Print this page

Mozilla - CA Program

Case Information

Case Number	00000051	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Symantec	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Add Symantec-brand Class 1 and Class 2 roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=833986

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	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes 3) Audit Criteria: Yes 4) Document Handling of IDNs in CP/CPS: No 5) Revocation of Compromised Certificates: Yes (CPS section 4.9) 6) Verifying Domain Name Ownership: CPS section 3.2.2.3 7) Verifying Email Address Control: CPS session 3.2.3 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: No 10) Domain owned by a Natural Person: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity 11) OCSP: Confirm OCSP responds according to expected 12) Network Security Controls: CPS section 6.7	**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 Practices	* Delegation of Domain / Email validation to third parties - CPS section 3.2.3: Third parties, who enter into a contractual relationship with Symantec, may operate their own 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	**Verified?**	Verified

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 1 Public Primary Certification Authority - G6	**Root Case No**	R00000067
Request Status	Ready for Public Discussion	**Case Number**	00000051

Additional Root Case Information

Subject	Add Symantec Class 1 Public Primary Certification Authority - G6 root cert

Technical Information about Root Certificate

O From Issuer Field	Symantec Corporation	**Verified?**	Verified
OU From Issuer Field	Symantec Trust Network	**Verified?**	Verified
Certificate Summary	This SHA2 root will eventually replace the VeriSign Class 1 Root.	**Verified?**	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/PCA_1_G6.pem	**Verified?**	Verified
Valid From	2011 Oct 18	**Verified?**	Verified
Valid To	2037 Dec 01	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	example cert: https://bugzilla.mozilla.org/attachment.cgi?id=8705364	**Verified?**	Verified
CRL URL(s)	http://crl.ws.symantec.com/pca1-g6.crl	**Verified?**	Verified
OCSP URL(s)	None	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

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

Revocation Tested	**Verified?**	Not Applicable
CA/Browser Forum Lint Test	**Verified?**	Not Applicable
Test Website Lint Test	**Verified?**	Not Applicable
EV Tested	**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	51:7F:61:1E:29:91:6B:53:82:FB:72:E7:44:D9:8D:C3:CC:53:6D:64	**Verified?**	Verified
SHA-256 Fingerprint	9D:19:0B:2E:31:45:66:68:5B:E8:A8:89:E2:7A:A8:C7:D7:AE:1D:8A:AD:DB:A3:C1:EC:F9:D2:48:63:CD:34:B9	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root will be used to sign Class 1 SubCAs for SMIME and Client Auth purposes. SubCA keys will operate at Symantec or Symantec Affiliate sites.	**Verified?**	Verified
Externally Operated SubCAs	Yes, there may be externally operated SubCAs chaining to this Root. The externally operated CAs will be run by Symantec Affiliates.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**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	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting the websites trust bit for this root.	**Verified?**	Not Applicable
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	CP and CPS section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec or an Affiliate authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. CP and CPS section 3.2.3: Class 1 -- No identity authentication. Limited confirmation that the certificate subscriber has access to the email address.	**Verified?**	Verified
Email Address Verification Procedures	CP and CPS section 3.2.3: Class 1 - Symantec performs a challenge-response type of procedure in which Symantec sends email to the email address to be included in the certificate, containing unpredictable information such as a randomly generated PIN/Password unique to the owner of the email address. The owner of the email address (the subscriber of the certificate) demonstrates control over the email address by using the information within the email, to then proceed with accessing a portal with the unique information sent in the email, to download and install the certificate.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	**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	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Not Applicable

Root Case Record # 2

Root Case Information

Root Certificate Name	Symantec Class 2 Public Primary Certification Authority - G6	**Root Case No**	R00000068
Request Status	Ready for Public Discussion	**Case Number**	00000051

Additional Root Case Information

Subject	Add Symantec Class 2 Public Primary Certification Authority - G6 root cert

