Print this page

Mozilla - CA Program

Case Information

Case Number	00000081	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	SSL.com	Request Status	Need Information from CA

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	SSL.com 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

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	NEED CA's response to each of the items listed in https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	Verified?	Verified

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
7) Verifying Email Address Control: section 3.2.2.8
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: section 7.1.4.2.1
10) Domain owned by a Natural Person: section 7.1.4.2 and 3.2.3
11) OCSP: sections 2.2.2.2, 4.9.9, 4.9.10
12) Network Security Controls: section 6.7

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	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	Initial Request Received	Case Number	00000081

Additional Root Case Information

Subject	

Technical Information about Root Certificate

O From Issuer Field	SSL Corporation	Verified?	Verified
OU From Issuer Field		Verified?	Not Applicable
Certificate Summary	This “SSL.com 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
Valid From	2016 Feb 12	Verified?	Verified
Valid To	2041 Feb 12	Verified?	Verified
Certificate Version	3	Verified?	Verified
Certificate Signature Algorithm	SHA-256	Verified?	Verified
Signing Key Parameters	4096	Verified?	Verified
Test Website URL (SSL) or Example Cert	https://test-ov-rsa.ssl.com https://test-dv-rsa.ssl.com	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://ocsps.ssl.com	Verified?	Verified
Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV	Verified?	Verified
EV Policy OID(s)		Verified?	Not Applicable
Root Stores Included In		Verified?	Need Response From CA
Mozilla Applied Constraints	No	Verified?	Verified

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	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. Test tool under maintenance.	Verified?	Not Verified
EV Tested	NA	Verified?	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	b7:ab:33:08:d1:ea:44:77:ba:14:80:12:5a:6f:bd:a9:36:49:0c:bb	Verified?	Verified
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	Verified?	Verified

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	• 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/2016/07/SSLcom_CP_CPS_Version_1_0.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2016/07/SSLcom_CP_CPS_Version_1_0.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/2014/06/SSL-2-12-16-RKGC-Ind-Auditor-Report.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	2/12/2016	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2016/07/SSL-COM-SSL-Baseline-Acct-Report-and-Mgmt-Assertion-FINAL-7-15-16.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/20/2016	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
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

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of	Verified?	Need Response From CA

Mozilla's CA Certificate Inclusion Policy.

Root Case Record # 2

Root Case Information

Root Certificate Name	SSL.com Root Certification Authority ECC	**Root Case No**	R00000120
Request Status	Initial Request Received	**Case Number**	00000081

Additional Root Case Information

Subject	

Technical Information about Root Certificate

O From Issuer Field	SSL Corporation	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Not Applicable
Certificate Summary	This “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 as far as the Mozilla Root CA Program is concerned.	**Verified?**	Verified
Root Certificate Download URL	https://www.ssl.com/repository /SSLcomRootCertificationAuthorityECC.cer	**Verified?**	Verified
Valid From	2016 Feb 12	**Verified?**	Verified
Valid To	2041 Feb 12	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://test-ov-ecc.ssl.com https://test-dv-ecc.ssl.com	**Verified?**	Verified
CRL URL(s)	http://crls.ssl.com/ssl.com-ecc-RootCA.crl http://crls.ssl.com /SSLcomECCSSLsubCA.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsps.ssl.com	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores Included In		**Verified?**	Need Response From CA

Mozilla Applied Constraints	No	**Verified?**	Verified

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	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. test tool under maintenance	**Verified?**	Not Verified
EV Tested	NA	**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	c3:19:7c:39:24:e6:54:af:1b:c4:ab:20:95:7a:e2:c3:0e:13:02:6a	**Verified?**	Verified
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	**Verified?**	Verified

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 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	• 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/2016/07/SSLcom_CP_CPS_Version_1_0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2016/07/SSLcom_CP_CPS_Version_1_0.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/2014/06/SSL-2-12-16-RKGC-Ind-Auditor-Report.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/12/2016	**Verified?**	Verified
BR Audit	https://www.ssl.com/app/uploads/2016/07/SSL-COM-SSL-Baseline-Acct-Report-and-Mgmt-Assertion-FINAL-7-15-16.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	7/20/2016	**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
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

