Status	Need Information from CA	**Case Number**	00000060

Certificate Data

Certificate Issuer Common Name	SwissSign Gold Root CA - G3
O From Issuer Field	SwissSign AG
OU From Issuer Field	
Valid From	2009 Aug 04
Valid To	2037 Aug 04
Certificate Serial Number	00dec4f244f31da6fc
Subject	CN=SwissSign Gold Root CA - G3, OU=null, O=SwissSign AG, C=CH
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	0B:71:99:A1:C7:F3:AD:DF:7B:A7:EA:B8:EB:57:4A:E8:0D:60:DD:DE
SHA-256 Fingerprint	7A:F6:EA:9F:75:3A:1E:70:9B:D6:4D:0B:EB:86:7C:11:E8:C2:95:A5:6E:24:A6:E0:47:14:59:DC:CD:AA:15:58
Certificate Fingerprint	3C:E6:02:44:40:98:61:FC:70:06:5C:05:29:A2:4E:C5:01:85:4B:32:25:D6:59:63:59:42:67:25:E2:63:79:7C
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root will eventually replace the SHA-1 SwissSign Gold CA - G2 root that was included via Bugzilla Bug #343756.	**Verified?**	Verified
Root Certificate Download URL	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified
CRL URL(s)	ldap://directory.swisssign.net/CN=5C97064634ABDF30C57CC50D55716630B5608F9E%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint ldap://directory.swisssign.net/CN=70788578BC1AE745A2922EABFAE907CCA4DB181A%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint CP/CPS section 4.9.7: 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.	**Verified?**	Verified
OCSP URL(s)	http://gold-root-g3.ocsp.swisssign.net/5C97064634ABDF30C57CC50D55716630B5608F9E http://gold-ev-g3.ocsp.swisssign.net/70788578BC1AE745A2922EABFAE907CCA4DB181A CP/CPS section 4.9.7: Real-time. The OCSP responder will report a certificate's revocation immediately after the revocation has been completed.	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified

EV Policy OID(s)	2.16.756.1.89.1.2.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://ev-g3-valid-cert-demo.swisssign.net	**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	Tested. No errors.	**Verified?**	Verified
CA/Browser Forum Lint Test	CABlint Tested. No errors.	**Verified?**	Verified
Test Website Lint Test	Tested. No errors.	**Verified?**	Verified
EV Tested	// CN=SwissSign Gold Root CA - G3,O=SwissSign AG,C=CH "2.16.756.1.89.1.2.1.1", "SwissSign EV OID", SEC_OID_UNKNOWN, { 0x7A, 0xF6, 0xEA, 0x9F, 0x75, 0x3A, 0x1E, 0x70, 0x9B, 0xD6, 0x4D, 0x0B, 0xEB, 0x86, 0x7C, 0x11, 0xE8, 0xC2, 0x95, 0xA5, 0x6E, 0x24, 0xA6, 0xE0, 0x47, 0x14, 0x59, 0xDC, 0xCD, 0xAA, 0x15, 0x58 }, "MEoxCzAJBgNVBAYTAkNIMRUwEwYDVQQKEwxTd2lzc1NpZ24gQUcxJDAiBgNVBAMT" "G1N3aXNzU2lnbiBHb2xkIFJvb3QgQ0EgLSBHMw==", "AN7E8kTzHab8", Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1: 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.	**Verified?**	Verified
Externally Operated SubCAs	No - CA is operating In-House CAs.	**Verified?**	Verified
Cross Signing	No	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	External RAs are tecnical constrained CP/CPS section 1.3.2: Third parties may operate their own registration authority services, if these third parties abide by all the rules and regulations of this CP/CPS and the stipulations of standards (see chapter 1). Any RA operating under this CP/CPS must adhere to the following rules: - The RA must have a contractual agreement with SwissSign AG ... - The registration process of any other RA must be documented and presented to SwissSign AG. The other RA is only allowed to execute their registration process if SwissSign AG has audited and approved the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the SwissSign RA. - The RA must pass an annual audit.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Repository (History of Gold CA G2): https://www.swisssign.com/en/gold-cpcps	**Verified?**	Verified
CA Document Repository	http://swisssign.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	http://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf	**Verified?**	Verified
Other Relevant Documents	End User Agreement: http://repository.swisssign.com/SwissSign-Gold-EUA-R4.pdf	**Verified?**	Verified
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	https://home.kpmg.com/ch/de/home.html	**Verified?**	Verified
Auditor Qualifications	https://www.sas.admin.ch/sas/en/home/akkreditiertestellen/akkrstellensuchesas/pki.html Certification Body SCESm 071, KPMG AG Switzerland	**Verified?**	Verified
Standard Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	3/18/2016	**Verified?**	Verified
BR Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	3/18/2016	**Verified?**	Verified
EV Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
EV Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV Audit Statement Date	3/18/2016	**Verified?**	Verified
BR Commitment to Comply	CP/CPS section 1	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.1.1: The use of a FQDN requires authorization of the domain owner. ... The use of a FQDN may be authorized through domain validation if an organizational name is part of the subject. Domain validation must be obtained by one of the following methods: - The requester proves control of an administrative mail address in the domain. - The requester proves control of the DNS entry. - The requester proves control over the web server. CP/CPS section 3.2.2: The use of a domain name in an FQDN must be authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization must be given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual must personally sign the registration form. The RA will create a high-quality copy or scan of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to chapter 3.1.1 may be used to obtain authorization of the use of the domain name in an FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.	**Verified?**	Verified
EV SSL Verification Procedures	CP/CPS section 3.2.2: EV Certificates will only be issued in accordance with the EV Guidelines to the following types of organizations: - Private Organizations - Government Entities - Business Entities - Non-commercial Entities Any RA operating under this CP/CPS must implement a registration process that meets the requirements of the EV Guidelines and that authenticates the organization identity in accordance with these guidelines. section 4.2.1: Before issuing an EV certificate, SwissSign ensures that all subject organisation information in the EV certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended accomplish the following: - Verify the organization's existence and identity, including: -- Verify the organization's legal existence and identity (as established with an incorporating agency). -- Verify the organization's physical existence (business presence at a physical	**Verified?**	Verified

