

Mozilla - CA Program

Case Information

Case Number	00000081	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	SSL.com	Request Status	Ready for Public Discussion

Additional Case Information

Subject	Include SSLcom Root Certificates	Case Reason
----------------	----------------------------------	--------------------

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1277336
-----------------------------	---

General information about CA's associated organization

CA Email Alias 1	compliance@ssl.com		
CA Email Alias 2			
Company Website	https://www.ssl.com/	Verified?	Verified
Organizational Type	Commercial Organization	Verified?	Verified
Organizational Type (Others)		Verified?	Not Applicable
Geographic Focus	USA, Global	Verified?	Verified
Primary Market / Customer Base	<u>SSL.com</u> provides digital certificates in over 150 countries worldwide, with the goal of expanding adoption of encryption technologies and best practices through education, tools and expertise.	Verified?	Verified
Impact to Mozilla Users	see above	Verified?	Verified

Required and 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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: https://www.ssl.com/repository 2) CA Hierarchy: CP/CPS Section 1.3 3) Audit Criteria: section 8 4) Document Handling of IDNs in CP/CPS: section 3.1.3 5) Revocation of Compromised Certificates: section 4.9.1.1 6) Verifying Domain Name Ownership: section 3.2.2.4	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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: in section 6.3.2 2) Wildcard DV SSL certificates: in section 3.2.2.6 3) Email Address Prefixes for DV Certs: in section 3.2.2.4 method 4. 4) Delegation of Domain / Email validation to third parties: in section 1.3.2 5) Issuing end entity certificates directly from roots: limited usage of private key described in section 6.1.7 6) Allowing external entities to operate subordinate CAs: Not allowed. 7) Distributing generated private keys in PKCS#12 files: in section 6.1.2 8) Certificates referencing hostnames or private IP addresses: in section 3.1.1.1 9) Issuing SSL Certificates for Internal Domains: .int is a legitimate TLD and is treated as such. Refer to CP/CPS section 3.2.2.4. 10) OCSP Responses signed by a certificate under a different root: OCSP Responses use a certificate under the corresponding RootCA 11) SHA-1 Certificates: in section 6.1.5, SHA-1 certificates expire after 16th Jan 2017 12) Generic names for CAs: Yes, use generic name for CAs 13) Lack of Communication With End Users: in section 9.11 14) Backdating the notBefore date: no backdate certificates in order to avoid some deadline or code-enforced	Verified?	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	SSL.com Root Certification Authority RSA	Root Case No	R00000118
Request Status	Ready for Public Discussion	Case Number	00000081

Certificate Data

Certificate Issuer Common Name	SSL.com Root Certification Authority RSA
O From Issuer Field	SSL Corporation
OU From Issuer Field	
Valid From	2016 Feb 12
Valid To	2041 Feb 12

Certificate Serial Number	7b2c9bd316803299
Subject	CN= <u>SSL.com</u> Root Certification Authority RSA, OU=null, O=SSL Corporation, C=US
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	B7:AB:33:08:D1:EA:44:77:BA:14:80:12:5A:6F:BD:A9:36:49:0C:BB
SHA-256 Fingerprint	85:66:6A:56:2E:E0:BE:5C:E9:25:C1:D8:89:0A:6F:76:A8:7E:C1:6D:4D:7D:5F:29:EA:74:19:CF:20:12:3B:69
Certificate Fingerprint	D2:8E:CE:72:02:92:F9:E7:56:C0:FF:66:73:0E:D9:84:96:EC:E7:F2:FF:40:88:36:E8:F2:89:9A:DA:DE:2B:10
Certificate Version	3

Technical Information about Root Certificate			
Certificate Summary	This “ <u>SSL.com</u> Root Certification Authority RSA” will be used to produce end-entity Certificates using RSA signature algorithms for SSL (non-EV), S/MIME purposes as far as the Mozilla Root CA Program is concerned.	Verified?	Verified
Root Certificate Download URL	https://www.ssl.com/repository/SSLcomRootCertificationAuthorityRSA.cer	Verified?	Verified
CRL URL(s)	http://crls.ssl.com/ssl.com-rsa-RootCA.crl http://crls.ssl.com/SSLcomRSASSLsubCA.crl	Verified?	Verified
OCSP URL(s)	http://ocspssl.com	Verified?	Verified
Mozilla Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV	Verified?	Verified
Mozilla EV Policy OID(s)		Verified?	Not Applicable
Root Stores Included In		Verified?	Verified
Mozilla Applied Constraints	No	Verified?	Verified

Test Websites or Example Cert			
Test Website - Valid	https://test-ov-rsa.ssl.com	Verified?	Verified
Test Website - Expired	https://expired-rsa-dv.ssl.com		
Test Website - Revoked	https://revoked-rsa-dv.ssl.com		
Example Cert			
Test Notes	https://test-dv-rsa.ssl.com		

Test Results (When Requesting the SSL/TLS Trust Bit)			
Revocation Tested	no errors.	Verified?	Verified
CA/Browser Forum Lint Test	certificate not found	Verified?	Verified
Test Website Lint Test	Test not currently available	Verified?	Not Applicable

EV Tested NA

Verified? Not Applicable

CA Hierarchy Information

CA Hierarchy	"SSL.com Root Certification Authority RSA" currently has the following internally-operated intermediate CAs: - SSL.com RSA SSL subCA	Verified?	Verified
Externally Operated SubCAs	There are currently no externally operated subCAs issued from this Root. If we issue externally operated CAs, they will comply to Mozilla's Root CA Program and be either technically constrained or publicly disclosed and audited.	Verified?	Verified
Cross Signing	This Root has not been cross-signed by any other CAs.	Verified?	Verified
Technical Constraint on 3rd party Issuer	in CP/CPS section 7.1.5	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document Repository	<ul style="list-style-type: none"> https://www.ssl.com/repository/ https://www.ssl.com/relying-party-agreement/ https://www.ssl.com/terms-of-use/ 	Verified?	Verified
CP Doc Language	English		
CP	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
Other Relevant Documents		Verified?	Not Applicable
Auditor Name	BDO	Verified?	Verified
Auditor Website	https://www.bdo.com/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	Verified?	Verified
Standard Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTCA-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	7/27/2017	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTBR-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/27/2017	Verified?	Verified
EV Audit	NA	Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit		Verified?	Not

Statement Date			Applicable
BR Commitment to Comply	in CP/CPS section 1.1.2	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8881939	Verified?	Verified
SSL Verification Procedures	in CP/CPS section 3.2.2.1, 3.2.2.2, 3.2.2.3 and 3.2.2.4	Verified?	Verified
EV SSL Verification Procedures	NA	Verified?	Not Applicable
Organization Verification Procedures	in CP/CPS section 3.2.2	Verified?	Verified
Email Address Verification Procedures	in CP/CPS section 3.2.2.8	Verified?	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	SSL.com uses multi-factor authentication for the issuance of SSL certificates and for managing the RA and CA engines	Verified?	Verified
Network Security	SSL.com confirms that the actions listed in #7 of the https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices have been	Verified?	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	SSL.com Root Certification Authority ECC	Root Case No	R00000120
Request Status	Ready for Public Discussion	Case Number	00000081

Certificate Data

Certificate Issuer Common Name	SSL.com Root Certification Authority ECC
O From Issuer Field	SSL Corporation
OU From Issuer Field	
Valid From	2016 Feb 12
Valid To	2041 Feb 12
Certificate Serial Number	75e6dfcbc1685ba8
Subject	CN= SSL.com Root Certification Authority ECC, OU=null, O=SSL Corporation, C=US
Signature Hash Algorithm	ecdsaWithSHA256
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	C3:19:7C:39:24:E6:54:AF:1B:C4:AB:20:95:7A:E2:C3:0E:13:02:6A
SHA-256 Fingerprint	34:17:BB:06:CC:60:07:DA:1B:96:1C:92:0B:8A:B4:CE:3F:AD:82:0E:4A:A3:0B:9A:CB:C4:A7:4E:BD:CE:BC:65
Certificate Fingerprint	ED:F7:70:3B:AE:9B:C0:A4:20:10:AB:9E:F4:A9:2E:88:B4:4F:F3:7F:1E:68:10:AE:1E:61:0A:AB:EC:B5:01:F3

Certificate Version	3
---------------------	---

Technical Information about Root Certificate			
Certificate Summary	The SSL.com Root Certification Authority ECC will be used to produce end-entity Certificates using ECDSA signature algorithms for SSL (non-EV), S/MIME purposes.	Verified?	Verified
Root Certificate Download URL	https://www.ssl.com/repository/SSLcomRootCertificationAuthorityECC.cer	Verified?	Verified
CRL URL(s)	http://crls.ssl.com/ssl.com-ecc-RootCA.crl	Verified?	Verified
OCSP URL(s)	http://ocspssl.com	Verified?	Verified
Mozilla Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV	Verified?	Verified
Mozilla EV Policy OID(s)		Verified?	Not Applicable
Root Stores Included In		Verified?	Verified
Mozilla Applied Constraints	No	Verified?	Verified

Test Websites or Example Cert			
Test Website - Valid	https://test-ov-ecc.ssl.com	Verified?	Verified
Test Website - Expired	https://expired-ecc-dv.ssl.com		
Test Website - Revoked	https://revoked-ecc-dv.ssl.com		
Example Cert			
Test Notes	https://test-dv-ecc.ssl.com		

Test Results (When Requesting the SSL/TLS Trust Bit)			
Revocation Tested	no errors.	Verified?	Verified
CA/Browser Forum Lint Test	certificate not found	Verified?	Verified
Test Website Lint Test	Test not currently available	Verified?	Not Applicable
EV Tested	NA	Verified?	Not Applicable

CA Hierarchy Information			
CA Hierarchy	" SSL.com Root Certification Authority ECC" currently has the following internally-operated intermediate CAs: - SSL.com ECC SSL subCA	Verified?	Verified
Externally Operated SubCAs	There are currently no externally operated subCAs issued from this Root. If we issue externally operated CAs, they will comply to Mozilla's Root CA Program and be either technically	Verified?	Verified

constrained or publicly disclosed and audited.

Cross Signing	This Root has not been cross-signed by any other CAs.	Verified?	Verified
Technical Constraint on 3rd party Issuer	in CP/CPS section 7.1.5	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document Repository	<ul style="list-style-type: none"> https://www.ssl.com/repository/ https://www.ssl.com/relying-party-agreement/ https://www.ssl.com/terms-of-use/ 	Verified?	Verified
CP Doc Language	English		
CP	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
Other Relevant Documents		Verified?	Not Applicable
Auditor Name	BDO	Verified?	Verified
Auditor Website	https://www.bdo.com/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	Verified?	Verified
Standard Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTCA-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	7/27/2017	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTBR-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/27/2017	Verified?	Verified
EV Audit	NA	Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply	in CP/CPS section 1.1.2	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8881939	Verified?	Verified
SSL Verification Procedures	in CP/CPS section 3.2.2.1, 3.2.2.2, 3.2.2.3 and 3.2.2.4	Verified?	Verified
EV SSL Verification Procedures	NA	Verified?	Not Applicable
Organization	in CP/CPS section 3.2.2	Verified?	Verified

Verification Procedures			
Email Address Verification Procedures	in CP/CPS section 3.2.2.8	Verified?	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	SSL.com uses multi-factor authentication for the issuance of SSL certificates and for managing the RA and CA engines	Verified?	Verified
Network Security	SSL.com confirms that the actions listed in #7 of the https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices have been	Verified?	Verified

Root Case Record # 3

Root Case Information			
Root Certificate Name	SSL.com EV Root Certification Authority RSA	Root Case No	R00000121
Request Status	Ready for Public Discussion	Case Number	00000081

Certificate Data	
Certificate Issuer Common Name	SSL.com EV Root Certification Authority RSA
O From Issuer Field	SSL Corporation
OU From Issuer Field	
Valid From	2016 Feb 12
Valid To	2041 Feb 12
Certificate Serial Number	1d6c11eb6fda399d
Subject	CN= SSL.com EV Root Certification Authority RSA, OU=null, O=SSL Corporation, C=US
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	1C:B7:ED:E1:76:BC:DF:EF:0C:86:6F:46:FB:F9:80:E9:01:E5:CE:35
SHA-256 Fingerprint	5A:DF:A2:50:13:BE:D3:71:08:31:57:2D:E5:1C:4B:9A:21:17:1C:00:31:32:49:C4:CB:47:19:D3:7F:BB:8D:20
Certificate Fingerprint	0D:DA:8B:3C:6D:FC:89:A3:7F:1D:33:80:C3:8B:FC:6C:DF:B7:78:3A:40:F0:1B:91:B6:6F:DB:E9:57:9D:5D:BD
Certificate Version	3