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA

Root Case Record # 3

Root Case Information

Root Certificate Name	SSL.com EV Root Certification Authority RSA	**Root Case No**	R00000121
Request Status	Initial Request Received	**Case Number**	00000081

Additional Root Case Information

Subject	

Technical Information about Root Certificate

O From Issuer Field	SSL Corporation	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Not Applicable
Certificate Summary	This “SSL.com 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
Valid From	2016 Feb 12	**Verified?**	Verified
Valid To	2041 Feb 12	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://test-ov-rsa.ssl.com https://test-dv-rsa.ssl.com	**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://ocsps.ssl.com	**Verified?**	Verified

Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	No	**Verified?**	Verified

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	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. test tool under maintenance	**Verified?**	Not Verified
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described herehttps://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Test tool under maintenance.	**Verified?**	Not Verified

Digital Fingerprint Information

SHA-1 Fingerprint	b7:ab:33:08:d1:ea:44:77:ba:14:80:12:5a:6f:bd:a9:36:49:0c:bb	**Verified?**	Verified
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	**Verified?**	Verified

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	• 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/2016/07/SSLcom_CP_CPS_Version_1_0.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2016/07/SSLcom_CP_CPS_Version_1_0.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/2014/06/SSL-2-12-16-RKGC-Ind-Auditor-Report.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	2/12/2016	Verified?	Verified
BR Audit	https://www.ssl.com/app/uploads/2016/07/SSL-COM-SSL-Baseline-Acct-Report-and-Mgmt-Assertion-FINAL-7-15-16.pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	7/20/2016	Verified?	Verified
EV Audit	BDO	Verified?	Verified
EV Audit Type	WebTrust	Verified?	Verified
EV Audit Statement Date	7/20/2016	Verified?	Verified
BR Commitment to Comply	in CP/CPS section 1.1.2	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

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA

Root Case Record # 4

Root Case Information

Root Certificate Name	SSL.com EV Root Certification Authority ECC	**Root Case No**	R00000122
Request Status	Initial Request Received	**Case Number**	00000081

Additional Root Case Information

Subject	

Technical Information about Root Certificate

O From Issuer Field	SSL Corporation	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Not Applicable
Certificate Summary	This “SSL.com EV Root Certification Authority RSA” will be used to produce end-entity Certificates using RSA signature algorithms for SSL (EV) 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
Valid From	2016 Feb 12	**Verified?**	Verified
Valid To	2041 Feb 12	**Verified?**	Verified

Certificate Version	3	Verified?	Verified
Certificate Signature Algorithm	SHA-256	Verified?	Verified
Signing Key Parameters	4096	Verified?	Verified
Test Website URL (SSL) or Example Cert	https://test-ov-rsa.ssl.com https://test-dv-rsa.ssl.com	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://ocsps.ssl.com	Verified?	Verified
Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	EV	Verified?	Verified
EV Policy OID(s)	2.23.140.1.1	Verified?	Verified
Root Stores Included In		Verified?	Need Response From CA
Mozilla Applied Constraints	No	Verified?	Verified

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	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. test tool under maintenance	Verified?	Not Verified
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described herehttps://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Test tool under maintenance.	Verified?	Not Verified

Digital Fingerprint Information

SHA-1 Fingerprint	b7:ab:33:08:d1:ea:44:77:ba:14:80:12:5a:6f:bd:a9:36:49:0c:bb	Verified?	Verified
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	Verified?	Verified

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	• 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/2016/07/SSLcom_CP_CPS_Version_1_0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.ssl.com/app/uploads/2016/07/SSLcom_CP_CPS_Version_1_0.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/2014/06/SSL-2-12-16-RKGC-Ind-Auditor-Report.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/12/2016	**Verified?**	Verified
BR Audit	https://www.ssl.com/app/uploads/2016/07/SSL-COM-SSL-Baseline-Acct-Report-and-Mgmt-Assertion-FINAL-7-15-16.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	7/20/2016	**Verified?**	Verified
EV Audit	BDO	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified

EV Audit Statement Date	7/20/2016	**Verified?**	Verified
BR Commitment to Comply	in CP/CPS section 1.1.2	**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

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA