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**	Ready for Public Discussion

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	compliance@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 as Issuing CA for publicly trusted certificates, and 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

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices**	I have reviewed Mozilla's list of

		Statement	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	Reviewed and responded to. No concerns raised.	**Verified?**	Verified

Forbidden and 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	Reviewed and responded to. No concerns raised.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	SwissSign Gold Root CA - G3	**Root Case No**	R00000076
Request Status	Ready for Public Discussion	**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 ID	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 SHA-256 root will eventually replace the SHA-1 SwissSign Gold CA - G2 root that was included via Bugzilla Bug #343756. This request is to turn on the Websites and Email trust bits, and to enable EV treatment for this root.	**Verified?**	Verified
Root Certificate Download URL	http://swisssign.net/cgi-bin/authority/download /5C97064634ABDF30C57CC50D55716630B5608F9E	**Verified?**	Verified
CRL URL(s)	http://crl.swisssign.net /70788578BC1AE745A2922EABFAE907CCA4DB181A http://crl.swisssign.net /6DD68E20A622FDADCEE45AB3FCE154B7B1500CA7 CP/CPS section 4.9.7: At least once every 24 hours.	**Verified?**	Verified
OCSP URL(s)	http://gold-ev-g3.ocsp.swisssign.net /70788578BC1AE745A2922EABFAE907CCA4DB181A http://gold-server-g3.ocsp.swisssign.net /6DD68E20A622FDADCEE45AB3FCE154B7B1500CA7	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
Mozilla 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 - Valid	https://ev-g3-valid-cert-demo.swisssign.net/	**Verified?**	Verified
Test Website - Expired	https://ev-g3-expired-cert-demo.swisssign.net/		
Test Website - Revoked	https://ev-g3-revoked-cert-demo.swisssign.net/		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/ev-g3-valid-cert-demo.swisssign.net OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=2187&opt=cablint,zlint,x509lint&minNotBefore=2009-01-01 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1: The “SwissSign Gold CA” has three subordinate CAs: 1) SwissSign Personal Gold 2) SwissSign Server Gold 3) SwissSign EV Gold	**Verified?**	Verified
Externally Operated SubCAs	CPS section 1.3.1: The SwissSign Gold CA and its subsidiary CAs ...are the only public CAs operated by SwissSign AG that issue certificates under this CP/CPS. SwissSign may under this CP/CPS issue at any time additional subsidiary CAs for private or enterprise purposes.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	CPS section 1.3.2: Third parties may operate their own registration authority services... 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 au-thorization for their role as RA and clearly details the minimum requirements, processes and liabilities. • 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. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit may lead to the revocation of RA priv-ileges.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in German and English. https://www.swisssign.com/en/certifications	**Verified?**	Verified
CA Document Repository	https://www.swisssign.com/en/cp-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	http://repository.swisssign.com/RA_Delegation.pdf http://repository.swisssign.com/PDS.pdf http://repository.swisssign.com/SubscriberAgreement.pdf https://www.swisssign.com/en/ca-prod	**Verified?**	Verified
Auditor (New)	TÜViT - TÜV Informationstechnik GmbH	**Verified?**	Verified
Auditor Location (New)	Germany	**Verified?**	Verified

Standard Audit	https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/AA2017113002_Browser_Audit_Atesttation_s.pdf	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	11/30/2017	**Verified?**	Verified
BR Audit	https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/AA2017113002_Browser_Audit_Atesttation_s.pdf	**Verified?**	Verified
BR Audit Type	ETSI EN 319 411	**Verified?**	Verified
BR Audit Statement Date	11/30/2017	**Verified?**	Verified
EV SSL Audit	https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/AA2017113002_Browser_Audit_Atesttation_s.pdf	**Verified?**	Verified
EV SSL Audit Type	ETSI EN 319 411	**Verified?**	Verified
EV SSL Audit Statement Date	11/30/2017	**Verified?**	Verified
BR Commitment to Comply	CP/CPS section 1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8864741	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.2.2	**Verified?**	Verified
EV SSL Verification Procedures	CP/CPS sections 3.2.2, 4.2.1:	**Verified?**	Verified
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5.	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3	**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	CPS section 5.2.2.	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	SwissSign Silver Root CA - G3	**Root Case No**	R00000077

Request Status	Ready for Public Discussion	**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 ID	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 SHA-256 root will eventually replace the SHA-1 SwissSign Silver CA - G2 root that was included via Bugzilla Bug #343756. The request is to turn on the Websites and Email trust bits. Not requesting EV treatment for this root.	**Verified?**	Verified
Root Certificate Download URL	http://swisssign.net/cgi-bin/authority/download /A18C45930A12630BA7575F324A7DE121E7B73E66	**Verified?**	Verified
CRL URL(s)	http://crl.swisssign.net /5F1B8EC9BD340373BA8DFD25CE8CA5C9E3E60759 CP/CPS section 4.9.7: At least once every 24 hours.	**Verified?**	Verified
OCSP URL(s)	http://silver-server-g3.ocsp.swisssign.net /5F1B8EC9BD340373BA8DFD25CE8CA5C9E3E60759	**Verified?**	Verified

Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
Mozilla 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 - Valid	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		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/silver-g3-valid-cert-demo.swisssign.net OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=9964&opt=cablint,zlint,x509lint&minNotBefore=2009-01-01 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
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: “SwissSign Sliver Personal ” and “SwissSign Silver Server Silver".	**Verified?**	Verified
Externally Operated SubCAs	CP/CPS section 1.3.1: The SwissSign Silver CA and its subsidiary CAs (SwissSign	**Verified?**	Verified

	Personal Silver CA, SwissSign Server Silver CA) are the only CAs operated by SwissSign AG that issue certificates under this CP/CPS. SwissSign may under this CP/CPS issue at any time additional subsidiary CAs for private or enterprise purposes.		
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CP/CPS section 1.3.2: Third parties may operate their own registration authority services ... 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 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. All costs related to this audit are to be paid by the operator of this RA. Failure to pass the annual audit may lead to the revocation of RA privileges.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in German and English. https://www.swisssign.com/en/certifications	**Verified?**	Verified
CA Document Repository	https://www.swisssign.com/en/cp-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 Documents	http://repository.swisssign.com /RA_Delegation.pdf http://repository.swisssign.com/PDS.pdf http://repository.swisssign.com /SubscriberAgreement.pdf https://www.swisssign.com/en/ca-prod	**Verified?**	Verified
Auditor (New)	KPMG	**Verified?**	Verified
Auditor Location (New)	Switzerland	**Verified?**	Verified
Standard Audit	https://bug1142323.bmoattachments.org /attachment.cgi?id=8867948	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	3/22/2017	**Verified?**	Verified
BR Audit	https://bug1142323.bmoattachments.org /attachment.cgi?id=8867948	**Verified?**	Verified
BR Audit Type	ETSI EN 319 411	**Verified?**	Verified
BR Audit Statement Date	3/22/2017	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CP/CPS section 1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org /attachment.cgi?id=8864741	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.2.2	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment for this root.	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5.	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3	**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	CPS section 5.2.2.	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Root Case Record # 3

Root Case Information

Root Certificate Name	SwissSign Platinum Root CA - G3	**Root Case No**	R00000078
Request Status	Ready for Public Discussion	**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 ID	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 SHA-256 root will eventually replace the SHA-1 SwissSign Platinum CA - G2 root that was included via Bugzilla Bug #343756. The request is to turn on the Email trust bit for this root.	**Verified?**	Verified
Root Certificate Download URL	http://swisssign.net/cgi-bin/authority/download/562A3F9058F4175A14B2D7081B855B546A541A28	**Verified?**	Verified

CRL URL(s)	http://crl.swisssign.net /562A3F9058F4175A14B2D7081B855B546A541A28	**Verified?**	Verified
OCSP URL(s)	http://platinum-g3.ocsp.swisssign.net /562A3F9058F4175A14B2D7081B855B546A541A28	**Verified?**	Verified
Mozilla Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
Mozilla 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 - Valid		**Verified?**	Not Applicable
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes			

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: SwissSign Platinum G3 has the following subordinate CAs. 1) SwissSign Platinum Personal 2) SwissSign Platinum Qualified 3) SwissSign Platinum SuisseID 4) SwissSign Platinum Server 5) SwissSign Platinum TSA	**Verified?**	Verified

Externally Operated SubCAs	CPS section 1.3.1: SwissSign AG operates a Public Key Infrastructure, consisting of a “SwissSign Platinum CA” and its subordinated issuing CAs. The “SwissSign Platinum CA” and its subordinated issuing CAs are the only CAs operated by SwissSign AG that issue certificates under this CP/CPS.	**Verified?**	Verified
Cross Signing	No	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	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. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit may lead to the revocation of RA privileges.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are provided in German and English. https://www.swisssign.com/en/certifications	**Verified?**	Verified
CA Document Repository	https://www.swisssign.com/en/cp-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	http://repository.swisssign.com /RA_Delegation.pdf http://repository.swisssign.com/PDS.pdf http://repository.swisssign.com /SubscriberAgreement.pdf https://www.swisssign.com/en/ca-prod	**Verified?**	Verified
Auditor (New)	KPMG	**Verified?**	Verified
Auditor Location (New)	Switzerland	**Verified?**	Verified
Standard Audit	https://bug1142323.bmoattachments.org /attachment.cgi?id=8867948	**Verified?**	Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Verified
Standard Audit Statement Date	3/22/2017	**Verified?**	Not Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	N/A	**Verified?**	Not Applicable
BR Self Assessment	N/A	**Verified?**	Not Applicable
SSL Verification Procedures	N/A	**Verified?**	Not Applicable
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5.	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS section 3.2.3	**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	CPS section 5.2.2.	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified