Bugzilla ID: 507360
Bugzilla Summary: Add a SHA256 Root CA to the NSS store for GlobalSign

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	GlobalSign
Website URL (English version)	http://www.globalsign.com/
Organizational type	Public corporation
Primary market / customer base	GlobalSign is a commercial CA based in Portsmouth NH and serving customers worldwide.

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

Info Needed	**Data**
Certificate Name	GlobalSign Root CA – R3
Cert summary / comments	This is the SHA256 version of the GlobalSign root (SHA1) that is already included in NSS. This root is primarily suitable for Server and Client Authentication, Secure e-mail, Code Signing and Timestamping. However the root itself is marked for all issuance policies and therefore can also be used for OCSP, Encrypting File System, IP Sec (Tunnel, User) and CA Encryption Certificate purposes.
The root CA certificate URL	http://secure.globalsign.net/cacert/Root-R3.crt
SHA-1 fingerprint.	D6:9B:56:11:48:F0:1C:77:C5:45:78:C1:09:26:DF:5B:85:69:76:AD
Valid from	2009-03-18
Valid to	2029-03-18
Cert Version	3
Modulus length / key length	2048
Test Website	Please provide the url to a website whose EV-SSL cert chains up to this root. This may be a test site.
CRL URL	http://crl.globalsign.net/Root-r3.crl (Not yet published) What is the nextUpdate set to in the CRLs for end-entity certificates? From prior request: GlobalSign issues CRLs on a 3-hour schedule
OCSP Responder URL	Is OCSP provided for this root? From prior request, OCSP responder URL: http://evssl-ocsp.globalsign.com/responder

	If OCSP is provided for this root, what is the maximum time until OCSP responders are updated to reflect end-entity revocation? http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf 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.”
List or description of subordinate CAs operated by the CA organization associated with the root CA.	What is the planned CA hierarchy for this root? From prior request: GlobalSign has multiple intermediate CAs under a single root. Different types of certificates (e.g., personal vs. SSL vs. object signing) and different classes of certificates (e.g., personal class 1 vs. class 2, DV SSL vs. OV vs. EV) are issued by different subordinates.
Subordinate CAs operated by third parties	Will this root have externally operated subordinate CAs? From prior request: Subordinate CA requirements are described in the CPS, including following CPS and audits. CPS section 1.10.7.3 describes requirements for subordinate EV CAs. With the exception of one extremely well known brand, all CA issuing certificates are signed such that they can only issue end entity certs and not create additional CAs. As a CA is then run by an enterprise, domains are not technically restricted, however domains are contractually restricted. GlobalSign audits periodically as part of our own brand protection program.It also helps to ensure the latest certificate end entity profile information is provided to our enterprise partners to improve interoperability of the certificates in the majority of systems/appliances.
List any other root CAs that have issued cross-signing certificates for this root CA	Will this root be involved in cross-signing with any other CAs?
Requested Trust Bits	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV – only the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber.	DV, IV/OV, EV

• OV – in addition to verifying the domain name, the value of the Organization attribute is verified to be that associated with the certificate subscriber. • EV -- Extended Validation Certificate	
EV policy OID(s)	1.3.6.1.4.1.4146.1.1
CP/CPS	Repository of All Legal Documents: http://www.globalsign.com/repository/ GlobalSign Certification Practice Statement: http://www.globalsign.com/repository/GlobalSign_CPS_v6.5.pdf The CPS is the primary document describing verification procedures GlobalSign CA Certificate Policy: http://www.globalsign.com/repository/GlobalSign_CA_CP_v3.4.pdf
AUDIT	WebTrust for CA Ernst & Young: http://www.ey.com/be https://cert.webtrust.org/SealFile?seal=761&file=pdf (2008.03.31) WebTrust for EV Ernst & Young: http://www.ey.com/be http://www.globalsign.com/repository/webtrust_for_ev_ssl.pdf (2008.03.31) Have you had WebTrust for CA and WebTrust for EV audits performed this year, which have included this new root?

Review CPS sections dealing with subscriber verification (section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - GlobalSign verifies domain ownership/control as specified in the CPS in sections 1.8 (OrganizationSSL), 1.9 (DomainSSL), 1.10 (ExtendedSSL), 1.11 (Eductational ServerSign), and 3.3.1 (Documents used for subscriber registration).
        - OrganizationSSL: GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit. This may also include checks in third party databases or resources, against standard bodies such as

the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN), and independent verification through telephone.

        - DomainSSL certificates are issued to entities and individuals who own a domain name, or have the right to request a DomainSSL for a specific domain. Additional documentation in support of the application may be required so that GlobalSign verifies that the domain name belongs to the applicant, or that the applicant is authorized to request a certificate for that domain name. The applicant submits to GlobalSign the additional documentation. Upon verification of ownership or right to use of the domain name, GlobalSign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server.
        - GlobalSign has the right to request proof of the ownership of any of the domain names or IP addresses in the certificate (including those incorporated as Subject Alternative Names) or can ask the owner of the domain name to validate the request of the applicant. GlobalSign will not verify the country code within the certificate request.
        - GlobalSign verifies the submitted information by checking domain ownership or domain right to use and any other information as it sees fit. This may also include checks in third party databases or resources, against standard bodies such as the Internet Engineering Task Force (IETF) or the Internet Corporation for Assigned Names and Numbers (ICANN), and independent verification through telephone.
        - ExtendedSSL (CPS section 1.10.5): As to data verification, GlobalSign ensures that the following Subject organization information has been submitted by the applicant and shall be verified by the CA in accordance with the EV Guidelines (Sections 14 through 25) by taking all verification steps reasonably necessary:
            - 1 Applicant‟s existence and identity, including where applicable:
            - (a) Applicant‟s legal existence and identity (as established with an Incorporating Agency),
            - (b) Applicant‟s physical existence (business presence at a physical address), and
            - (c) Applicant‟s operational existence (business activity) and where applicable to the Business Category type,
            - (d) The principle individual(s)
            - 2 Applicant‟s exclusive control of the domain name and applicable Subject Alternative Name domains to be included in certificate;
            - 3 Applicant‟s authorization for the ExtendedSSL certificate, including;
            - (a) Contract Signer, certificate Approver and certificate Requester name, title, and authority
            - (b) Subscriber Agreement signing by Contract Signer
            - (c) Approval by the certificate Approver of the certificate Request.

- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber’s legal identity.
    - GlobalSign verifies that the entity submitting the request controls the email account associated with the email address referenced in the certificate, using an email-based challenge/response mechanism. (CPS section 1.3)
    - From CPS: A certificate request can be made as follows:
        - **On-line:** Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by GlobalSign. Additional documentation in support of the application may be required so that

        GlobalSign verifies the identity of the applicant. The applicant submits to GlobalSign such additional documentation. The applicant must in person appear in front of a GlobalSign RA or LRA. Upon verification of identity, GlobalSign issues the certificate and sends a notice to the applicant. to the e-mail address from which the certificate application had originated. The applicant downloads and installs the certificate to its device. The applicant must notify GlobalSign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of information to be included in the certificate.
        - **API:** The certificate applicant submits an appropriately formatted certificate request via an approved API (Application Programming Interface) to GlobalSign. Additional documentation in support of the application may be required to verify the identity of the applicant. If necessary, the applicant submits to GlobalSign or a GlobalSign approved Registration Authority such additional documentation. Upon verification of identity, GlobalSign either directly or via the API issues the certificate or sends such certificate to the e-mail address from which the certificate application had originated. The certificate applicant must promptly notify GlobalSign or the Registration Authority of any inaccuracy or defect in a certificate or earlier notice of the information to be included in the certificate.
- Verify identity info in code signing certs is that of subscriber
    - GlobalSign verifies that the entity submitting the certificate signing request is the same entity referenced in the certificate. (CPS section 1.12)
        - ObjectSign certificates are used for the signing of software objects, such as software packages or applets. ObjectSign certificates validity period is between one and three years. ObjectSign certificates are issued to legal persons and self-employed professionals. (For self-employed persons belonging to an association or professional group, an official document from the professional group and membership card may be required. GlobalSign may require additional identification proof in support of the verification of the applicant.
        - GlobalSign verifies the submitted information by checking organizational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.

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

- Long-lived DV certificates
    - OrganizationSSL certificates validity period is between one and five years according to the choice of the applicant.
    - DomainSSL certificates validity period is between one and five years.
    - ExtendedSSL certificates validity period is between one year and 27 months.
    - Educational ServerSign certificates validity period is between one and three years.
- