Summary of the Current VeriSign Requests
Bugzilla ID: 409235
Bugzilla Summary: add Verisign's G4 ECC root certificate
Bugzilla ID: 484901
Bugzilla Summary: Add Verisign's SHA256 root
Bugzilla ID: 490895
Bugzilla Summary: Add SHA1 version of Verisign PCA3-G1 root

General Information	**Data**
CA Name	VeriSign
Website URL (English version)	www.verisign.com
Organizational type	Commercial
Primary market / customer base	VeriSign is a major commercial CA with worldwide operations and customer base.

This document summarizes VeriSign’s request for inclusion of five roots, as described in bugs #409235, #484901, and #490895.
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.

Attestation of VeriSign’s conformance to the stated verification requirements can be found here:
http://www.verisign.com/repository/index.html (Click on the "AICPA/CICA WebTrust for Certification Authorities Audit Report" link)

Audit Type: WebTrust for CA
Auditor: KPMG, http://www.kpmg.com/
Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=304&file=pdf
(November, 2007) – When is the new WebTrust for CA audit expected? Will it include all of these roots?

Audit Type: WebTrust for EV – needed for EV-enablement of the PCA3-G1 SHA1 root.
Auditor: KPMG, http://www.kpmg.com/
Audit Report & Management Assertions: NEED

Verification procedures relating to section 7 of http://www.mozilla.org/projects/security/certs/policy/:

- VeriSign’s procedures for issuing Extended Validation SSL Certificates are described in Appendix B1 of the CPS.Verification of domain ownership for SSL
    - 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.

    - 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;

- Verification that the email account associated with the email address in the cert is owned by the subscriber.
    - 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
- Verify identity info in code signing certs is that of 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 identity, provides the details for verifying the identity of the certificate subscriber.

VeriSign Class 3 Public Primary Certificate Authority - G4: This CA 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. VeriSign is not yet actively issuing certificates from this root, so they have not published a CRL yet.

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.
No subordinated CAs will be operated by third parties for this root.
This root has not been involved in cross-signing with another root.

VeriSign Universal Root Certification Authority: This SHA256 root CA 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.
Please provide a description and/or diagram of the CA Hierarchy of VeriSign Universal Root Certification Authority.
Does the VeriSign Universal Root Certification Authority root CA have any subordinate CAs that are operated by external third parties?
Has this root been involved in cross-signing with another root?

VeriSign Class 1 Public Primary Certification Authority (PCA1 G1 SHA1): Add SHA1 version of root already included in NSS.
SubCAs of PCA1 G1 SHA1:
VeriSign Class 1 CA-Individual Subscriber-Persons-Not Validated
<Affiliate> SC Class 1 Consumer Individual Subscriber CA
<Affiliate> Class 1 Consumer Individual Subscriber CA

VeriSign Class 2 Public Primary Certification Authority (PCA2 G1 SHA1): Add SHA1 version of root already included in NSS.
SubCAs of PCA2 G1 SHA1:
VeriSign Class 2 Onsite Individual CA
<Managed PKI Consumer> CA
VeriSign Class 2 Personnel CA
--VeriSign Class2 Employee CA
-- VeriSign Class2 Contractor CA
<Affiliate> SC Class 2 Consumer Individual Subscriber CA
<Affiliate> Class 2 Consumer Individual Subscriber CA
<Affiliate> Class 2 CA
<Affiliate> Class 2 OnSite Individual Subscriber CA

VeriSign Class 3 Public Primary Certification Authority (PCA3-G1 SHA1): Add SHA1 version of root already included in NSS, and EV-enabled this version of the root. This root CA (also known as PCA3 - G1) participates in the cross-signing scheme by which EV certs issued under the VeriSign Class 3 Public Primary Certification Authority - G5 hierarchy may chain up to existing VeriSign roots.
SubCAs of PCA3 G1 SHA1:

- Class 3 Secure Server CA
- Class 3 Code Signing
- Class 3 Open Financial Exchange
- International Server
- Class 3 Secure Intranet Server
- Class 3 WLAN Secure Server
- Time stamping

Similar intermediate CAs are also provided for OnSite (enterprise) customers and Affiliates.
The PCA3 G1 SHA1 also signs the VeriSign Class 3 Public Primary Certification Authority – G5, which has two intermediate CAs:

- VeriSign Class 3 Extended Validation SSL CA
- VeriSign Class 3 Extended Validation SSL SGC CA

This root CA (PCA3 - G1) participates in the cross-signing scheme by which EV certs issued under the VeriSign Class 3 Public Primary Certification Authority - G5 hierarchy may chain up to existing VeriSign roots.

These PCA1 G1 SHA1, PCA2 G1 SHA1, and PCA3 G1 SHA1 roots all have externally-operated subCAs:
OnSite (enterprise internal use)
Affiliate (issue certs externally)

The OnSite agreements are here:
http://www.verisign.com/repository/onsite/index.html

Affiliate agreements?
Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
I think it would be too cumbersome to do this checklist for every Affiliate, so let's approach it from the standpoint of what VeriSign requires of their affiliates.

	Data for Bug #409235	**Data for Bug #484901**	**Data for Bug #490895**	**Data for Bug #490895**	**Data for Bug #490895**
Cert Name	VeriSign Class 3 Public Primary Certificate Authority - G4	VeriSign Universal Root Certification Authority	VeriSign Class 1 Public Primary Certification Authority (PCA1 G1 SHA1)	VeriSign Class 2 Public Primary Certification Authority (PCA2 G1 SHA1)	VeriSign Class 3 Public Primary Certification Authority (PCA3-G1 SHA1)
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=335538	https://bugzilla.mozilla.org/attachment.cgi?id=368998	https://bugzilla.mozilla.org/attachment.cgi?id=375224	https://bugzilla.mozilla.org/attachment.cgi?id=375223	https://bugzilla.mozilla.org/attachment.cgi?id=375222
SHA-1 fingerprint	22:D5:D8:Df:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54	CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1	57:F0:3D:CE:FB:45:69:4C:1C:25:E6:EE:A0:2C:43:D7:52:38:D3:C4	A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B
Valid from	2007-11-04	2008-04-01	1996-01-28	1996-01-28	1996-01-28
Valid to	2038-01-18	2037-12-01	2028-08-02	2028-08-02	2028-08-02
Cert Version	3	3	1	1	1
Modulus length	Type of signing key: SECG elliptic curve secp384r1 (aka NIST P-384)	2048	1024	1024	1024
Cert Signature Algorithm	Object Identifier (1 2 840 10045 4 3 3)	Sha256RSA	PKCS #1 SHA-1 With RSA Encryption	PKCS #1 SHA-1 With RSA Encryption	PKCS #1 SHA-1 With RSA Encryption
Requested Trust Bits	Websites Code Signing	Websites Code Signing	Email	Email	Websites Email Code Signing
CRL URL	**No CRL URL exists yet.** VeriSign does not yet have a CRL URL for this root, because they are not yet actively issuing certificates from this root. They are trying to get this	Need CRL for end-entity SSL certs	Need CRL for end-entity certs	Need CRL for end-entity certs	Need CRL for end-entity SSL and EV-SSL certs.

	root into the NSS database in anticipation of a market in the near future				
CRL update frequency	CPS: 4.9.7 CRL Issuance Frequency CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA Certificate is revoked. 14 CRLs for Authenticated Content Signing (ACS) root CAs are published annually and also whenever a CA Certificate is revoked.				
OCSP Responder URL	None yet. In the future VeriSign may provide OCSP service for certs signed by this root.	Is OCSP provided under this root?	Is OCSP provided under this root?	Is OCSP provided under this root?	Is OCSP provided under this root? Also need max time until OCSP responders updated to reflect end-entity revocation EV Guidelines section 26(a): “OCSP responses from this service MUST have a maximum expiration time of ten days.”
Verif. Type	OV	OV	DV	IV/OV	OV, EV
EV policy OID(s)	NOT requesting EV at this time?	NOT EV	NOT EV	NOT EV	2.16.840.1.113733.1.7.23.6
Test URL Or Sample cert	https://205.180.234.250 which needs to be mapped to https://ecc-test-valid.verisign.com by adding the following to your etc/hosts file: 205.180.234.250 ecc-test-valid.verisign.com	Please provide url to website whose ssl cert chains up to this root.	Please provide example cert chaining up to this root.	Please provide example cert chaining up to this root.	Please provide url to website whose EV-ssl cert chains up to this root.

Potentially Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - 6.3.2 Certificate Operational Periods and Key Pair Usage Periods: Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to five years, if the following requirements are met:
        - The Certificates are individual Certificates,
        - Subscribers' key pairs reside on a hardware token, such as a smart card,
        - Subscribers are required to undergo reauthentication at least every 25 months under Section 3.2.3,
        - Subscribers shall prove possession of the private key corresponding to the public key within the Certificate at least every 25 months under Section 3.2.3
- Wildcard DV SSL certificates
    - 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.
- Delegation of Domain / Email validation to third parties
    - The PCA1, PCA2, and PCA3 roots sign sub-CAs that are operated by external third parties. The Affiliates do their own domain and email validation.
- Issuing end entity certificates directly from roots
    - Roots are offline, and only sign intermediate CAs.
- Allowing external entities to operate unconstrained subordinate CAs
    - The PCA1, PCA2, and PCA3 roots sign sub-CAs that are operated by external third parties.
        - OnSite (enterprise internal use)
        - Affiliate (issue certs externally)
- 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 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
    - ?
- OCSP Responses signed by a certificate under a different root
    - ?
- CRL with critical CIDP Extension
    - ?
- Generic names for CAs
    - The CA names aren't too generic.