Bugzilla ID: 602107
Bugzilla Summary: Turn on the code signing trust bit 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	VeriSign
Website URL	http://www.verisign.com
Organizational type	Commercial
Primary market / customer base	VeriSign is a major commercial CA with worldwide operations and customer base.
CA Contact Information	CA Email Alias: practices@verisign.com CA Phone Number: 650.961.7500 Title / Department: Certificate Policy Manager

Info Needed	Data
Certificate Name	VeriSign Class 3 Public Primary Certification Authority - G5
Cert summary / comments	This request is to enable the code signing trust bit for this root. This root 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	Please provide a URL to a website whose EV SSL cert chains up to this root.
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/ What is the max expiration time of the OCSP responses? CA/B Forum EV Guidelines Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."

CA Hierarchy	CA Hierarchy Diagram: http://www.verisign.com/repository/hierarchy/hierarchy.pdf This diagram shows that this root has the following 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 Are these all of the sub-CAs signed by this root?
Externally operated subCAs	Does this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (already enabled) 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/
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. 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 VeriSign 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	Not requesting email trust bit.
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 3.2.2: Authentication of Organization CPS Section 3.2.5: Validation of Authority
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information. • 1.1 Long-lived DV certificates ○ SSL certs are OV/EV

	• 1.2 Wildcard DV SSL certificates
	  ○ SSL certs are OV/EV
	• 1.3 Email Address Prefixes for DV Certs
	  ○ SSL certs are OV/EV
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ ?
	• 1.5 Issuing end entity certificates directly from roots
	  ○ Root signs intermediate CAs which sign the end-entity certs.
	• 1.6 Allowing external entities to operate subordinate CAs
	  ○ ?
	• 1.7 Distributing generated private keys in PKCS#12 files
	  ○ ?
	• 1.8 Certificates referencing hostnames or private IP addresses
	  ○ ?
	• 1.9 Issuing SSL Certificates for 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