Print this page

# Mozilla - CA Program

## Case Information

| | | | |
|---|---|---|---|
| **Case Number** | 00000051 | **Case Record Type** | CA Owner/Root Inclusion Request |
| **CA Owners/Certificate Name** | Symantec | **Request Status** | Need Information from CA |

## Additional Case Information

| | | | |
|---|---|---|---|
| **Subject** | Add Symantec-branded Roots - first group | **Date/Time Opened** | 11/18/2014 2:59 PM |
| **Case Reason** | | **Date/Time Closed** | |
| **Case Origin** | | **Type** | |
| **Status** | New | **Priority** | Medium |

## Bugzilla Information

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

## General information about CA's associated organization

| | | | |
|---|---|---|---|
| **Company Website** | http://www.symantec.com/ | **Verified?** | Verified |
| **Organizational Type** | Public Corporation | **Verified?** | Verified |
| **Organizational Type (Others)** | | **Verified?** | Not Applicable |
| **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 |

## Existing CA Contact Information

| | | | |
|---|---|---|---|
| **Contact Name** | Rashmi Tabada | **Contact Department** | |
| **Contact Phone** | | **Contact Title** | |
| **Contact Email** | rashmi_tabada@symantec.com | | |

## New CA Contact Information

| | | | |
|---|---|---|---|
| **New Contact Name** | Symantec | **New Contact Department** | Enterprise Security Group |
| **New Contact Phone** | (650) 527-7181 | **New Contact Title** | Senior Product Manager |
| **New Contact Email** | dl-eng-root-certificate-management@symantec.com | | |

## Response to Mozilla's list of Recommended Practices

| | | | |
|---|---|---|---|
| **Recommended Practices** | https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices | **Recommended Practices Statement** | Do you agree with this statement?<br>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** | From my previous notes. Please correct if needed:<br>CA Hierarchy -- see http://www.verisign.com/repository/root.html,, http://www.verisign.com/repository/ca-ra.html and http://www.verisign.com/repository/hierarchy/hierarchy.pdf<br><br>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.<br>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.<br><br>Revocation of Compromised Certificates -- CPS section 4.9<br><br>DNS names go in SAN -- CPS section 7.1.2.3<br><br>Domain owned by a Natural Person -- SSL certs are only issued to organizations. | **Verified?** | Need Clarification From CA |

## 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** | Do you agree with this statement?<br>I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below |
| **CA's Response to Problematic Practices** | From my previous notes. Please correct if needed:<br>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 RA and authorize the issuance of certificates by a VTN CA. Third party CAs must abide by all the requirements of the VTN CP the VTN CPS, and the terms of their enterprise services agreement with VeriSign. RAs may, however implement more restrictive practices based on their internal requirements.<br>Does this include SSL cert issuance?<br>Does this include EV SSL cert issuance?<br><br>Allowing external entities to operate subordinate CAs -- Symantec does not allow any external entities to operate subordinate CAs signed by any VeriSign or Symantec root.<br><br>SHA1 Certificate issuance?<br><br>Certificates referencing hostnames or private IP addresses -- Symantec fully complies with the CAB Forum Baseline | **Verified?** | Need Clarification From CA |

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 Cases

**Root Cases Record # 1**

## Root Case Information

| | | | |
|---|---|---|---|
| **Root Case No** | R00000067 | **Owner** | Kathleen Wilson |
| **Case Number** | 00000051 | **Request Status** | Need Information from CA |
| **Root Certificate Name** | Symantec Class 1 Public Primary Certification Authority - G6 | | |

## Additional Root Case Information

| | | | |
|---|---|---|---|
| **Subject** | Add Symantec Class 1 Public Primary Certification Authority - G6 root cert | **Date/Time Opened** | |
| | | **Date/Time Closed** | |

## CA Hierarchy information for each root certificate

| | | | |
|---|---|---|---|
| **CA Hierarchy** | ??? | **Verified?** | Need Clarification From CA |
| **Externally Operated SubCAs** | ??? | **Verified?** | Need Clarification From CA |
| **Cross Signing** | ??? | **Verified?** | Need Clarification From CA |
| **Technical Constraint on 3rd party Issuer** | Are there any technical constraints on the RAs and external subCAs who can issue certs in this hierarchy? Please explain. | **Verified?** | Need Clarification From CA |

## Technical information about each 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 |
| **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 |
| **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)** | example cert: https://bugzilla.mozilla.org/attachment.cgi?id=717223 | **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 |
| **EV Tested** | | **Verified?** | Not Applicable |
| **Browsers Included In** | Internet Explorer | **Verified?** | Verified |
| **Mozilla Applied Constraints** | None | **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/content/en/us/about/media/repository/ | **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** | 6/18/2014 | **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 Reply** | | **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** | STN-CP 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.<br><br>STN-CP section 3.2.3: Class 1 -- No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.<br><br>See also STN-CPS sections 3.2.2 and 3.2.3. | **Verified?** | Verified |
| **Email Address Verification Procedures** | Email certs can be issued for Class 1, 2, and 3 verification levels, for both individuals and organizations.<br>The absolute minimum verification is for Class 1 individual.<br>STN-CPS section 3.2.3<br>Class 1: No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address. | **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** | What is the link to the publicly disclosed/audited subCAs for this root? i.e. for the subCAs that are not technically constrained. See https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions | **Verified?** | Need Clarification From CA |

**Root Cases Record # 2**

## Root Case Information

| | | | |
|---|---|---|---|
| **Root Case No** | R00000068 | **Owner** | Kathleen Wilson |
| **Case Number** | 00000051 | **Request Status** | Need Information from CA |
| **Root Certificate Name** | Symantec Class 2 Public Primary Certification Authority - G6 | | |

## Additional Root Case Information

| | | | |
|---|---|---|---|
| **Subject** | Add Symantec Class 2 Public Primary Certification Authority - G6 root cert | **Date/Time Opened** | |
| | | **Date/Time Closed** | |

## CA Hierarchy information for each root certificate

| | | | |
|---|---|---|---|
| **CA Hierarchy** | ??? | **Verified?** | Need Clarification From CA |
| **Externally Operated SubCAs** | ??? | **Verified?** | Need Clarification From CA |
| **Cross Signing** | ??? | **Verified?** | Need Clarification From CA |
| **Technical Constraint on 3rd party Issuer** | Are there any technical constraints on the RAs and external subCAs who can issue certs in this hierarchy? Please explain. | **Verified?** | Need Clarification From CA |

## Technical information about each 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 |
| **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 |
| **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)** | example cert: https://bugzilla.mozilla.org/attachment.cgi?id=717223 | **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 |
| **EV Tested** | | **Verified?** | Not Applicable |
| **Browsers Included In** | Internet Explorer | **Verified?** | Verified |
| **Mozilla Applied Constraints** | None | **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/content/en/us/about/media/repository/ | **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** | 6/18/2014 | **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 Reply** | | **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** | STN-CP 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.<br><br>STN-CP section 3.2.3:<br>Class 1 -- No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.<br>Class 2 -- Authenticate identity by matching the identity provided by the Subscriber to:<br>- information residing in the database of a Symantec-approved identity proofing service, such as a major credit bureau or other reliable source of information providing services in Symantec's or the Affiliate's country or territory, or<br>- information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals<br><br>See also STN-CPS sections 3.2.2 and 3.2.3. | **Verified?** | Verified |
| **Email Address Verification Procedures** | Email certs can be issued for Class 1, 2, and 3 verification levels, for both individuals and organizations.<br>The absolute minimum verification is for Class 1 individual.<br>STN-CPS section 3.2.3<br>Class 1: No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.<br>Class 2 individual: Authenticate identity by matching the identity provided by the Subscriber to:<br>- information residing in the database of a Symantec-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or<br>- information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals | **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** | What is the link to the publicly disclosed/audited subCAs for this root? i.e. for the subCAs that are not technically constrained. See https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions | **Verified?** | Need Clarification From CA |

**Root Cases Record # 3**

## Root Case Information

| | | | |
|---|---|---|---|
| **Root Case No** | R00000069 | **Owner** | Kathleen Wilson |
| **Case Number** | 00000051 | **Request Status** | Need Information from CA |
| **Root Certificate Name** | Symantec Class 3 Public Primary Certification Authority - G7 | | |

## Additional Root Case Information

| | | | |
|---|---|---|---|
| **Subject** | Add Symantec Class 3 Public Primary Certification Authority - G7 root | **Date/Time Opened** | |
| | | **Date/Time Closed** | |

## CA Hierarchy information for each root certificate

| | | | |
|---|---|---|---|
| **CA Hierarchy** | ??? | **Verified?** | Need Clarification From CA |
| **Externally Operated SubCAs** | ???<br>Current?<br>Can there be?<br>Policies regarding externally-operated subCAs? | **Verified?** | Need Clarification From CA |
| **Cross Signing** | ??? | **Verified?** | Need Clarification From CA |
| **Technical Constraint on 3rd party Issuer** | Are there any technical constraints on the RAs and external subCAs who can issue certs in this hierarchy? Please explain. | **Verified?** | Need Clarification From CA |

