**Bugzilla ID:**

**Bugzilla Summary:**

CAs wishing to have their certificates included in Mozilla products must

1. Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2. Supply all of the information listed in <http://wiki.mozilla.org/CA:Information_checklist>.
   1. Review the Recommended Practices at <https://wiki.mozilla.org/CA:Recommended_Practices>
   2. Review the Potentially Problematic Practices at <https://wiki.mozilla.org/CA:Problematic_Practices>

**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | Symantec Corporation |
| Website URL | [www.symantec.com](http://www.symantec.com), <www.verisign.com> |
| Organizational type | Commercial |
| Primary Market / Customer Base | Symantec is a major commercial CA with worldwide operations and customer base. |
| Impact to Mozilla Users | Firefox users may encounter SSL certs that chain up to some of these roots, and Thunderbird users may encounter S/MIME certificates that chain up to some of these roots. |
| CA Contact Information | CA Email Alias: DL-ENG-Root-Certificate-Management@symantec.com  CA Phone Number: Gautam Kanaparthi, 650-527-7181  Title / Department: Senior Product Manager, Enterprise Security Group |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 1 Public Primary Certification Authority - G7 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 1 Public Primary Certification Authority - G7 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 79197e497c60c6150c64ddc0407cfd9c3ec2fbfe |
| Valid From | 2012-10-14 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithDSA |
| Signing key parameters | DSA 2048, 256 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIGfDCCBiKgAwIBAgIQGWT6v/pCR62/Ng1I7+QUGDALBglghkgBZQMEAwIwgZQx  CzAJBgNVBAYTAlVTMR0wGwYDVQQKExRTeW1hbnRlYyBDb3Jwb3JhdGlvbjEfMB0G  A1UECxMWU3ltYW50ZWMgVHJ1c3QgTmV0d29yazFFMEMGA1UEAxM8U3ltYW50ZWMg  Q2xhc3MgMSBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAt  IEc3MB4XDTEyMTEwMTAwMDAwMFoXDTE0MTAzMTIzNTk1OVowgdAxCzAJBgNVBAYT  AlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3  MR0wGwYDVQQKExRTeW1hbnRlYyBDb3Jwb3JhdGlvbjE6MDgGA1UECxMxRk9SIFRF  U1QgUFVSUE9TRVMgT05MWSAtIENsYXNzIDEgRFNBIFRlc3QgRUUgQ2VydDE5MDcG  A1UEAxMwU3ltYW50ZWMgQ2xhc3MgMSBUZXN0IERTQSBFbmQgRW50aXR5IENlcnRp  ZmljYXRlMIIDRjCCAjkGByqGSM44BAEwggIsAoIBAQC5nykhvhXnPZfHSOzDqcZV  3w56ozXwaf5qY/HHfgLA9JLeiXa5T7SZ33g/kJMIrlL39Kmfi37hDQsFcDWFKxVu  QpMTo7CEAg8o13o/cGUUIihpNIyxMq+W6fqr8ryuUuBlR8f1wt8B1ZeMkuy2N8Nr  rdH3uXXD5uJOHTM0aKTAzBA6X3GGoJaHKNaBv1Ah6PI7NXD89WuScY+IH+5iV5/e  6P4pFqyU52tIY0AaBfFxl3rmIgSR386GKEI2rKf9lT6XMdzYLI56663SoLOcTc8t  A9HF+nQG2d6H0DQCxVcXiLOM5tqddynFnPHjsDz/xCIQgY155YwTqmtF2tsCiRYV  AiEAshyr2P9zqmaNl1A3GLatVgPR0hbTS30n2ZwQFqCtM80CggEASiE05ifB5mNk  34PETryY44Wi2S8p7zr+0zjt/y1IR7bZX7XWxEWxehM4F3ykhF0ya30zv+QPwY/o  eYGJqsaA+o5fzGUAbGXTaYSkixekiOqBDbfQKrMDN2EAohgvhMF7qy3Yeoc1sHOp  Ug0saeVcdMWh+aLe97wW3hltoo4mwbt5kRRujj5znJtZN0zJ70XjsUiVedQp52bK  Ohh9mEVc0M3NqM5EHDaZWYKWys72gKI7xSFdGax/1DfOnHQz+iaYfihvfSxZjMl3  3wHXSarnevHJj9xi2TM8NOHdXarOrMOUF1eW1ZVaL0T2uqN14ah71IXbnlNgEjUr  gzCZzRxWMwOCAQUAAoIBABAk9JvOw9POxwcDH0fTM6SEB4+ewPfWsmPFcSp+UKqu  bDQ8LRdUEbe0yTh5ew8pFI+JSwCnPrMPqMS+k/K+1v3a07AEqejXc4ae29j0pn/t  r8E3ghMiSi/8Z+8DOUDj8KPWdAQNvN8lSNae49zqEUaALSs5OTM/x+wnjvAEhoHw  stN8zWmxMBNsC4oRkOdg2zuBPi67DXZkAmIfU5R2GzhhnFxTWOUChFDb8IEjgm4/  pQQyaL9zbzxnUcwJ9L5mHM/kZy0wkpWr4sGquwqijOl2L1TyPCoCV11iyNQ0j0dP  /aqiqw4dQTd8Z0rzxlGkDAUJ0dcLMoUn1EjDlLk/SxijggEmMIIBIjAMBgNVHRMB  Af8EAjAAMEIGA1UdIAQ7MDkwNwYLYIZIAYb4RQEHFwEwKDAmBggrBgEFBQcCARYa  aHR0cDovL3d3dy5zeW1hdXRoLmNvbS9jcHMwNwYDVR0fBDAwLjAsoCqgKIYmaHR0  cDovL2NybC53cy5zeW1hbnRlYy5jb20vcGNhMS1nNy5jcmwwHQYDVR0lBBYwFAYI  KwYBBQUHAwIGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIHgDAmBgNVHREEHzAdgRtt  YXR0aGV3X3NvcmljaEBzeW1hbnRlYy5jb20wHQYDVR0OBBYEFKsNrSu2FKr+hsf6  fuYYjaleZ+MgMB8GA1UdIwQYMBaAFECWMs1V/Ejd//x1kAGmlyf83cziMAsGCWCG  SAFlAwQDAgNHADBEAiAiBpy6VNRjiyU1EIT6PlQ9IAFgf0guViY6k9U7vvieWgIg  Q3bldvBvT+owCnyWvjlX6dK5WlzaIc2+v5OgfjRGcuo=  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca1-g7.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for Email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 1 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 2 Public Primary Certification Authority - G7 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 2 Public Primary Certification Authority - G7 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 1ca37bb1b757bc8f90fc20c096c00ad2d466db63 |