	address). -- Verify the organization's operational existence (business activity). -- Verify that the organization (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV certificate. -- Verify the requester's authorization for the EV certificate, including: -- Verify the name, title, and authority of the certificate requester. -- Verify that the certificate requester signed the registration form		
Organization Verification Procedures	CP/CPS section 3.2.2 - Authentication of organization identity section 3.2.3: Authentication of individual identity section 3.2.5: Validation of authority	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3: The /email= field must be verified during the registration process. The requester must prove that he has access to the mailbox and that he can use it to receive mail. CP/CPS section 4.4.1: Once the Certificate is issued by the CA, the subscriber receives an email with a link to download the certificate. If the subscriber utilize this link, then he has accepted the certificates.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit for root certificates.	**Verified?**	Not Applicable
Multi-Factor Authentication	It is implemented, all Operators have to log in with hardware token. BR #16.5: The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.	**Verified?**	Verified
Network Security	Chapter 6.7 and 8 of CP/CPS	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	SwissSign Silver Root CA - G3	**Root Case No**	R00000077
Request Status	Need Information from CA	**Case Number**	00000060

Certificate Data

Certificate Issuer Common Name	SwissSign Silver Root CA - G3
O From Issuer Field	SwissSign AG
OU From Issuer Field	
Valid From	2009 Aug 04
Valid To	2037 Aug 04
Certificate Serial Number	00aa88b05a0bb1769b
Subject	CN=SwissSign Silver Root CA - G3, OU=null, O=SwissSign AG, C=CH
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	8D:08:FC:43:C0:77:0C:A8:4F:4D:CC:B2:D4:1A:5D:95:6D:78:6D:C4
SHA-256 Fingerprint	1E:49:AC:5D:C6:9E:86:D0:56:5D:A2:C1:30:5C:41:93:30:B0:B7:81:BF:EC:50:E5:4A:1B:35:AF:7F:DD:D5:01
Certificate Fingerprint	63:C1:58:09:DB:A9:55:46:31:A9:B0:7A:53:86:59:EF:99:00:DB:8D:5A:5A:C5:29:A2:8E:90:FA:80:2C:CF:E3
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root will eventually replace the SHA-1 SwissSign Silver CA - G2 root that was included via Bugzilla Bug #343756.	**Verified?**	Verified
Root Certificate Download URL	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified
CRL URL(s)	http://crl.swisssign.net/5F1B8EC9BD340373BA8DFD25CE8CA5C9E3E60759	**Verified?**	Verified

	CP/CPS section 4.9.7: 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 URL(s)	http://silver-server-g3.ocsp.swisssign.net/5F1B8EC9BD340373BA8DFD25CE8CA5C9E3E60759 CP/CPS section 4.9.7: Real-time. The OCSP responder will report a certificate's revocation immediately after the revocation has been completed.	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://silver-g3-valid-cert-demo.swisssign.net	**Verified?**	Verified
Test Website - Expired	https://silver-g3-expired-cert-demo.swisssign.net		
Test Website - Revoked	https://silver-g3-revoked-cert-demo.swisssign.net		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	No Errors	**Verified?**	Verified
CA/Browser Forum Lint Test	No Erros	**Verified?**	Verified
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment for this root.	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1: The “SwissSign Silver CA” has two subordinate CAs: the “SwissSign Personal Silver CA” and the “SwissSign Server Silver CA”. The “SwissSign Personal Silver CA” issues certificates that support digital signing and/or encryption for individuals. The “SwissSign Server Silver CA” issues certificates for servers.	**Verified?**	Verified
Externally Operated SubCAs	No	**Verified?**	Verified
Cross Signing	No	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Repository (History of Silver CA G2): https://www.swisssign.com/en/silver-cpcps	**Verified?**	Verified
CA Document Repository	http://swisssign.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf	**Verified?**	Verified
Other Relevant	End User Agreement: https://www.swisssign.com/documents/SwissSign-Silver-EUA-	**Verified?**	Verified

Documents	R3.pdf		
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	https://home.kpmg.com/ch/de/home.html	**Verified?**	Verified
Auditor Qualifications	https://www.sas.admin.ch/sas/en/home/akkreditiertestellen/akkrstellensuchesas/pki.html Certification Body SCESm 071, KPMG AG Switzerland	**Verified?**	Verified
Standard Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	3/18/2016	**Verified?**	Verified
BR Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	3/18/2016	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CP/CPS section 1	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.1.1: The use of a FQDN requires authorization of the domain owner. ... The use of a FQDN may be authorized through domain validation if an organizational name is part of the subject. Domain validation must be obtained by one of the following methods: - The requester proves control of an administrative mail address in the domain. - The requester proves control of the DNS entry. - The requester proves control over the web server. CP/CPS section 3.2.2: SwissSign validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain (eg. webmaster@domain, postmaster@domain etc.). Additionally, the domain will only be accepted if a printout of the WHOIS entry for the domain is included. The owner of the domain must approve the request with a handwritten personal signature in the appropriate position on the registration form and provide information as to his identity. The RA will creat a high-quality copy or scan of all required supporting documentation.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment for this root.	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS section 3.2.2 - Authentication of organization identity section 3.2.3: Authentication of individual identity section 3.2.5: Validation of authority	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3: The /email= field must be verified during the registration process. The requester must prove that he has access to the mailbox and that he can use it to receive mail. CP/CPS section 4.4.1: Once the Certificate is issued by the CA, the subscriber receives an email with a link to download the certificate. If the subscriber utilize this link, then he has accepted the certificates.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit for root certificates.	**Verified?**	Not Applicable
Multi-Factor Authentication	It is implemented, all Operators have to log in with hardware token. BR #16.5: The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.	**Verified?**	Verified
Network Security	Chapter 6.7 and 8 of CP/CPS	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified

Root Case Record # 3

Root Case Information

Root Certificate Name	SwissSign Platinum Root CA - G3	**Root Case No**	R00000078
Request Status	Need Information from CA	**Case Number**	00000060

