Bugzilla ID: 602107
Bugzilla Summary: Turn on the code signing and email trust bits for the VeriSign Class 3 Public Primary Certification Authority - G5
CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Symantec VeriSign Authentication Services
Website URL	http://www.symantec.com http://www.verisign.com
Organizational type	Commercial
Primary 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	practices@verisign.com, 650.961.7500, Certificate Policy Manager

Info Needed	Data
Certificate Name	VeriSign Class 3 Public Primary Certification Authority - G5
Cert summary / comments	Request is to turn on the email and code signing trust bits for this root, which was approved for inclusion in bug #402947.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=304810
SHA-1 fingerprint	4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5
Valid from	2006-11-07
Valid to	2036-07-16
Cert Version	3
Modulus length	2048
Test Website	https://www.verisign.com
CRL URL	http://evintl-crl.verisign.com/EVIntl2006.crl CPS section 4.9.7: CRLs for end-user Subscriber Certificates are issued at least once per day.
OCSP Responder URL	http://evintl-ocsp.verisign.com/
CA Hierarchy	CA Hierarchy Diagram: http://www.verisign.com/repository/hierarchy/hierarchy.pdf This root has the following internally-operated sub-CAs: - VeriSign Extended Validation SSL CA - VeriSign Extended Validation SSL SGC CA - VeriSign Secure Server CA – G3 - VeriSign Class 3 Code Signing 2010 CA - VeriSign Class 3 International Server CA – G3 - Thawte SGC CA - G2
Externally operated subCAs	None

Cross-Signing	For compatibility reasons Symantec has implemented a cross-signing scheme involving the VeriSign Class 3 Public Primary CA - G5. In this scheme, if applications not supporting EV functionality (e.g., Firefox 2 and earlier) encounter VeriSign EV certificates then they will end up treating the CA as a subordinate CA under the existing VeriSign Class 3 Public Primary CA root.
Requested Trust Bits	Websites (already enabled) Email Code Signing
SSL Validation Type	OV, EV 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.
EV policy OID(s)	2.16.840.1.113733.1.7.23.6
CP/CPS	CPS: http://www.verisign.com/repository/CPS/ CP: http://www.verisign.com/repository/vtnCp.html
AUDIT	Auditor: KPMG Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=304&file=pdf (2009.11.30)
Organization Identity Verification	See Section 3.2.2 of the CPS. See Section 3.2.3 (Class 3) for authentication of individual identity. For EV see Section B1 of the CPS, sub-sections F. 14, 15, 16, and 17.
Domain Name Ownership / Control	For EV see Section B1 of the CPS, sub-section F.18. 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.
Email Address Ownership / Control	CPS Section 1.4.1: According to tables 1 and 2, S/MIME certificates may be issued to individuals or organizations according to Class 1, 2, or 3 assurance levels. CPS section 1.4.2.1: 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 1.4.1.3: Low assurance (Class 1) certificates are certificates that should not be used for authentication purposes or to support non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The certificate, however, provides no proof of the identity of the subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate. 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
Identity of Code Signing Subscriber	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. CPS Section 3.2, Authentication of Organization Identity Table 6, Additional Procedures: Before Symantec digitally signs any content using ACS it authenticates that the content is the original content signed by the Organization using its Code Signing Certificate. CPS Section 3.2.5: Validation of Authority

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• 1.1 Long-lived DV certificates
	  ○ SSL certs are 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.
	• 1.2 Wildcard DV SSL certificates
	  ○ SSL certs are OV/EV
	  ○ The only mention of wildcard certs in the CPS is to state that wildcard certificates are not allowed for EV certificates.
	• 1.3 Email Address Prefixes for DV Certs
	  ○ SSL certs are OV/EV
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ From Audit: "For the VeriSign/RSA Secure Server CA, VeriSign International Server CA – Class 3, VeriSign Class 3 Secure Server CA, VeriSign Class 3 Secure Server CA – G2, and VeriSign Class 3 Public Primary Certification Authority – G5, Symantec makes use of external registration authorities for specific subscriber registration activities as disclosed in the VTN CPS on Symantec's VeriSign website. Our examination did not extend to the controls of external registration authorities."
	• 1.5 Issuing end entity certificates directly from roots
	  ○ Roots are offline, and only sign intermediate certificates.
	• 1.6 Allowing external entities to operate subordinate CAs
	  ○ No externally-operated subCAs are planned to be issued under this root.
	• 1.7 Distributing generated private keys in PKCS#12 files
	  ○ CPS Section 3.2.1, Method to Prove Possession of Private Key: The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another Symantec-approved method.

	This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pregenerated keys are placed on smart cards.
	• 1.8 Certificates referencing hostnames or private IP addresses
	  ○ Non EV certificates may contain host names after verification with the organization. IP addresses verified to be within the private range may be refenced in Standard Intranet and Premium Intranet Certificates.
	  ○ CPS section 3.2.2, Table 6: Symantec verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber.
	• 1.9 Issuing SSL Certificates for Internal Domains
	  ○ Non EV certificates may contain internal domains.
	• 1.10 OCSP Responses signed by a certificate under a different root
	  ○ Not applicable
	• 1.11 CRL with critical CIDP Extension
	  ○ Not applicable
	• 1.12 Generic names for CAs
	  ○ CA names include VeriSign