| Valid From | 2012-10-14 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithDSA |
| Signing key parameters | DSA 2048, 256 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIGfDCCBiKgAwIBAgIQaDIQ+n+JB3ggFJr4uxcLdTALBglghkgBZQMEAwIwgZQx  CzAJBgNVBAYTAlVTMR0wGwYDVQQKExRTeW1hbnRlYyBDb3Jwb3JhdGlvbjEfMB0G  A1UECxMWU3ltYW50ZWMgVHJ1c3QgTmV0d29yazFFMEMGA1UEAxM8U3ltYW50ZWMg  Q2xhc3MgMiBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAt  IEc3MB4XDTEyMTEwMTAwMDAwMFoXDTE0MTAzMTIzNTk1OVowgdAxCzAJBgNVBAYT  AlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3  MR0wGwYDVQQKExRTeW1hbnRlYyBDb3Jwb3JhdGlvbjE6MDgGA1UECxMxRk9SIFRF  U1QgUFVSUE9TRVMgT05MWSAtIENsYXNzIDIgRFNBIFRlc3QgRUUgQ2VydDE5MDcG  A1UEAxMwU3ltYW50ZWMgQ2xhc3MgMiBUZXN0IERTQSBFbmQgRW50aXR5IENlcnRp  ZmljYXRlMIIDRjCCAjkGByqGSM44BAEwggIsAoIBAQD5cJIABNAaSWifRgq4U4X5  7WUwbTAK4o2zFzPRZzl2ChKzNvKDqMgMthF9d4GWsjU5w2C8v0zmg2GPq5IjAiuc  8LJP6FgT0WtDerQ9zvMmGYK79zZlAt7uvNw82G+5c+ti1q0oMEXWVPrfm1Gjcz7P  8LoCATeYxFHRrx3k7ePj5FNd/1EdEjyjcaeXyzBb3onibxYtRp9tTKxOfuBHsMi+  eUqL9xOTNOTPxMp/QmkK0QlQtfzjLzx5iG8Es8Egg1QXBxF+vNSd9m/oBSh/nep5  YA7dp3kCrwCGRTy/V3LW0LRoYV3io0qsIjarbukMuTaMoDa88umm8JGFeZRzjBRL  AiEAgjXkh8cGa0OodOsLMrcSIOmkbHZyI7GpPNMRaI+Ob/MCggEATh7qH2qE7ile  geyJHXllMF0FvgA6xQT5zasd4dNSuyKSVxAYq3D295ryMCvh4Fjv6OkwZn5FJqaK  LxzEOTPQTViagERehbZMMbnbJZQq5Hl9M7eN/Hd5kBZuOv8I3zn3chWrahcc59Q5  9P6vaUOeDb4PQwBz8WhH0kGNAd0u8QWPMo8lDlx8ss+MeI7pWesJUqBju7gya+Kh  5g28dirK3f/VIUVgnPauLApB6FM3MpatW4ku1TMSGLz9MGXZovaexeJ9y5Rpkdax  9jnP8SvUzC9fqvm6Xf4A54g/ExXSzHKqt94CV4D8OS+TA6bchNDo/+1ZBw0wW4ui  dRFMTqub8QOCAQUAAoIBAHuGA/Y5wo7l3a8NOFMSVbh/PS/u+66JTEq0RzR8pFjA  TyHNO1DzlGvf4xxTB9kTZUnyN4GYxbG/enGzjAEiRR83bSnfsvA8m5Lgyda5qtkh  C6BuV9eSGODKntwiPnYGffOo7/ULljQNWlS1BhQtrqMt7W9Wu7hnN6xHFCd0IeGr  n/GXfUpXuv/P0Bu4+gT7pBSncfRt1aZrOYPyniTuexwZfDlB/G14C5oojG9Vr7pM  pQ3nPHVMWLkruNDTXE8Srf8Lya+7Sb3kkr9cE9pBnF5W381yoDAyVDemeC5EJtEo  /yB/4j1IaBF2Pqi1CJGLyZKv8KWgGB5F4WfMLpHUl6qjggEmMIIBIjAMBgNVHRMB  Af8EAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAOBgNVHQ8BAf8E  BAMCB4AwJgYDVR0RBB8wHYEbbWF0dGhld19zb3JpY2hAc3ltYW50ZWMuY29tMEIG  A1UdIAQ7MDkwNwYLYIZIAYb4RQEHFwIwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3  dy5zeW1hdXRoLmNvbS9jcHMwNwYDVR0fBDAwLjAsoCqgKIYmaHR0cDovL2NybC53  cy5zeW1hbnRlYy5jb20vcGNhMi1nNy5jcmwwHQYDVR0OBBYEFHskfltaTrnqSaPP  9thC6qyecBj2MB8GA1UdIwQYMBaAFGchMhdJZXjlbAxzmp9CvDhZe/GdMAsGCWCG  SAFlAwQDAgNHADBEAiAaOzxTgq8WL6my0nQtz5iFLmmUZsiwdGfkoICiTIu7HgIg  dOBAR5++5cFPH448kLqvzfdD60YThQCmQoYhg90M7SM=  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca2-g7.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for Email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 2 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 3 Public Primary Certification Authority - G7 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 3 Public Primary Certification Authority - G7 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 759275240490c9e403f3b486994033fff4d7e566 |
| Valid From | 2012-10-14 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithDSA |
| Signing key parameters | DSA 2048, 256 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://ssltest37.ssl.symclab.com> |
| CRL URL | URL: <http://crl.ws.symantec.com/pca3-g7.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*   1. *Browsing to test website with OCSP enforced in Firefox browser*    1. Minefield returns an error: “ssl\_error\_bad\_handshake\_hash\_value” I believe DSA 2048 is not yet supported in Firefox?   *b) If requesting EV*: Not able to test until DSA 2048 is supported |
