Bugzilla ID: 536318
Bugzilla Summary: EV enable VeriSign ECC and SHA256 root certificates

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	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 An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. **CA Phone Number:** 1 650.961.7500 **Title / Department:** The Certificate Policy Manager

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

	SHA 256 Root	**ECC Root**
Cert Name	VeriSign Universal Root Certification Authority	VeriSign Class 3 Public Primary Certificate Authority - G4
Description	This SHA256 root is currently included in NSS. Inclusion bug #484901. This root will be used to sign certificates for SSL-enabled servers, and may in the future be used to sign certificates for digitally-signed executable code objects.	This ECC root is currently included in NSS. Inclusion bug #409235 This root will be used to sign certificates for SSL-enabled servers, and may in the future be used to sign certificates for digitally-signed executable code objects.
Root cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=368998	https://bugzilla.mozilla.org/attachment.cgi?id=335538
SHA-1 fingerprint	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54	22:D5:D8:Df:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
Valid from	2008-04-01	2007-11-04
Valid to	2037-12-01	2038-01-18
Cert Version	3	3
Modulus length	2048	Type of signing key: SECG elliptic curve secp384r1 (aka NIST P-384)
Cert Signature Algorithm	Sha256RSA	Object Identifier (1 2 840 10045 4 3 3)
Enabled Trust Bits	Websites Email Code Signing	Websites Email Code Signing

Test URL	Please provide the url to a website whose EV SSL cert chains up to this root.	Please provide the url to a website whose EV SSL cert chains up to this root.
CRL URL	No CRL URL exists yet – Is this still the case?	No CRL URL exists yet – Is this still the case?
CRL update frequency	CPS section 4.9.7, CRL Issuance Frequency**:** CRLs for end-user Subscriber Certificates are issued at least once per day. Verisign: CRLs are issued at least once per day (they are actually issued more often than that). They have a validity period of 2 weeks. 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) VeriSign's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days	
OCSP Responder	None yet	None yet
Verification Type	OV, EV	OV, EV
EV policy OID	2.16.840.1.113733.1.7.23.6	2.16.840.1.113733.1.7.23.6
Hierarchy	What will the hierarchy look like in regards to EV? CPS Section 1.3.1: VeriSign also operates the "VeriSign Universal Root Certification Authority"… is not defined under a particular certificate Class, and may issue any class of Subordinate CA. The VeriSign Universal Root CA has not yet issued any intermediate or subordinate CA certificates. It may be used to issue Subordinate CA certificates for SSL, Code Signing, OFX, and Client Authentication. It will also be used to sign CRLs. This root does not have any subordinate CAs that are operated by external third parties, and this root has not been involved in cross-signing with another root.	Planned subCAs of VeriSign Class 3 Public Primary Certificate Authority - G4: • Class 3 Secure Server CA • Class 3 Secure Intranet Server CA • Class 3 Extended Validation SSL CA • Class 3 Code Signing • OnSite Administrator CA - Class 3 • Class 3 Open Financial Exchange CA - G2 • Time Stamping Authority CA • Class 3 Mobile CA • Class 3 WLAN CA • Class 3 Organizational CA All of these will be operated by the CA organization.
SubCAs operated by 3rd parties	Will this root ever have sub-CAs operated by external third parties?	No subordinated CAs will be operated by third parties for this root.
Cross-Signing	Will this root ever be involved in cross-signing with another root?	This root has not been (and will not be) involved in cross-signing with another root.
CP/CPS	CA Hierarchy Diagram: http://www.verisign.com/repository/hierarchy/hierarchy.pdf CPS: http://www.verisign.com/repository/CPS/ CP: http://www.verisign.com/repository/vtnCp.html VeriSign doesn't list all of their roots in the CPS. They refer to the PCAs generally. The ECC root is a Class 3 PCA (generation four), so even though it is not specifically mentioned the same Class 3 procedures would apply.	

