Print this page

Mozilla - CA Program

Case Information

Case Number	00000059	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Symantec	**Request Status**	Need Information from CA

Additional Case Information

Subject	Add Symantec-brand Class 3 roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1099311

General information about CA's associated organization

CA Email Alias 1	dl-eng-root-certificate-management@symantec.com		
CA Email Alias 2			
Company Website	http://www.symantec.com/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA, Global	**Verified?**	Verified
Primary Market / Customer Base	Symantec is a major commercial CA with worldwide operations and customer base.	**Verified?**	Verified
Impact to Mozilla Users	Firefox users may encounter SSL certs that chain up to Symantec roots, and Thunderbird users may encounter S/MIME certificates that chain up to Symantec roots.	**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	* CA Hierarchy: See https://www.symantec.com/about/profile/policies/repository.jsp Roots tab *CPS session 1.3.1 https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf * CPS section 3.2.2.2: For requests for internationalized domain names (IDNs) in Certificates, Symantec performs domain name owner verification to detect cases of homographic spoofing of IDNs. Symantec employs an automated process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA manually rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label. Symantec actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and fully commits to conforming with standards drafted by that body. * Revocation of Compromised Certificates -- CPS section 4.9 * DNS names go in SAN -- CPS section 7.1.2.3 * Domain owned by a Natural Person -- SSL certs are only issued to organizations.	**Verified?**	Verified

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	* Delegation of Domain / Email validation to third parties - CPS section 1.3.2: Third parties, who enter into a contractual relationship with Symantec, may operate their own	**Verified?**	Verified

Practices

RA and authorize the issuance of certificates by a STN CA. Third party RAs must abide by all the requirements of the STN CP, the STN CPS and the terms of their enterprise services agreement with Symantec. RAs may, however implement more restrictive practices based on their internal requirements.

* Allowing external entities to operate subordinate CAs -- CPS section 1.3.1: Symantec enterprise customers may operate their own CAs as subordinate CAs to a public STN PCA. Such a customer enters into a contractual relationship with Symantec to abide by all the requirements of the STN CP and the STN CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements.

* Certificates referencing hostnames or private IP addresses -- Symantec fully complies with the CAB Forum Baseline Requirements concerning certificates with non-FQDN or private IP addresses.

* Issuing SSL Certificates for Internal Domains -- Symantec's Authentication Team is aware that .int is a valid TLD. Symantec has issued certificates to .int, and we have verified that the subscriber owns the domain name. Symantec correctly identifies internal and external domain names and verifies that subscribers own/control the domain name to be included in their certificate.

Root Case Record # 1

Root Case Information

Root Certificate Name	Symantec Class 3 Public Primary Certification Authority - G4	**Root Case No**	R00000110
Request Status	Need Information from CA	**Case Number**	00000059

Certificate Data

Certificate Issuer Common Name	Symantec Class 3 Public Primary Certification Authority - G4
O From Issuer Field	Symantec Corporation
OU From Issuer Field	Symantec Trust Network
Valid From	2012 Oct 18
Valid To	2037 Dec 01
Certificate Serial Number	4c79b59a289c763164f58944d09102de
Subject	CN=Symantec Class 3 Public Primary Certification Authority - G4, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	58:D5:2D:B9:33:01:A4:FD:29:1A:8C:96:45:A0:8F:EE:7F:52:92:82
SHA-256 Fingerprint	53:DF:DF:A4:E2:97:FC:FE:07:59:4E:8C:62:D5:B8:AB:06:B3:2C:75:49:F3:8A:16:30:94:FD:64:29:D5:DA:43
Certificate Fingerprint	D0:36:85:A2:93:7C:F9:45:F4:C1:E2:40:C0:AF:0A:2D:D5:FA:5F:96:29:AE:6C:DA:4A:F5:20:44:88:2C:A2:71
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root signs internally-operated SubCAs which issue OV and EV TLS/SSL certificates, as well as Code Signing certificates.	**Verified?**	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/Symantec_Class_3_Public_Primary_Certification_Authority_G4.pem	**Verified?**	Verified
CRL URL(s)	http://s.symcb.com/symc-pca3-g4.crl http://rf.symcb.com/rf.crl	**Verified?**	Verified
OCSP URL(s)	http://s.symcd.com http://rf.symcd.com	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.840.1.113733.1.7.23.6	**Verified?**	Verified
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://ssltest36.ssl.symclab.com/	**Verified?**	Verified
Test Website - Expired			
Test Website - Revoked			

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

Revocation Tested	https://certificate.revocationcheck.com/ssltest36.ssl.symclab.com no errors	**Verified?**	Verified
CA/Browser Forum Lint Test	No Error	**Verified?**	Verified
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	// CN=Symantec Class 3 Public Primary Certification Authority - G4,OU=Symantec Trust Network,O=Symantec Corporation,C=US "2.16.840.1.113733.1.7.23.6", "Symantec EV OID", SEC_OID_UNKNOWN, { 0x53, 0xDF, 0xDF, 0xA4, 0xE2, 0x97, 0xFC, 0xFE, 0x07, 0x59, 0x4E, 0x8C, 0x62, 0xD5, 0xB8, 0xAB, 0x06, 0xB3, 0x2C, 0x75, 0x49, 0xF3, 0x8A, 0x16, 0x30, 0x94, 0xFD, 0x64, 0x29, 0xD5, 0xDA, 0x43 }, "MIGUMQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24x" "HzAdBgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxRTBDBgNVBAMTPFN5bWFu" "dGVjIENsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3Jp" "dHkgLSBHNA==", "THm1miicdjFk9YlE0JEC3g==", Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CPS 1.3.1 https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf	**Verified?**	Verified
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.	**Verified?**	Verified
Cross Signing	N/A	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	N/A	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	The CPS is a single document that defines the policies for all 4 classes of Certs.	**Verified?**	Verified
CA Document Repository	https://www.symantec.com/about/profile/policies/repository.jsp	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	http://www.us.kpmg.com	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/5/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified

EV Audit Statement Date	5/5/2015	Verified?	Verified
BR Commitment to Comply	STN-CP and STN-CPS section 1	Verified?	Verified
SSL Verification Procedures	CPS section 3.2.2.3: Symantec uses the following methods of vetting a domain name, with option 1 being the primary method: 1. Confirm the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by performing a whois look up. 2. Communicate directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Rely upon a Domain Authorization Document; 4. Communicate directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 5. Communicate with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; 6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.	Verified?	Verified
EV SSL Verification Procedures	CPS sections 3.1.1.1, 3.2.2.1, 4.1.2.2, 4.3.3, 4.9.1.1, 4.9.3.2: EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively. CPS section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. For Organization Validated (OV) and Extended Validation (EV) Certificates domain validation is completed in all cases along with Organizational validation. Symantec's procedures for issuing EV SSL Certificates are described in Appendix B1 to this CPS. Appendix B1, and Appendix D all just say: The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-requirements-documents/ EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS.	Verified?	Verified
Organization Verification Procedures	CPS Section 1.4.1: According to tables 1 and 2, only Class 3 certificates issued to organizations can be used for SSL and Code Signing. Therefore all SSL certs are of OV or EV verification type. CPS Section 3.2.2: Authentication of Organization Identity CPS section 3.2.3: Authentication of Individual Identity CPS section 3.2.5: Validation of Authority	Verified?	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	Verified?	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit for root certs.	Verified?	Not Applicable
Multi-Factor Authentication	STN-CPS section 5.2	Verified?	Verified
Network Security	STN-CPS section 6.7	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1019864	Verified?	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	Symantec Class 3 Public Primary Certification Authority - G6	Root Case No	R00000111
Request Status	Need Information from CA	Case Number	00000059