| Requested Trust Bits | Websites (SSL/TLS)  Email (S/MIME)  Code Signing |
| SSL Validation Type | OV, and/or EV |
| EV Policy OID(s) | 2.16.840.1.113733.1.7.23.6 |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 3 Root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 1 Public Primary Certification Authority - G4 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 1 Public Primary Certification Authority - G4 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 84f2e3dd83133ea91d19527f02d729bfc15fe667 |
| Valid From | 2011-10-05 |
| Valid To | 2038-01-18 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA384WithECC |
| Signing key parameters | ECC p384 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIDyDCCA0+gAwIBAgIQODgpYgAfyXlfvjvVCDnQ5jAKBggqhkjOPQQDAzCBlDEL  MAkGA1UEBhMCVVMxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMR8wHQYD  VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMUUwQwYDVQQDEzxTeW1hbnRlYyBD  bGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0g  RzQwHhcNMTIxMTAxMDAwMDAwWhcNMTMxMDMxMjM1OTU5WjCB0DELMAkGA1UEBhMC  VVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcx  HTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMTowOAYDVQQLEzFGT1IgVEVT  VCBQVVJQT1NFUyBPTkxZIC0gQ2xhc3MgMSBFQ0MgVGVzdCBFRSBDZXJ0MTkwNwYD  VQQDEzBTeW1hbnRlYyBDbGFzcyAxIFRlc3QgRUNDIEVuZCBFbnRpdHkgQ2VydGlm  aWNhdGUwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAR4vaBxAaGGKrwR2aLt3pVLQI7L  gluUj4KmWcgRZrPB2xC3odccLpAOP1CSektcmUuw2isObua/J2edNLuTKUiGDSUW  /30TF+iFyfmrIdh5PJleqohzTbh1E9UdoxlXqVyjggEmMIIBIjAMBgNVHRMBAf8E  AjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAmBgNVHREEHzAdgRtt  YXR0aGV3X3NvcmljaEBzeW1hbnRlYy5jb20wQgYDVR0gBDswOTA3BgtghkgBhvhF  AQcXATAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LnN5bWF1dGguY29tL2NwczA3  BgNVHR8EMDAuMCygKqAohiZodHRwOi8vY3JsLndzLnN5bWFudGVjLmNvbS9wY2Ex  LWc0LmNybDAOBgNVHQ8BAf8EBAMCA4gwHQYDVR0OBBYEFDlcseb8ZEZ8klehuaih  IfDA2bQSMB8GA1UdIwQYMBaAFGXAjSX1DLqXd5A/ni7gWvXO1eHkMAoGCCqGSM49  BAMDA2cAMGQCMCNm7xMAazdCaclu8yvN/qRphKow57nyCVul2u5jOMxu7iJzmwa6  2dB3uyCr94bmtgIwWF1LMmmkKwoYmVQTormfh/qayWjODj2V2L2imMup8GiMmBQc  zxDYQLDy0wDA4kcD  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca1-g4.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 1 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 2 Public Primary Certification Authority - G4 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 2 Public Primary Certification Authority - G4 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 6724902e4801b02296401046b4b1672ca975fd2b |
| Valid From | 2011-10-05 |
| Valid To | 2038-01-18 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA384WithECC |
| Signing key parameters | ECC p384 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIDyjCCA0+gAwIBAgIQDOpBN3tW+FMTPImfz3vJMjAKBggqhkjOPQQDAzCBlDEL  MAkGA1UEBhMCVVMxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMR8wHQYD  VQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMUUwQwYDVQQDEzxTeW1hbnRlYyBD  bGFzcyAyIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0g  RzQwHhcNMTIxMTAxMDAwMDAwWhcNMTMxMDMxMjM1OTU5WjCB0DELMAkGA1UEBhMC  VVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcx  HTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMTowOAYDVQQLEzFGT1IgVEVT  VCBQVVJQT1NFUyBPTkxZIC0gQ2xhc3MgMiBFQ0MgVGVzdCBFRSBDZXJ0MTkwNwYD  VQQDEzBTeW1hbnRlYyBDbGFzcyAyIFRlc3QgRUNDIEVuZCBFbnRpdHkgQ2VydGlm  aWNhdGUwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQR/IVzF9z37ZgW8cbrnbk4xtvg  qC82Ww9mqs89HmJ8tbAH+NAxEBcoEojp9Diq+3R+zmtoQ3ZKyVlfjspGrPO1jU8r  Ioekb4Vu21tBUJRdf9NjQ31QMQ+wLTvluLdhxgOjggEmMIIBIjAMBgNVHRMBAf8E  AjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDAmBgNVHREEHzAdgRtt  YXR0aGV3X3NvcmljaEBzeW1hbnRlYy5jb20wDgYDVR0PAQH/BAQDAgOIMEIGA1Ud  IAQ7MDkwNwYLYIZIAYb4RQEHFwIwKDAmBggrBgEFBQcCARYaaHR0cDovL3d3dy5z  eW1hdXRoLmNvbS9jcHMwNwYDVR0fBDAwLjAsoCqgKIYmaHR0cDovL2NybC53cy5z  eW1hbnRlYy5jb20vcGNhMi1nNC5jcmwwHQYDVR0OBBYEFMj6cCTbhvdmDN8xhVpx  fMUNJ3mpMB8GA1UdIwQYMBaAFD0y8zqpDJCE+aKMaQZhVC+Hcv4FMAoGCCqGSM49  BAMDA2kAMGYCMQDsLerJJOYgrlAnYabMe+5bM+GogQrlwejIMLb0OHHYpa4E4bpg  fJCO+CsCprSId38CMQC2rtxXrxosTHWV5FmNAmgurqkl3jO3TX1K7+ax9FItd30r  5/NBdqf9UPD3hkmU2XM=  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca2-g4.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 1 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 3 Public Primary Certification Authority - G4 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 3 Public Primary Certification Authority - G4 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 58d52db93301a4fd291a8c9645a08fee7f529282 |
| Valid From | 2012-10-18 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA384WithECC |
| Signing key parameters | ECC p384 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://ssltest36.ssl.symclab.com> |
| CRL URL | URL: <http://crl.ws.symantec.com/symc-pca3-g4.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  *a) Browsing to test website with OCSP enforced in Firefox browser* – No warning when visiting site.  *b) If requesting EV:* - No green bar. Kathleen says ECC not yet fully enabled in Firefox due to patent concerns. |
| Requested Trust Bits | Websites (SSL/TLS)  Email (S/MIME)  Code Signing |
| SSL Validation Type | OV, and/or EV |
| EV Policy OID(s) | 2.16.840.1.113733.1.7.23.6 |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 3 Root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 1 Public Primary Certification Authority - G6 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 1 Public Primary Certification Authority - G6 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 517f611e29916b5382fb72e744d98dc3cc536d64 |
| Valid From | 2011-10-18 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithRSA |
| Signing key parameters | RSA 2048 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIFJjCCBA6gAwIBAgIQRfVp5hxRUV7ThmXEUa89eDANBgkqhkiG9w0BAQsFADCB  lDELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMR8w  HQYDVQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMUUwQwYDVQQDEzxTeW1hbnRl  YyBDbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5  IC0gRzYwHhcNMTIxMTA2MDAwMDAwWhcNMTQxMTA1MjM1OTU5WjCB3jELMAkGA1UE  BhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDU1vdW50YWluIFZp  ZXcxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMUEwPwYDVQQLEzhGT1Ig  VEVTVCBQVVJQT1NFUyBPTkxZIC0gQ2xhc3MgMSBSU0EtU0hBMjU2IFRlc3QgRUUg  Q2VydDFAMD4GA1UEAxM3U3ltYW50ZWMgQ2xhc3MgMSBUZXN0IFJTQS1TSEEyNTYg  RW5kIEVudGl0eSBDZXJ0aWZpY2F0ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC  AQoCggEBANNAFkbTX5nVThJqT+Zb4o9VS5xqT0S5cJU72LrMc7ZKM9JTpY6jTyUo  ubzX371R8+j7uHJiJd4Oek5rvQrgMpKM34yJ2ysEJ0fKilL1XM4jhubvP7nZuD3Q  JNcNmsV5/azuHIWkgptv8+RwylzOZF1N200MoPmlFEwPdmHgxGWtntDMKrFqv0Nb  hocUwS02BtOyCTWWu+4aaNPEpJ06pB1mVxgQfehvT+GCTnT81VnnCwkHLo7R6q9B  lI2hia48rGXifpuFE+19A1sPfIw89cB5WN63jgsLlyIsjf3FZJWqnBawAFyH+SRf  FMjinhws4kyo2tiu12bK+L6pnpNyHTkCAwEAAaOCASYwggEiMAwGA1UdEwEB/wQC  MAAwQgYDVR0gBDswOTA3BgtghkgBhvhFAQcXATAoMCYGCCsGAQUFBwIBFhpodHRw  Oi8vd3d3LnN5bWF1dGguY29tL2NwczA3BgNVHR8EMDAuMCygKqAohiZodHRwOi8v  Y3JsLndzLnN5bWFudGVjLmNvbS9wY2ExLWc2LmNybDAdBgNVHSUEFjAUBggrBgEF  BQcDAgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgeAMCYGA1UdEQQfMB2BG21hdHRo  ZXdfc29yaWNoQHN5bWFudGVjLmNvbTAdBgNVHQ4EFgQUoAJwwLobFTuEWGxLqp8L  2z8ZBtowHwYDVR0jBBgwFoAUM0HoyDkSFZNI8pYyLlr12pRfU2AwDQYJKoZIhvcN  AQELBQADggEBALWacay5XJCdwcDMh1sGCqwCBgPne5FNPVcj3MBnuMUnNXxX8/+V  /UoLYzhdm1Uf/WUJbTOk1Y5Qb8DNGTj/cdG7NY4tm5g5UJshz7n32ueefCJe18+v  qldp2EnAVXR/OBwScMvE8iKjriMd82WAq7AN4d92xjEROuA4Js8OWDK7ybIt7xKT  x5rqH4SFzYQ1bGyp5D3EhQE0Sm1fyE4mOf4zjJIU/SWt3cSXMRIjgMuVxtgF12hd  UUJlvME+z0GBedbzQV0OgMaY8wF/kNL+4xp+iflQZ6/hLdAFvOx/QEYBS0qlSSEa  rPExohT0xQEh6jJ6AmKFIk8XMLIjmoTBbUU=  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca1-g6.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 1 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 2 Public Primary Certification Authority - G6 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 2 Public Primary Certification Authority - G6 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 40b331a0e9bfe855bc3993ca704f4ec251d41d8f |