Technical Information about Root Certificate			
Certificate Summary	This " SSL.com Root Certification Authority RSA" will be used to produce end-entity Certificates using RSA signature algorithms for SSL (EV), S/MIME purposes as far as the Mozilla Root CA Program is concerned.	Verified?	Verified
Root Certificate Download URL	http://www.ssl.com/repository/SSLcomEVRootCertificationAuthorityRSA.cer	Verified?	Verified
CRL URL(s)	URL: http://crls.ssl.com/ssl.com-EVrsa-RootCA.crl	Verified?	Verified

OCSP URL(s)	http://ocsp.ssl.com	Verified?	Verified
Mozilla Trust Bits	Websites	Verified?	Verified
SSL Validation Type	EV	Verified?	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	Verified?	Verified
Root Stores Included In		Verified?	Verified
Mozilla Applied Constraints	No	Verified?	Verified

Test Websites or Example Cert

Test Website - Valid	https://test-ev-rsa.ssl.com	Verified?	Verified
Test Website - Expired	https://expired-ev-rsa.ssl.com		
Test Website - Revoked	https://revoked-ev-rsa.ssl.com		
Example Cert			
Test Notes	https://test-dv-rsa.ssl.com		

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

Revocation Tested	no errors.	Verified?	Verified
CA/Browser Forum Lint Test	certificate not found	Verified?	Verified
Test Website Lint Test	Test not currently available	Verified?	Not Applicable
EV Tested	Test tool under maintenance.	Verified?	Not Applicable

CA Hierarchy Information

CA Hierarchy	" SSL.com Root Certification Authority RSA" currently has the following internally-operated intermediate CAs: - SSL.com RSA SSL subCA	Verified?	Verified
Externally Operated SubCAs	There are currently no externally operated subCAs issued from this Root. If we issue externally operated CAs, they will comply to Mozilla's Root CA Program and be either technically constrained or publicly disclosed and audited.	Verified?	Verified
Cross Signing	This Root has not been cross-signed by any other CAs.	Verified?	Verified
Technical Constraint on 3rd party Issuer	in CP/CPS section 7.1.5	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document	• https://www.ssl.com/repository/	Verified?	Verified

Repository	<ul style="list-style-type: none"> • https://www.ssl.com/relying-party-agreement/ • https://www.ssl.com/terms-of-use/ 		
CP Doc Language	English		
CP	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
Other Relevant Documents		Verified?	Not Applicable
Auditor Name	BDO	Verified?	Verified
Auditor Website	https://www.bdo.com/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	Verified?	Verified
Standard Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTCA-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	7/27/2017	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTBR-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/27/2017	Verified?	Verified
EV Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WT-SSL-EV-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
EV Audit Type	WebTrust	Verified?	Verified
EV Audit Statement Date	7/27/2017	Verified?	Verified
BR Commitment to Comply	in CP/CPS section 1.1.2	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8881939	Verified?	Verified
SSL Verification Procedures	in CP/CPS section 3.2.2.1, 3.2.2.2, 3.2.2.3 and 3.2.2.4	Verified?	Verified
EV SSL Verification Procedures	In CP/CPS section 3.2	Verified?	Verified
Organization Verification Procedures	in CP/CPS section 3.2.2	Verified?	Verified
Email Address Verification Procedures	in CP/CPS section 3.2.2.8	Verified?	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	SSL.com uses multi-factor authentication for the issuance of SSL certificates and for managing the RA and CA engines	Verified?	Verified
Network Security	SSL.com confirms that the actions listed in #7 of the https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices have been	Verified?	Verified

Root Case Record # 4

Root Case Information			
Root Certificate Name	SSL.com EV Root Certification Authority ECC	Root Case No	R00000122
Request Status	Ready for Public Discussion	Case Number	00000081