Certificate Data

Certificate Issuer Common Name	SwissSign Platinum Root CA - G3
O From Issuer Field	SwissSign AG
OU From Issuer Field	
Valid From	2009 Aug 04
Valid To	2037 Aug 04
Certificate Serial Number	223fa91720de8194
Subject	CN=SwissSign Platinum Root CA - G3, OU=null, O=SwissSign AG, C=CH
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	A1:E7:C6:00:AA:41:70:E5:B7:4B:C9:4F:9B:97:03:ED:C2:61:B4:B9
SHA-256 Fingerprint	59:B3:82:9F:1F:F4:43:34:49:58:FA:E8:BF:F6:21:B6:84:C8:48:CF:BF:7E:AD:6B:63:A6:CA:50:F2:79:4F:89
Certificate Fingerprint	07:08:C1:51:EB:A5:DA:61:12:A9:0C:E4:28:85:69:C7:DF:38:AC:4E:AB:99:76:74:DD:50:F0:A5:38:C7:BD:A3
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root will eventually replace the SHA-1 SwissSign Platinum CA - G2 root that was included via Bugzilla Bug #343756.	**Verified?**	Verified
Root Certificate Download URL	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified
CRL URL(s)	http://crl.swisssign.net/562A3F9058F4175A14B2D7081B855B546A541A28	**Verified?**	Verified
OCSP URL(s)	http://platinum-g3.ocsp.swisssign.net/562A3F9058F4175A14B2D7081B855B546A541A28	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	NEED: Please attach to the bug an example/test cert chaining up to this root.	**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	Not requesting Websites trust bit for this root.	**Verified?**	Not Applicable
CA/Browser Forum Lint Test		**Verified?**	Not Applicable
Test Website Lint Test		**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment for this root.	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1: The “SwissSign Platinum CA” has several subordinate CAs: the “SwissSign Qualified Platinum CA”, the “SwissSign Personal Platinum CA”, the “SwissSign SuisseID Platinum CA”, the “SwissSign Server Platinum CA” and the “Swiss Post Platinum CA”. The “SwissSign Qualified Platinum CA” issues qualified certificates that meet the stipulations of the Swiss Digital Signature Law and which may be distributed under different trade marks. The “SwissSign Personal Platinum CA” issues certificates that support digital signing and/or encryption for individuals and organizations. The “Swiss Post Platinum CA” issues certificates for distribution under the trade mark of the Swiss Post that support digital signing and/or encryption for individuals and organizations.	**Verified?**	Verified
Externally Operated SubCAs	No	**Verified?**	Verified
Cross Signing	No	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	In-House CP/CPS section 1.3.2: Third parties may operate their own registration authority services, if these third parties abide by all the rules and regulations of this CP/CPS, Swiss law and the stipulations of applicable standards (see chapter 1). Any RA operating under this CP/CPS must adhere to the following rules: - The RA must have a contractual agreement with SwissSign AG which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities. - The registration process must meet the stipulations of Swiss Digital Signature Law. It must be documented, published, and distributed to all parties involved in the RA process. - The RA must be certified according to Swiss Digital Signature Law and must pass an annual audit.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Repository (History of Platinum CA G2): https://www.swisssign.com/en/platinum-cpcps	**Verified?**	Verified
CA Document Repository	http://swisssign.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	**Verified?**	Verified
Other Relevant Documents	End User Agreement: http://repository.swisssign.com/SwissSign-Platinum-EUA-R4.pdf	**Verified?**	Verified
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	https://home.kpmg.com/ch/de/home.html	**Verified?**	Verified
Auditor Qualifications	https://www.sas.admin.ch/sas/en/home/akkreditiertestellen/akkrstellensuchesas/pki.html Certification Body SCESm 071, KPMG AG Switzerland	**Verified?**	Verified
Standard Audit	https://bug343756.bmoattachments.org/attachment.cgi?id=8781268	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified

Standard Audit Statement Date	3/18/2016	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Not requesting Websites trust bit for this root.	**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting Websites trust bit for this root.	**Verified?**	Not Applicable
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS section 3.2.2 - Authentication of organization identity section 3.2.3: Authentication of individual identity section 3.2.5: Validation of authority	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3: The /email= field must be verified during the registration process. The requester must prove that he has access to the mailbox and that he can use it to receive mail. section 4.3.2: The CA may: - email the certificate to the subscriber - email the certificate to the requesting RA - email information permitting the subscriber to download the certificate from a web site or repository - email information permitting the RA to download the certificate from a web site or repository section 4.4.1: Subscribers are not required to confirm the acceptance of the certificate. The registration authority ensures that certificate issuance will only take place when the subscriber is ready to download and install the certificate. This step is considered sufficient and no further confirmation is required.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit for root certificates.	**Verified?**	Not Applicable
Multi-Factor Authentication	all Operators have to log in with hardware token	**Verified?**	Verified
Network Security	Chapter 6.7 and 8 of CP/CPS	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://swisssign.net/cgi-bin/authority/download	**Verified?**	Verified