| Valid From | 2011-10-18 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA256WithRSA |
| Signing key parameters | RSA 2048 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | -----BEGIN CERTIFICATE-----  MIIFIDCCBAigAwIBAgIQCLfFrS1dgSkGh4yHftLsqzANBgkqhkiG9w0BAQsFADCB  lDELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMR8w  HQYDVQQLExZTeW1hbnRlYyBUcnVzdCBOZXR3b3JrMUUwQwYDVQQDEzxTeW1hbnRl  YyBDbGFzcyAyIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5  IC0gRzYwHhcNMTIxMTA2MDAwMDAwWhcNMTQxMTA1MjM1OTU5WjCB2DELMAkGA1UE  BhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDU1vdW50YWluIFZp  ZXcxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcmF0aW9uMT4wPAYDVQQLEzVGT1Ig  VEVTVCBQVVJQT1NFUyBPTkxZIC0gQ2xhc3MgMiBSU0EtMjU2IFRlc3QgRUUgQ2Vy  dDE9MDsGA1UEAxM0U3ltYW50ZWMgQ2xhc3MgMiBUZXN0IFJTQS0yNTYgRW5kIEVu  dGl0eSBDZXJ0aWZpY2F0ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  ALVxgqmJAN+9wCuBd4CHZXgn3eKVvSAdlGwOpShAEkB1GTT9To3YogbZL4hXh0wt  n0zC8RPAoB4i5K6xZ1zEs4VpS+Oyau1gxhRHeaHtVuz132Gd5hkALobRZjRJvLOk  V1vl79qdqheeHjTGfPdqYVzrJHvZljRWOF+4j58CT8fH5jFTBA5DXUVhkXY4H1zC  yP5cykS1Z2Lva944Nx7uwQrETH5Zg2VKboKyEAXYCI30+xXLRz+UiSOlVwC3n6zR  pd5sUTa8ObhjTN0KgMqwEx1WgnJHLLaKIpDlR8GtK3ZSw9zg/wIyh+8IivBt892K  wWm2ryoIlG1filRYXvvAHvMCAwEAAaOCASYwggEiMAwGA1UdEwEB/wQCMAAwHQYD  VR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIHgDAmBgNV  HREEHzAdgRttYXR0aGV3X3NvcmljaEBzeW1hbnRlYy5jb20wQgYDVR0gBDswOTA3  BgtghkgBhvhFAQcXAjAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LnN5bWF1dGgu  Y29tL2NwczA3BgNVHR8EMDAuMCygKqAohiZodHRwOi8vY3JsLndzLnN5bWFudGVj  LmNvbS9wY2EyLWc2LmNybDAdBgNVHQ4EFgQUn9LvDTTwCflDK4Plz958mHODijAw  HwYDVR0jBBgwFoAUh4wglciYStHWgAZKkDRE3xxNv7AwDQYJKoZIhvcNAQELBQAD  ggEBABJnLyShr7OYZ1XK3iCdzTpa/3qsLS/ds8YphwU9FsynbJXfAuoLJsbOM0O/  awA5mc91aVr5EcFfirsHlTsGYU1e82d4pJCJ9fkJ2VV3Io2SDtfM59Fl9pOApnXu  ax8xzQhu/jkiZtQ/Lc/IL4+QFXf7EySuGs0p5hSdF7BmnGI6HFWz3dXYGSdxQM3C  HKydQJmVzcvliM/Qxyq3pNpQwmdgF8qlbH/p80zcojppoCKjb11kiQPmwR5pu48r  qCZFj0XVQmm1Tj4JwWJn9N2mP2K6bMbvMpv52asnyeV9x0pqfnFEjxt4zLjNTPNl  vGIgEiyZqnvkt8soWVn81rLCVTo=  -----END CERTIFICATE----- |
| CRL URL | URL: <http://crl.ws.symantec.com/pca2-g6.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  OCSP service will not be enabled until the Root is placed into Production use.  *Maximum expiration time of OCSP responses*: 7 days  *Testing results*  This root is intended for email only. |
| Requested Trust Bits | Email (S/MIME) |
| SSL Validation Type | n/a |
| EV Policy OID(s) | n/a |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 2 Root will be used to issue internally-operated SubCAs which will issue SMIME and clientAuth certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Symantec Class 3 Public Primary Certification Authority - G6 |
| Certificate Issuer Field | Country = US  Organization = Symantec Corporation  Organizational Unit = Symantec Trust Network  Common Name = Symantec Class 3 Public Primary Certification Authority - G6 |
| Certificate Summary | Root is offline. Used only to issue SubCAs, CRLs every quarter (or as needed), and OCSP certificates. |
| Root Cert URL | <http://www.verisign.com/support/roots.html> |
| SHA1 Fingerprint | 26a16c235a2472229b23628025bc8097c88524a1 |
| Valid From | 2012-10-18 |
| Valid To | 2037-12-01 |
| Certificate Version | 3 |
| Certificate Signature Algorithm | SHA384WithRSA |
| Signing key parameters | RSA 4096 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://ssltest38.ssl.symclab.com> |
| CRL URL | URL: <http://crl.ws.symantec.com/pca3-g6.crl> |