## Technical information about each 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 3 Root. | **Verified?** | Verified |
| **Root Certificate Download URL** | https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1916&actp=search&viewlocale=en_US&searchid=1417452592505 | **Verified?** | Verified |
| **SHA-1 Fingerprint** | 75:92:75:24:04:90:C9:E4:03:F3:B4:86:99:40:33:FF:F4:D7:E5:66 | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **SHA-256 Fingerprint** | C4:FA:68:F8:27:09:24:C3:00:CB:C0:D3:61:5A:7B:88:E8:22:31:74:9C:F6:52:24:52:27:22:22:C9:F0:A8:3E | **Verified?** | Verified |
| **Valid From** | 2012 Oct 15 | **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)** | Need a test website whose EV SSL cert chains up to this root. | **Verified?** | Need Clarification From CA |
| **CRL URL(s)** | Need | **Verified?** | Need Clarification From CA |
| **OCSP URL(s)** | Need | **Verified?** | Need Clarification From CA |
| **Trust Bits** | Code; Email; Websites | **Verified?** | Verified |
| **SSL Validation Type** | DV; OV; EV | **Verified?** | Verified |
| **EV Policy OID(s)** | Requesting EV Treatment? | **Verified?** | Need Clarification From CA |
| **EV Tested** | Please provide EV test output: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version | **Verified?** | Need Clarification From CA |
| **Browsers Included In** | Internet Explorer | **Verified?** | Need Clarification From CA |
| **Mozilla Applied Constraints** | None | **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/content/en/us/about/media/repository/ | **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** | 6/18/2014 | **Verified?** | Verified |
| **BR Audit** | http://www.symantec.com/content/en/us/about/media/repository/symantec-webtrust-audit-report.pdf | **Verified?** | Verified |
| **BR Audit Type** | WebTrust | **Verified?** | Verified |
| **BR Audit Statement Date** | 6/18/2014 | **Verified?** | Verified |
| **EV Audit** | https://cert.webtrust.org/SealFile?seal=1565&file=pdf | **Verified?** | Verified |
| **EV Audit Type** | WebTrust | **Verified?** | Verified |
| **EV Audit Statement Date** | 6/18/2014 | **Verified?** | Verified |
| **BR Commitment to Reply** | STN-CP and STN-CPS section 1 | **Verified?** | Verified |
| **SSL Verification Procedures** | CPS section 3.2.2: Symantec's procedures for issuing OV and DV certificates, distinguished throughout the CPS as 'CABF requirements for OV and DV certificates' are described in Appendix D to this CPS.<br><br>CPS section 3.2.2.1: 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, in section 11 of Appendix B1, Appendix C and Appendix D, respectively.<br><br>The Appendix B1 and D 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/<br><br>Please see https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs "It is not sufficient to simply reference section 11 of the CA/Brower Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate." | **Verified?** | Need Clarification From CA |
| **EV SSL Verification Procedures** | CPS section 3.2.2: Symantec's procedures for issuing EV SSL Certificates are described in Appendix B1 to this CPS.<br><br>The Appendix B1 and D 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/<br><br>Please see https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs "It is not sufficient to simply reference section 11 of the CA/Brower Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section | **Verified?** | Need Clarification From CA |

| | | | |
|---|---|---|---|
| | 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate." | | |
| **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 verification type.<br><br>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.<br><br>CPS section 3.2.3: The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport or driver's license and one other identification credential.<br>The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the identity and authorization of the person to act as Administrator.<br><br>CPS section 3.2.5: Validation of Authority | **Verified?** | Verified |
| **Email Address Verification Procedures** | Email certs can be issued for Class 1, 2, and 3 verification levels, for both individuals and organizations.<br>The absolute minimum verification is for Class 1 individual.<br>STN-CPS section 3.2.3<br>Class 1: No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.<br>Class 2 individual: Authenticate identity by matching the identity provided by the Subscriber to:<br>- information residing in the database of a Symantec-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or<br>- information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals<br>Class 3: See above. | **Verified?** | Verified |
| **Code Signing Subscriber Verification Pro** | According to CPS section 1.4.1.2 Table 2, Code Signing certificates are of Class 3 only.<br><br>See CPS sections 3.2.2, 3.2.3, and 3.2.5. | **Verified?** | Verified |
| **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** | What is the link to the publicly disclosed/audited subCAs for this root? i.e. for the subCAs that are not technically constrained. See https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions | **Verified?** | Need Clarification From CA |