AUDIT	Auditor: KPMG, http://www.kpmg.com/ Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=304&file=pdf (2008.11.30) Audit Type: This document contains three audit reports and the corresponding management assertions. The WebTrust for CA audit includes VeriSign Universal Root Certification Authority and VeriSign Class 3 Public Primary Certification Authority – VeriSign, Inc (PCA3-G1 SHA1). It does not include the VeriSign Class 3 Public Primary Certificate Authority - G4 root. The WebTrust for EV audit does not include either of these roots. Bug #409235, Comment #22: VeriSign has committed to include this ECC root in their upcoming WTCA audit, and provide the updated audit report to Mozilla as soon as it is ready. Both of these roots will need to be in a WebTrust for EV audit (readiness) before they may be approved for EV-enablement.
Organization Identity Verification	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 VeriSign 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.
Domain Name Ownership / Control	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 VeriSign authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.
EV Validation	CPS Appendix B1, Section 3, EV Certificate Warranties and Representations Right to Use Domain Name: VeriSign 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; CPS Appendix B1 Section*18*, Verification of Applicant's Domain Name VeriSign verifies Applicant's registration of the domain name(s) to be listed in the EV Certificate, satisfy the following requirements: (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA); (2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.

	For Government Entity Applicants, the VeriSign MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. (3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name (4) The Applicant is aware of its registration or exclusive control of the domain name; VeriSign performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, VeriSign will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name. In cases where Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, VeriSign may obtain positive confirmation from the registered domain holder that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, VeriSign also verifies the Applicant's exclusive right to use the domain name using one of the following methods: (A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or (B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, that it controls the confirmed domain name. In cases where the registered domain holder cannot be contacted, VeriSign shall: Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, *and* o Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name. by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN; VeriSign may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a Confirmation from Corporate Contact verifying that the Applicant is aware that it has exclusive control of the domain name.
Email Address Ownership / Control	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 VeriSign-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 table 2, only Class 3 (High Assurance) certificates can be used for Code Signing.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  o SSL certs are OV.
	  o According to CPS section 6.3.2, Class 3 certs may be issued beyond 3 years and up to a maximum of 5 years in circumstances where:
	  ▪ The certificate key pair is stored in hardware, and
	  ▪ VeriSign has authenticated the Organization in terms of this CPS and
	  ▪ When used to protect a server using SSL/TLS, the server is only accessible via a private network or intranet.
	  ▪ Footnote: At a minimum, the Distinguished Name of four and five year validity SSL certificates is reverified after three years from date of certificate issuance.
	• Wildcard DV SSL certificates
	  o SSL certs are OV. The only one mention of wildcard certs in CPS section on Domain Name: This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.
	• Issuing end entity certificates directly from roots
	  o Roots are offline, and only sign intermediate CAs.
	• Delegation of Domain / Email validation to third parties
	  o From Audit: "For the VeriSign/RSA Secure Server CA, VeriSign International Server CA – Class 3, and VeriSign Class 3 Secure Server CA, VeriSign makes use of external registration authorities for specific subscriber registration activities as disclosed in the VeriSign CPS on the VeriSign website. Our examination did not extend to the controls of the external registration authorities."
	• Allowing external entities to operate unconstrained subordinate CAs
	  o The PCA1, PCA2, and PCA3 roots may sign sub-CAs that are used by external third parties: OnSite (enterprise internal use), Affiliate (issue certs externally). The OnSite agreements are here: http://www.verisign.com/repository/onsite/index.html
	  o VeriSign: Under problematic practices, one of the items asked about by Mozilla is some of our roots issue out SubCAs operated by external third parties. For customers we create private subcas for that are signed by one of our roots - we host and control the subCA. Plus, for validation, we do upfront validation and delegate RA functionality out to them. This is all covered in our CPS. There are some additional documents that our CPS references that can only be shared under NDA as they include our trade secrets with regards to our processes. We could provide certain pieces of the relevant sections once under NDA if necessary.
	• Distributing generated private keys in PKCS#12 files
	  o 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 VeriSign-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.
	• Certificates referencing hostnames or private IP addresses
	  o Not found
	• OCSP Responses signed by a certificate under a different root
	  o No
	• CRL with critical CIDP Extension
	  o No