Print this page

Mozilla - CA Program

Case Information

Case Number	00000045	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Symantec / VeriSign	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Enable EV for VeriSign ECC root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=833974

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	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 are asking why certs chaining to this root do not get EV treatment, when other browsers show EV treatment.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* CA Hierarchy: See https://www.symantec.com/about/profile/policies/repository.jsp Roots tab * CPS 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	**Verified?**	Verified

name that visually appears to be made up of multiple scripts within one hostname label.
Symantec actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and fully commits to conforming with standards drafted by that body.

* Revocation of Compromised Certificates -- CPS section 4.9

* DNS names go in SAN -- CPS section 7.1.2.3

* Domain owned by a Natural Person -- SSL certs are only issued to organizations.

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 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 STN CA. Third party RAs must abide by all the requirements of the STN CP, the STN CPS and the terms of their enterprise services agreement with Symantec. RAs may, however implement more restrictive practices based on their internal requirements. * Allowing external entities to operate subordinate CAs -- CPS section 1.3.1: Symantec enterprise customers may operate their own CAs as subordinate CAs to a public STN PCA. Such a customer enters into a contractual relationship with Symantec to abide by all the requirements of the STN CP and the STN CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements. * Certificates referencing hostnames or private IP addresses -- Symantec fully complies with the CAB Forum Baseline Requirements concerning certificates with non-FQDN or private IP addresses. * Issuing SSL Certificates for Internal Domains -- Symantec's Authentication Team is aware that .int is a valid TLD. Symantec has issued certificates to .int, and we have verified that the subscriber owns the domain name. Symantec correctly identifies internal and external domain names and verifies that subscribers own/control the domain name to be included in their certificate.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	VeriSign Class 3 Public Primary Certification Authority - G4	**Root Case No**	R00000060
Request Status	Ready for Public Discussion	**Case Number**	00000045

Additional Root Case Information

Subject	Enable EV Treatment for VeriSign Class 3 G4 ECC root

Technical Information about Root Certificate

O From Issuer Field	VeriSign, Inc."	**Verified?**	Verified
OU From Issuer Field	VeriSign Trust Network	**Verified?**	Verified
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, OCSP certs.	**Verified?**	Verified
Root Certificate Download URL	Already Included	**Verified?**	Verified
Valid From	2007 Nov 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	https://ssltest35.ssl.symclab.com/	**Verified?**	Verified
CRL URL(s)	http://crl.ws.symantec.com/pca3-g4.crl http://EV256SecureECC-crl.ws.symantec.com/EV256SecureECC.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.ws.symantec.com http://EV256SecureECC-ocsp.ws.symantec.com	**Verified?**	Verified
Revocation Tested	https://certificate.revocationcheck.com/ssltest35.ssl.symclab.com No errors	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.840.1.113733.1.7.23.6	**Verified?**	Verified
EV Tested	// 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 "2.16.840.1.113733.1.7.23.6", "VeriSign EV OID", SEC_OID_UNKNOWN, { 0x69, 0xDD, 0xD7, 0xEA, 0x90, 0xBB, 0x57, 0xC9, 0x3E, 0x13, 0x5D, 0xC8, 0x5E, 0xA6, 0xFC, 0xD5, 0x48, 0x0B, 0x60, 0x32, 0x39, 0xBD, 0xC4, 0x54, 0xFC, 0x75, 0x8B, 0x2A, 0x26, 0xCF, 0x7F, 0x79 }, "MIHKMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNV" "BAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxOjA4BgNVBAsTMShjKSAyMDA3IFZl" "cmlTaWduLCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxRTBDBgNVBAMT" "PFZlcmlTaWduIENsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBB" "dXRob3JpdHkgLSBHNA==", "L4D+I4wOIg9IZxIokYessw==", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A	**Verified?**	Verified
SHA-256 Fingerprint	69:DD:D7:EA:90:BB:57:C9:3E:13:5D:C8:5E:A6:FC:D5:48:0B:60:32:39:BD:C4:54:FC:75:8B:2A:26:CF:7F:79	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root signs internally-operated SubCAs which issue OV and EV SSL certificates, as well as S/MIME and Code Signing certificates.	**Verified?**	Verified
Externally Operated SubCAs	None. None planned.	**Verified?**	Verified
Cross Signing	None. None planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No third parties can issue certificates signed by this root.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	The CPS 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	https://cert.webtrust.org/SealFile?seal=1565&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/5/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1565&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified

EV Audit Statement Date	5/5/2015	**Verified?**	Verified
BR Commitment to Comply	STN-CP and STN-CPS section 1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.3: Symantec uses the following methods of vetting a domain name, with option 1 being the primary method: 1. Confirm the Applicant as the Domain Name Registrant directly with the Domain Name Registrar by performing a whois look up. 2. Communicate directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Rely upon a Domain Authorization Document; 4. Communicate directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 5. Communicate with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; 6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN.	**Verified?**	Verified
EV SSL Verification Procedures	CPS sections 3.1.1.1, 3.2.2.1, 4.1.2.2, 4.3.3, 4.9.1.1, 4.9.3.2: EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively. CPS section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain. For Organization Validated (OV) and Extended Validation (EV) Certificates domain validation is completed in all cases along with Organizational validation. Symantec's procedures for issuing EV SSL Certificates are described in Appendix B1 to this CPS. Appendix B1, and Appendix D all just say: The current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates can be accessed at https://cabforum.org/baseline-	**Verified?**	Verified

	requirements-documents/ EV SSL certificate content and profile requirements are discussed in Section 6 of Appendix B3 to this CPS.		
Organization Verification Procedures	CPS Section 1.4.1: According to tables 1 and 2, only Class 3 certificates issued to organizations can be used for SSL and Code Signing. Therefore all SSL certs are of OV or EV verification type. CPS Section 3.2.2: Authentication of Organization Identity CPS section 3.2.3: Authentication of Individual Identity CPS section 3.2.5: Validation of Authority	**Verified?**	Verified
Email Address Verification Procedures	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. STN-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. 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 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. See CPS sections 3.2.2, 3.2.3, and 3.2.5.	**Verified?**	Verified
Multi-Factor Authentication	STN-CPS section 5.2.2	**Verified?**	Verified
Network Security	STN-CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

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