Certificate Data

Certificate Issuer	Symantec Class 3 Public Primary Certification Authority - G6

Common Name	
O From Issuer Field	Symantec Corporation
OU From Issuer Field	Symantec Trust Network
Valid From	2012 Oct 18
Valid To	2037 Dec 01
Certificate Serial Number	65637185d36f45c68f7f31f909879282
Subject	CN=Symantec Class 3 Public Primary Certification Authority - G6, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	26:A1:6C:23:5A:24:72:22:9B:23:62:80:25:BC:80:97:C8:85:24:A1
SHA-256 Fingerprint	B3:23:96:74:64:53:44:2F:35:3E:61:62:92:BB:20:BB:AA:5D:23:B5:46:45:0F:DB:9C:54:B8:38:61:67:D5:29
Certificate Fingerprint	EA:DC:50:0A:D8:8D:07:EA:31:EE:8E:98:AD:E2:1E:42:A9:7D:87:E8:BC:B7:CA:A2:C4:71:D5:79:A4:53:EF:33
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root signs internally-operated SubCAs which issue OV and EV TLS/SSL certificates, as well as Code Signing certificates.	Verified?	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/Symantec_Class_3_Public_Primary_Certification_Authority_G6.pem	Verified?	Verified
CRL URL(s)	http://s.symcb.com/pca3-g6.crl http://rg.symcb.com/rg.crl	Verified?	Verified
OCSP URL(s)	http://s.symcd.com http://rg.symcd.com	Verified?	Verified
Trust Bits	Websites	Verified?	Verified
SSL Validation Type	OV; EV	Verified?	Verified
EV Policy OID(s)	2.16.840.1.113733.1.7.23.6	Verified?	Verified
Root Stores Included In	Apple; Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://ssltest38.ssl.symclab.com/	Verified?	Verified
Test Website - Expired			
Test Website - Revoked			

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

Revocation Tested	Tested using https://certificate.revocationcheck.com/ -> Certificate Upload -> PEM of root cert, and OCSP urls.	Verified?	Verified
CA/Browser Forum Lint Test	No Error	Verified?	Verified
Test Website Lint Test	Test not currently available	Verified?	Not Applicable
EV Tested	// CN=Symantec Class 3 Public Primary Certification Authority - G6,OU=Symantec Trust Network,O=Symantec Corporation,C=US "2.16.840.1.113733.1.7.23.6", "Symantec EV OID", SEC_OID_UNKNOWN, { 0xB3, 0x23, 0x96, 0x74, 0x64, 0x53, 0x44, 0x2F, 0x35, 0x3E, 0x61, 0x62, 0x92, 0xBB, 0x20, 0xBB, 0xAA, 0x5D, 0x23, 0xB5, 0x46, 0x45, 0x0F, 0xDB, 0x9C, 0x54, 0xB8, 0x38, 0x61, 0x67, 0xD5, 0x29 }, "MIGUMQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24x" "HzAdBgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxRTBDBgNVBAMTPFN5bWFu" "dGVjIENsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3Jp" "dHkgLSBHNg==", "ZWNxhdNvRcaPfzH5CYeSgg==", Success!	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	CPS 1.3.1 https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf	**Verified?**	Verified
Externally Operated SubCAs	This root does not and will not have any subCAs that are operated by external third parties.	**Verified?**	Verified
Cross Signing	N/A	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	N/A	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	The CPS is a single document that defines the policies for all 4 classes of Certs.	**Verified?**	Verified
CA Document Repository	https://www.symantec.com/about/profile/policies/repository.jsp	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	KPMG	**Verified?**	Verified
Auditor Website	http://www.us.kpmg.com	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/5/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf Note: This new root will be covered in the next audit.	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Commitment to Comply	STN-CP and STN-CPS section 1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.3: Symantec uses the following methods of vetting a domain name, with option 1 being the primary method: 1. Confirm the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by performing a whois look up. 2. Communicate directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Rely upon a Domain Authorization Document; 4. Communicate directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 5. Communicate with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; 6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.	**Verified?**	Verified
EV SSL Verification Procedures	CPS sections 3.1.1.1, 3.2.2.1, 4.1.2.2, 4.3.3, 4.9.1.1, 4.9.3.2: EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively. CPS section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. For Organization Validated (OV) and	**Verified?**	Verified

	Extended Validation (EV) Certificates domain validation is completed in all cases along with Organizational validation. Symantec's procedures for issuing EV SSL Certificates are described in Appendix B1 to this CPS. Appendix B1, and Appendix D all just say: The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-requirements-documents/ EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS.		
Organization Verification Procedures	CPS Section 1.4.1: According to tables 1 and 2, only Class 3 certificates issued to organizations can be used for SSL and Code Signing. Therefore all SSL certs are of OV or EV verification type. CPS Section 3.2.2: Authentication of Organization Identity CPS section 3.2.3: Authentication of Individual Identity CPS section 3.2.5: Validation of Authority	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Mozilla is no longer enabling the Code Signing trust bit for root certs.	**Verified?**	Not Applicable
Multi-Factor Authentication	STN-CPS section 5.2	**Verified?**	Verified
Network Security	STN-CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://bugzilla.mozilla.org/show_bug.cgi?id=1019864	**Verified?**	Verified