Bugzilla ID: 833974
Bugzilla Summary: Enable EV for existing VeriSign ECC root

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.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. 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	http://www.symantec.com http://www.verisign.com
Organizational type	Symantec is a major commercial CA with worldwide operations and customer base.
Primark Market / Customer Base	Symantec acquired the VeriSign Authentication Services and root certificates, and is a major commercial CA with worldwide operations and customer base.
CA Contact Information	CA Email Alias: DL-ENG-Root-Certificate-Management@symantec.com CA Phone Number: 650-527-7181 Title / Department: Senior Product Manager, Enterprise Security Group

Technical information about each root certificate

Certificate Name	VeriSign Class 3 Public Primary Certification Authority - G4
Certificate Issuer Field	CN = VeriSign Class 3 Public Primary Certification Authority - G4 OU = "(c) 2007 VeriSign, Inc. - For authorized use only" OU = VeriSign Trust Network O = "VeriSign, Inc." C = US
Certificate Summary	This request is to enable EV treatment for the "VeriSign Class 3 Public Primary Certification Authority - G4" root certificate that was included via bug #409235. Root is offline. Used only to issue internally-operated SubCAs, CRLs every quarter (or as needed), and OCSP certificates.
Root Cert URL	http://www.verisign.com/repository/roots/root-certificates/PCA-3G4.pem
SHA1 Fingerprint	22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
Valid From	2007-11-05
Valid To	2038-01-18
Certificate Version	3
Cert Signature Algorithm	SHA384withECC
Signing key parameters	NIST P-384
Test Website URL (SSL)	https://ssltest35.ssl.symclab.com/ Please complete the EV Testing described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version, and attach a screenshot showing successful completion of the EV testing to the bug.
CRL URL	http://crl.ws.symantec.com/pca3-g4.crl

	http://SVR256SecureECC-crl.ws.symantec.com/SVR256SecureECC.crl (nextUpdate: 10 days)
OCSP URL	http://ocsp.ws.symantec.com http://EV256SecureECC-ocsp.ws.symantec.com
CRL nextUpdate and OCSP max expiration	CPS Appendix B1, Section 26: For EV Certificates: (A) CRLs are be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days; or (B) Symantec's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days
Requested Trust Bits	All three trust bits are already enabled for this root cert. Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV, and EV
EV Policy OID(s)	2.16.840.1.113733.1.7.23.6

CA Hierarchy information for each root certificate

CA Hierarchy	This 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	None and none planned.
Technical Constraints on Third-party Issuers	No third parties can issue certificates signed by this root.

Verification Policies and Practices

Policy Documentation	Documents are in English and Japanese. CP: http://www.verisign.com/repository/vtnCp.html CPS : http://www.verisign.com/repository/CPS/ Relying Party Agreement: http://www.verisign.com/repository/rpa/index.html
Audits	Audit Type: WebTrust for CA and WebTrust EV Auditor: KPMG, http://www.kpmg.com/ Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=304&file=pdf (2011.11.30) Need update audit statements. This document contains three audit reports and the corresponding management assertions.
Baseline Requirements (SSL)	CP section 1: STN Certificate Policy also adopts the current version of the CA/Browser Forum requirements as set forth in the following documents: · Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, · Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, · Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Organization Verification Procedures	CPS Table 2: Only Class 3 and Class 3 EV Certificates can be used for SSL/TLS. CPS Section 1.4.1: High assurance certificates are individual and organizational Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2. High assurance with extended validation certificates are Class 3 certificates issued by Symantec in conformance with the Guidelines for Extended Validation Certificates. CPS Section 3.2.2, Authentication of Organization identity, provides the details for verifying the identity of the certificate subscriber.
SSL 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. CPS Section 1.4.1.2, Certificates issued to Organizations: Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. 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.
EV	CPS Appendix B1 Section18, Verification of Applicant's Domain Name CPS Appendix B1, Section 3, EV Certificate Warranties and Representations Right to Use Domain Name: Symantec has taken all steps reasonably necessary in terms of the Guidelines to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate owns or has the exclusive right to use the domain name(s) listed in the EV Certificate;
Email Address Verification Procedures	Email certs can be issued for Class 1, 2, and 3 verification levels, for both individuals and organizations. The absolute minimum verification is for Class 1 individual. CPS 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. CPS section 3.2.3, Class 2 individual: Authenticate identity by matching the identity provided by the Subscriber to: 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 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
Code Signing Subscriber Verification Procedures	CPS Section 1.4.1: According to table 2, only Class 3 (High Assurance) certificates can be used for Code Signing. See section 3.2.2 for procedures to verify identity, authority, and organization.
Multi-factor Authentication	CPS section 5.2 Client certificate and username/passwords are required for all accounts that can cause the approval and/or issuance of end entity certificates.
Network Security	CPS section 6.7

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

Publicly Available CP and CPS	Yes
CA Hierarchy	http://www.verisign.com/repository/root.html,, http://www.verisign.com/repository/ca-ra.html and http://www.verisign.com/repository/hierarchy/hierarchy.pdf
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	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.
Revocation of Compromised Certificates	CPS section 4.9
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	CPS section 7.1.2.3
Domain owned by a Natural Person	SSL certs are only issued to organizations.
OCSP	Yes

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

Long-lived DV certificates	SSL certs under this root will be OV/EV. CPS section 6.3.2: Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to six years, if the following requirements are met: … Subscribers are required to undergo re-authentication at least every 3 years under section 3.2.3.
Wildcard DV SSL certificates	Symantec does not issue such certificates under its Symantec or VeriSign brands.
Email Address Prefixes for DV Certs	SSL certs under this root are OV/EV.
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. Does this include SSL cert issuance? Does this include EV SSL cert issuance?
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	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	Symantec does not engage in this problematic practice.
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.
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	Symantec issues only "full" CRLs.
Generic names for CAs	CN includes VeriSign
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.