Technical Information about Root Certificate

O From Issuer Field	Symantec Corporation	**Verified?**	Verified
OU From Issuer Field	Symantec Trust Network	**Verified?**	Verified
Certificate Summary	This SHA2 root will eventually replace the VeriSign Class 2 Root.	**Verified?**	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/PCA_2_G6.pem	**Verified?**	Verified
Valid From	2011 Oct 18	**Verified?**	Verified
Valid To	2037 Dec 01	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	example cert: https://bugzilla.mozilla.org/attachment.cgi?id=8705366	**Verified?**	Verified
CRL URL(s)	http://crl.ws.symantec.com/pca2-g6.crl	**Verified?**	Verified
OCSP URL(s)	None	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

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

Revocation Tested	**Verified?**	Not Applicable
CA/Browser Forum Lint Test	**Verified?**	Not Applicable
Test Website Lint Test	**Verified?**	Not Applicable
EV Tested	**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	40:B3:31:A0:E9:BF:E8:55:BC:39:93:CA:70:4F:4E:C2:51:D4:1D:8F	**Verified?**	Verified
SHA-256 Fingerprint	CB:62:7D:18:B5:8A:D5:6D:DE:33:1A:30:45:6B:C6:5C:60:1A:4E:9B:18:DE:DC:EA:08:E7:DA:AA:07:81:5F:F0	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root will be used to sign Class 2 SubCAs for SMIME and Client Auth purposes. SubCA keys will operate at Symantec or Symantec Affiliate sites.	**Verified?**	Verified
Externally Operated	There may be externally operated SubCAs chain to this Root. The externally	**Verified?**	Verified

SubCAs	operated CAs will be run by Symantec Affiliates.		
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**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	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting the websites trust bit for this root.	**Verified?**	Not Applicable
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	CP and CPS section 3.2.2, 3.2.3, and 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.3: Class 2 - Authenticate identity by: - Manual check performed by the enterprise administrator customer for each subscriber requesting a certificate, “in which the subscriber receives the certificate via an email sent to the address provided during enrollment” or - Passcode-based authentication where a randomly-generated passcode is delivered out-of-band by the enterprise administrator customer to the subscriber entitled to enroll for the certificate, and the subscriber provides this passcode at enrollment time or - Comparing information provided by the subscriber to information contained in business records or databases (customer directories such as Active Directory or LDAP.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	**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	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Not Applicable

Root Case Record # 3

Root Case Information

Root Certificate Name	Symantec Class 1 Public Primary Certification Authority - G4	**Root Case No**	R00000108
Request Status	Ready for Public Discussion	**Case Number**	00000051

Additional Root Case Information

Subject	Add Symantec Class 1 Public Primary Certification Authority - G4 cert

Technical Information about Root Certificate

O From Issuer Field	Symantec Corporation	**Verified?**	Verified
OU From Issuer Field	Symantec Trust Network	**Verified?**	Verified
Certificate Summary	This is the ECC version of the SHA2 Symantec Class 1 root.	**Verified?**	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/Symantec_Class_1_Public_Primary_Certification_Authority_G4.pem	**Verified?**	Verified
Valid From	2011 Oct 05	**Verified?**	Verified
Valid To	2038 Jan 18	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	Example cert: https://bugzilla.mozilla.org/attachment.cgi?id=8705361	**Verified?**	Verified
CRL URL(s)	http://crl.ws.symantec.com/pca1-g4.crl	**Verified?**	Verified
OCSP URL(s)	None yet.	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

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

Revocation Tested	**Verified?**	Not Applicable
CA/Browser Forum Lint Test	**Verified?**	Not Applicable
Test Website Lint Test	**Verified?**	Not Applicable
EV Tested	**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1 Fingerprint	84:F2:E3:DD:83:13:3E:A9:1D:19:52:7F:02:D7:29:BF:C1:5F:E6:67	**Verified?**	Verified
SHA-256 Fingerprint	36:3F:3C:84:9E:AB:03:B0:A2:A0:F6:36:D7:B8:6D:04:D3:AC:7F:CF:E2:6A:0A:91:21:AB:97:95:F6:E1:76:DF	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root will be used to sign Class 1 SubCAs for SMIME and Client Auth purposes. SubCA keys will operate at Symantec or Symantec Affiliate sites.	**Verified?**	Verified
Externally Operated SubCAs	Yes, there may be externally operated SubCAs chaining to this Root. The externally operated CAs will be run by Symantec Affiliates.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**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	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting the websites trust bit for this root.	**Verified?**	Not Applicable
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	CP and CPS section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec or an Affiliate authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. CP and CPS section 3.2.3: Class 1 -- No identity authentication. Limited confirmation that the certificate subscriber has access to the email address.	**Verified?**	Verified
Email Address Verification Procedures	CP and CPS section 3.2.3: Class 1 - Symantec performs a challenge-response type of procedure in which Symantec sends email to the email address to be included in the certificate, containing unpredictable information such as a randomly generated PIN/Password unique to the owner of the email address. The owner of the email address (the subscriber of the certificate) demonstrates control over the email address by using the information within the email, to then proceed with accessing a portal with the unique information sent in the email, to download and install the certificate.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	**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	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Not Applicable

Root Case Record # 4

Root Case Information

Root Certificate Name	Symantec Class 2 Public Primary Certification Authority - G4	**Root Case No**	R00000109
Request Status	Ready for Public Discussion	**Case Number**	00000051

Additional Root Case Information

Subject	Add Symantec Class 2 Public Primary Certification Authority - G4 root cert

Technical Information about Root Certificate

O From Issuer Field	Symantec Corporation	**Verified?**	Verified
OU From Issuer Field	Symantec Trust Network	**Verified?**	Verified
Certificate Summary	This is the ECC version of the SHA2 Symantec Class 2 root certificate.	**Verified?**	Verified
Root Certificate Download URL	https://www.symantec.com/content/en/us/enterprise/verisign/roots/Symantec_Class_2_Public_Primary_Certification_Authority_G4.pem	**Verified?**	Verified
Valid From	2011 Oct 05	**Verified?**	Verified
Valid To	2038 Jan 18	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	example cert: hhttps://bugzilla.mozilla.org/attachment.cgi?id=8705365	**Verified?**	Verified
CRL URL(s)	http://crl.ws.symantec.com/pca2-g4.crl	**Verified?**	Verified
OCSP URL(s)	None	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

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

Revocation Tested		**Verified?**	Not Applicable
CA/Browser Forum Lint Test		**Verified?**	Not Applicable
Test Website Lint Test		**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable

Digital Fingerprint Information

SHA-1	67:24:90:2E:48:01:B0:22:96:40:10:46:B4:B1:67:2C:A9:75:FD:2B	**Verified?**	Verified

Fingerprint			
SHA-256 Fingerprint	FE:86:3D:08:22:FE:7A:23:53:FA:48:4D:59:24:E8:75:65:6D:3D:C9:FB:58:77:1F:6F:61:6F:9D:57:1B:C5:92	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root will be used to sign Class 2 SubCAs for SMIME and Client Auth purposes. SubCA keys will operate at Symantec or Symantec Affiliate sites.	**Verified?**	Verified
Externally Operated SubCAs	There may be externally operated SubCAs chain to this Root. The externally operated CAs will be run by Symantec Affiliates.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**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	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply		**Verified?**	Not Applicable
SSL Verification Procedures	Not requesting the websites trust bit for this root.	**Verified?**	Not Applicable
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	CP and CPS section 3.2.2, 3.2.3, and 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.3: Class 2 - Authenticate identity by: - Manual check performed by the enterprise administrator customer for each subscriber requesting a certificate, “in which the subscriber receives the certificate via an email sent to the address provided during enrollment” or - Passcode-based authentication where a randomly-generated passcode is delivered out-of-band by the enterprise administrator customer to the subscriber entitled to enroll for the certificate, and the subscriber provides this passcode at enrollment time or - Comparing information provided by the subscriber to information contained in business records or databases (customer directories such as Active Directory or LDAP.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	**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	Only the email trust bit will be set for this root. See item #4 of https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Not Applicable