| OCSP URL | URL: <http://ocsp.ws.symantec.com> (not yet enabled for this Root)  *Maximum expiration time of OCSP responses:* 7 days  *Testing results*   1. *Browsing to test website with OCSP enforced in Firefox browser*    1. This results in a Minefield error: “The connection to the server was reset while the page was loading.” Is RSA 4096 supported?   *b) If requesting EV*: Gives warning when trying to load the page hence it seems it does not recognize the root. Hence of course No green bar is available. |
| Requested Trust Bits | Websites (SSL/TLS)  Email (S/MIME)  Code Signing |
| SSL Validation Type | OV, and/or EV |
| EV Policy OID(s) | 2.16.840.1.113733.1.7.23.6 |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Our Class 3 Root will be used to issue internally-operated SubCAs which will issue CodeSigning, SSL, and TimeStamping certificates. |
| Externally Operated SubCAs | This root does not and will not have any subCAs that are operated by external third parties. |
| Cross-Signing | n/a |
| Technical Constraints on  Third-party Issuers | No third parties can issue certificates signed by this root. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | *Language(s) that the documents are in*: English, Japanese  CP: <http://www.verisign.com/repository/vtnCp.html>  CPS in English: <http://www.verisign.com/repository/CPS/>  CPS in Japanese: <http://www.verisign.co.jp/repository/CPS/> Relying Party Agreement: <http://www.verisign.com/repository/rpa/index.html> |
| Audits | Audit Type: WebTrust for CA  Auditor: KPMG  Auditor Website: https://cert.webtrust.org/  URL to Audit Report and Management’s Assertions: <http://www.verisign.com/repository/> under “Additional Resources” |
| Baseline Requirements (SSL) | *What is your status in regards to complying with the CAB Forum Baseline Requirements? (*[*https://www.cabforum.org/Baseline\_Requirements\_V1.pdf*](https://www.cabforum.org/Baseline_Requirements_V1.pdf)*)* Since 1 July, 2012, Symantec has issued certificates in full compliance with the CAB Forum Baseline Requirements.  *As per the CAB Forum Baseline Requirement # 8.3, where is the “Commitment to Comply” statement that should be in your CP or CPS?* In Section 1, Introduction, of the CPS. |
| SSL Verification Procedures | *If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.*    + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2Initial Identity Validation * If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification.   + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2.1 CABF Verification Requirements for Organization Applicants. The list includes “admin‟, “administrator‟, “webmaster‟, “hostmaster‟, and “postmaster‟. * *Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).* We confirm that we have such automatic blocks in place.   + *Specify the procedure for additional verification of a certificate request that is blocked*. If our automatic check detects a high-profile domain name, it flags the order for manual review. A trained Authentication Specialist must review the order details and clear the flag if the order is legitimate. * *If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.*    + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2Authentication of Organization Identity * If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.   + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Appendix B1 |
| Organization Verification Procedures | See above |
| Email Address Verification Procedures | *If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.3 Authentication of Individual Identity |
| Code Signing Subscriber Verification Procedures | *If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)   * *URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence.*   + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2Authentication of Organization Identity |