Certificate Data	
Certificate Issuer Common Name	SSL.com EV Root Certification Authority ECC
O From Issuer Field	SSL Corporation
OU From Issuer Field	
Valid From	2016 Feb 12
Valid To	2041 Feb 12
Certificate Serial Number	2c299c5b16ed0595
Subject	CN= SSL.com EV Root Certification Authority ECC, OU=null, O=SSL Corporation, C=US
Signature Hash Algorithm	ecdsaWithSHA256
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	4C:DD:51:A3:D1:F5:20:32:14:B0:C6:C5:32:23:03:91:C7:46:42:6D
SHA-256 Fingerprint	22:A2:C1:F7:BD:ED:70:4C:C1:E7:01:B5:F4:08:C3:10:88:0F:E9:56:B5:DE:2A:4A:44:F9:9C:87:3A:25:A7:C8
Certificate Fingerprint	87:33:B4:5A:BC:04:58:A8:C5:49:F5:43:58:0C:96:AD:19:8C:A0:ED:99:05:65:11:55:86:85:22:0D:49:BA:8C
Certificate Version	3

Technical Information about Root Certificate			
Certificate Summary	The SSL.com EV Root Certification Authority ECC will be used to produce end-entity Certificates using ECDSA signature algorithms for SSL (EV) purposes.	Verified?	Verified
Root Certificate Download URL	www.ssl.com/repository/SSLcomEVRootCertificationAuthorityECC.cer	Verified?	Verified
CRL URL(s)	http://crls.ssl.com/ssl.com-EVecc-RootCA.crl	Verified?	Verified
OCSP URL(s)	http://ocspssl.com	Verified?	Verified
Mozilla Trust Bits	Websites	Verified?	Verified
SSL Validation Type	EV	Verified?	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	Verified?	Verified
Root Stores Included In		Verified?	Verified
Mozilla Applied Constraints	No	Verified?	Verified

Test Websites or Example Cert

Test Website - Valid	https://test-ev-ecc.ssl.com/	Verified?	Verified
Test Website - Expired	https://expired-ecc-ev.ssl.com		
Test Website - Revoked	https://revoked-ecc-ev.ssl.com		
Example Cert			
Test Notes	https://test-dv-rsa.ssl.com		

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

Revocation Tested	no errors.	Verified?	Verified
CA/Browser Forum Lint Test	certificate not found	Verified?	Verified
Test Website Lint Test	Test not currently available	Verified?	Not Applicable
EV Tested	Test tool under maintenance.	Verified?	Not Applicable

CA Hierarchy Information

CA Hierarchy	“ SSL.com Root Certification Authority RSA” currently has the following internally-operated intermediate CAs: - SSL.com RSA SSL subCA	Verified?	Verified
Externally Operated SubCAs	There are currently no externally operated subCAs issued from this Root. If we issue externally operated CAs, they will comply to Mozilla's Root CA Program and be either technically constrained or publicly disclosed and audited.	Verified?	Verified
Cross Signing	This Root has not been cross-signed by any other CAs.	Verified?	Verified
Technical Constraint on 3rd party Issuer	in CP/CPS section 7.1.5	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document Repository	<ul style="list-style-type: none"> https://www.ssl.com/repository/ https://www.ssl.com/relying-party-agreement/ https://www.ssl.com/terms-of-use/ 	Verified?	Verified
CP Doc Language	English		
CP	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2017/06/SSLcom_CP_CPS_Version_1_2_1.pdf	Verified?	Verified
Other Relevant Documents		Verified?	Not Applicable
Auditor Name	BDO	Verified?	Verified
Auditor Website	https://www.bdo.com/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	Verified?	Verified

Standard Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTCA-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	7/27/2017	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WTBR-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/27/2017	Verified?	Verified
EV Audit	https://www.ssl.com/app/uploads/2017/07/SSL-COM-WT-SSL-EV-Indp-Accountant-Report-and-Mgmt-Assertion-FINAL-2017.pdf	Verified?	Verified
EV Audit Type	WebTrust	Verified?	Verified
EV Audit Statement Date	7/27/2017	Verified?	Verified
BR Commitment to Comply	in CP/CPS section 1.1.2	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8881939	Verified?	Verified
SSL Verification Procedures	in CP/CPS section 3.2.2.1, 3.2.2.2, 3.2.2.3 and 3.2.2.4	Verified?	Verified
EV SSL Verification Procedures	In CP/CPS section 3.2	Verified?	Verified
Organization Verification Procedures	in CP/CPS section 3.2.2	Verified?	Verified
Email Address Verification Procedures	in CP/CPS section 3.2.2.8	Verified?	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	SSL.com uses multi-factor authentication for the issuance of SSL certificates and for managing the RA and CA engines	Verified?	Verified
Network Security	SSL.com confirms that the actions listed in #7 of the https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices have been	Verified?	Verified