This document summarizes VeriSign's request for inclusion of five roots, as described in bugs #409235, #484901, and #490895.
Bugzilla ID #409235 – "add Verisign's G4 ECC root certificate"
Bugzilla ID #484901 – "Add Verisign's SHA256 root"
Bugzilla ID #490895 – "Add SHA1 version of Verisign's PCA1-G1, PCA2-G1, and PCA3-G1 roots"

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 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.

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:

1) WebTrust for CA -- In regards to this request, this audit covers
    a. VeriSign Universal Root Certification Authority
    b. VeriSign Class 1 Public Primary Certification Authority – VeriSign, Inc (PCA1 G1 SHA1)
    c. VeriSign Class 2 Public Primary Certification Authority – VeriSign, Inc (PCA2 G1 SHA1)
    d. VeriSign Class 3 Public Primary Certification Authority – VeriSign, Inc (PCA3-G1 SHA1)
2) WebTrust for CA for the VeriSign ECA
    a. This audit is specifically for the VeriSign DOD External Certification Authority, which is not part of this request.
3) WebTrust for EV In regards to this request, this audit covers
    a. VeriSign Class 3 Public Primary Certification Authority – VeriSign, Inc (PCA3-G1 SHA1)

I did not find reference to VeriSign Class 3 Public Primary Certificate Authority - G4 in the audit.
VeriSign: per KPMG, our annual WebTrust for CAs reports for VeriSign cover the effectiveness of CA controls including the CA key generation process based on the WebTrust for CAs criteria. Each audit cycle, KPMG tests various CA key generation ceremonies and identify specific production CAs in their reports.

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.

Below is a summary of the five roots that VeriSign is requesting to be included

VeriSign Class 3 Public Primary Certificate Authority - G4

	Data for Bug #409235
Cert Name	VeriSign Class 3 Public Primary Certificate Authority - G4
Description	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.
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=335538
SHA-1 fingerprint	22:D5:D8:Df:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
Valid from	2007-11-04
Valid to	2038-01-18
Cert Version	3
Modulus length	Type of signing key: SECG elliptic curve secp384r1 (aka NIST P-384)
Cert Signature Algorithm	Object Identifier (1 2 840 10045 4 3 3)
Requested Trust Bits	Websites Email Code Signing
Test URL	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

CRL URL	**No CRL URL exists yet --** VeriSign not yet actively issuing certificates from this root.
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.
OCSP Responder URL	None yet. In the future VeriSign may provide OCSP service for certs signed by this root.
Verification Type	OV
EV policy OID(s)	Not EV in this request. A separate bug will be filed for EV-enabling this root.
Hierarchy	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

	Data for Bug #484901
Cert Name	VeriSign Universal Root Certification Authority
Description	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.
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=368998
SHA-1 fingerprint	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54
Valid from	2008-04-01
Valid to	2037-12-01
Cert Version	3
Modulus length	2048
Cert Signature Algorithm	Sha256RSA
Requested Trust Bits	Websites Email Code Signing
Test URL	https://ptnr-verisign256.bbtest.net As we are not using this root publically yet, we did not issue this using an intermediate root, which we will do in our production environment.
CRL URL	**No CRL URL exists yet**

	No certs have been issued from this root yet.
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.
OCSP Responder URL	No
Verification Type	OV
EV policy OID(s)	Not EV in this request. A separate bug will be filed for EV-enabling this root.
Hierarchy	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.

VeriSign Class 1 Public Primary Certification Authority (PCA1 G1 SHA1)

	Data for Bug #490895
Cert Name	VeriSign Class 1 Public Primary Certification Authority – VeriSign, Inc (PCA1 G1 SHA1)
Description	Add SHA1 version of root already included in NSS. VeriSign: For the SHA1 versions for the G1 PCA Roots, we would like you to leave in the MD2 roots alongside the SHA-1 roots, because we've issued intermediates with AKIs that point to the MD2 versions.
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=375224
SHA-1 fingerprint	CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1
Valid from	1996-01-28
Valid to	2028-08-02
Cert Version	1
Modulus length	1024
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Requested Trust Bits	Email
Test URL	https://bugzilla.mozilla.org/attachment.cgi?id=390566
CRL URL	http://crl.verisign.com/pca1.crl end-entity certs: http://crl.verisign.com/IndC1DigitalID.crl Next update: 10 days Verisign: The common Name of the SubCA ends with "G2", but it really is issued by PCA1 G1 Root.
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.
OCSP Responder URL	No
Verification Type	DV
EV policy OID(s)	NOT EV
Hierarchy	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)

	Data for Bug #490895
Cert Name	VeriSign Class 2 Public Primary Certification Authority – VeriSign, Inc (PCA2 G1 SHA1)
Description	Add SHA1 version of root already included in NSS. VeriSign: For the SHA1 versions for the G1 PCA Roots, we would like you to leave in the MD2 roots alongside the SHA-1 roots, because we've issued intermediates with AKIs that point to the MD2 versions.
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=375223
SHA-1 fingerprint	57:F0:3D:CE:FB:45:69:4C:1C:25:E6:EE:A0:2C:43:D7:52:38:D3:C4
Valid from	1996-01-28
Valid to	2028-08-02
Cert Version	1
Modulus length	1024
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Requested Trust Bits	Email
Test URL	No example cert provided -- There are no active subCAs under this PCA2 G1 root.
CRL URL	http://crl.verisign.com/pca2.crl Next update: 4 months. There are no active subCAs under this PCA2 G1 root.
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.
OCSP Responder URL	No
Verification Type	IV/OV
EV policy OID(s)	NOT EV
Hierarchy	VeriSign: We have no active SubCAs under this Root. VeriSign: We won't be adding any new CAs that are signed by this Root (PCA2 G1). We do feel these roots should be included because these roots enable our customers to read their archived S/MIME mail. There are business requirements to maintain 10 years or more of access to email. Our customers paid a premium in their choice of these roots to get the value of being imbedded in browsers with a long validation period. Removing these roots will "break" S/MIME in the eyes of most customers, even though technical workarounds could be implemented. The customer would be required to fully understand and manage roots, which we know today is not realistic. Given the huge number of terabytes of archived S/MIME mail worldwide we feel very strongly on these roots being included.

VeriSign Class 3 Public Primary Certification Authority (PCA3-G1 SHA1)

	Data for Bug #490895
Cert Name	VeriSign Class 3 Public Primary Certification Authority – VeriSign, Inc (PCA3-G1 SHA1)
Description	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. Reason for wanting to EV-enable this PCA3-G1 root: There are certain Asian sites wanting to show EV UI in Firefox, but their websites must support mobile users, so they chain up to this PCA3-G1root in order to support mobile devices that can't handle 2048-bit roots. For details, see Comment #7 in https://bugzilla.mozilla.org/show_bug.cgi?id=420760. VeriSign: leave in the MD2 roots, because we've issued intermediates with AKIs that point to the MD2 versions.
root CA cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=375222
SHA-1 fingerprint	A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B
Valid from	1996-01-28
Valid to	2028-08-02
Cert Version	1
Modulus length	1024
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Requested Trust Bits	Websites Email Code Signing
Test URL	Please provide url to website whose EV-ssl cert chains up to this root.
CRL URL	http://crl.verisign.com/pca3.crl, end-entity certs: http://crl.verisign.com/SVRSecure2005.crl Next update: 2 weeks
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.
OCSP Responder URL	http://ocsp.verisign.com maximum expiration time: 7 days.
Verification Type	OV, EV
EV policy OID(s)	2.16.840.1.113733.1.7.23.6
Hierarchy	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 sub-CAs: • VeriSign Class 3 Extended Validation SSL CA • VeriSign Class 3 Extended Validation SSL SGC CA

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

- Long-lived DV certificates
  - SSL certs are OV.
  - 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
  - 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
  - Roots are offline, and only sign intermediate CAs.
- Delegation of Domain / Email validation to third parties
  - 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
  - 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
  - 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
  - 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
  - Not found
- OCSP Responses signed by a certificate under a different root
  - No
- CRL with critical CIDP Extension
  - No