| Multi-factor Authentication | *Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.*   * *For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to username/password?* Yes. * *Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.* Client certificate and username/password are required. * *This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.* This applies to all accounts that can cause the approval and/or issuance of end-entity certificates. * *If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.* No additional technical controls are used for those accounts.   + See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 6.5.1.1CABF Requirements for System Security |
| Network Security | *Confirm that you have performed the actions listed in #7 of* [*https://wiki.mozilla.org/CA:Information\_checklist#Verification\_Policies\_and\_Practices*](https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices)  *Confirm that you have done the following, and will do the following on a regular basis:*   * *Check for mis-issuance of certificates, especially high-profile domains.* * *Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.* * *Ensure Intrusion Detection System and other monitoring software is up-to-date.* * *Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.*   We confirm that we have done the above, and continue to do them on a regular basis. |

**Response to Mozilla's CA Recommended Practices** (<https://wiki.mozilla.org/CA:Recommended_Practices>)

|  |  |
| --- | --- |
| [Publicly Available CP and CPS](https://wiki.mozilla.org/CA:Recommended_Practices#Publicly_Available_CP_and_CPS) | See above |
| [CA Hierarchy](https://wiki.mozilla.org/CA:Recommended_Practices#CA_Hierarchy) | <http://www.verisign.com/repository/root.html>, [http://www.verisign.com/repository/ca-ra.html](http://www.verisign.com/repository/ca-ra.html%20) and <http://www.verisign.com/repository/hierarchy/hierarchy.pdf> |
| [Audit Criteria](https://wiki.mozilla.org/CA:Recommended_Practices#Audit_Criteria) | See above (**Verification Policies and Practices:** Audits) |
| [Document Handling of IDNs in CP/CPS](https://wiki.mozilla.org/CA:Recommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS) | Symantec’s automated domain ownership process uses various ‘whois’ services to find the owner of a particular domain. We believe that in most cases of homographic spoofing, that automated process will fail, resulting in the order being flagged for manual review. Our authentication representatives who perform manual review are trained to reject any domain name made up of multiple scripts within one domain name label.  Symantec actively participates in the CA/Browser Forum, which has recently debated standards for IDN certificates. We intend to fully comply with whatever standards are drafted by that body.  Symantec will update its CPS by March 31, 2012 to reflect this policy. |
| [Revocation of Compromised Certificates](https://wiki.mozilla.org/CA:Recommended_Practices#Revocation_of_Compromised_Certificates) | See Section 4.9 Certificate Revocation and Suspension in each CPS mentioned above. |
| [Verifying Domain Name Ownership](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership) | * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2.1CABF Verification Requirements for Organization Applicants |
| [Verifying Email Address Control](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control) | See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.3 Authentication of Individual Identity |
| [Verifying Identity of Code Signing Certificate Subscriber](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber) | * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2Authentication of Organization Identity |
| [DNS names go in SAN](https://wiki.mozilla.org/CA:Recommended_Practices#DNS_names_go_in_SAN) | * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.1.1.1 CABF Naming Requirements |
| [Domain owned by a Natural Person](https://wiki.mozilla.org/CA:Recommended_Practices#Domain_owned_by_a_Natural_Person) | Mozilla’s recommendation conflicts with CAB Forum’s Baseline Requirements (<https://cabforum.org/Baseline_Requirements_V1_1.pdf>) Section 9.2.4 Subject Distinguished Name Fields. Symantec complies with the latest version of the CAB Forum Baseline Requirements. |
| [OCSP](https://wiki.mozilla.org/CA:Recommended_Practices#OCSP) | Symantec provides OCSP support for all certificates. OCSP service is updated at least every 3.5 days, and OCSP responses are valid for no more than 7 days. |

**Response to Mozilla's list of Potentially Problematic Practices** (<https://wiki.mozilla.org/CA:Problematic_Practices>)

|  |  |
| --- | --- |
| [Long-lived DV certificates](https://wiki.mozilla.org/CA:Problematic_Practices#Long-lived_DV_certificates) | Symantec complies with section 6 of the Mozilla CA Certificate Inclusion Policy |
| [Wildcard DV SSL certificates](https://wiki.mozilla.org/CA:Problematic_Practices#Wildcard_DV_SSL_certificates) | Symantec does not issue such certificates under its Symantec or VeriSign brands |
| [Email Address Prefixes for DV Certs](https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs) | * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 3.2.2.1CABF Verification Requirements for Organization Applicants * When using the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, Symantec uses a mail system address formed in one of the following ways:   + 1. Supplied by the Domain Name Registrar;   + 2. Taken from the Domain Name Registrant‟s “registrant”, “technical”, or “administrative” contact information, as it appears in the Domain‟s WHOIS record; or;   + 3. By pre-pending a local part to a Domain Name as follows:     - a. Local part - One of the following: “admin”, “administrator”, “webmaster”, “hostmaster”, or “postmaster”; and     - b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name. |
| [Delegation of Domain / Email validation to third parties](https://wiki.mozilla.org/CA:Problematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties) | * See <http://www.verisign.com/repository/CPSv3.8.10_final.pdf> Section 1.3.2 Registration Authorities   Symantec does not delegate the RA functions for EV Code Signing Certificates. |
| [Issuing end entity certificates directly from roots](https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_end_entity_certificates_directly_from_roots) | With the exception of a very limited number of certificates for test purposes, Symantec does not issue end entity certificates directly from its Symantec-branded or VeriSign-branded roots. |
| [Allowing external entities to operate subordinate CAs](https://wiki.mozilla.org/CA:Problematic_Practices#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. |
| [Distributing generated private keys in PKCS#12 files](https://wiki.mozilla.org/CA:Problematic_Practices#Distributing_generated_private_keys_in_PKCS.2312_files) | Symantec does not engage in this problematic practice. |
| [Certificates referencing hostnames or private IP addresses](https://wiki.mozilla.org/CA:Problematic_Practices#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](https://wiki.mozilla.org/CA:Problematic_Practices#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. |
| [OCSP Responses signed by a certificate under a different root](https://wiki.mozilla.org/CA:Problematic_Practices#OCSP_Responses_signed_by_a_certificate_under_a_different_root) | Symantec does not sign OCSP responses under a different root. |
| [CRL with critical CIDP Extension](https://wiki.mozilla.org/CA:Problematic_Practices#CRL_with_critical_CIDP_Extension) | Symantec issues only “full” CRLs. |
| [Generic names for CAs](https://wiki.mozilla.org/CA:Problematic_Practices#Generic_names_for_CAs) | Symantec does not use generic names in its root and intermediate CA certificates. |
| [Lack of Communication With End Users](https://wiki.mozilla.org/CA:Problematic_Practices#Lack_of_Communication_With_End_Users) | Symantec maintains a continuous 24x7 ability to accept and respond to certificate problem reports via Technical Support numbers, posted prominently on all corporate web portals. |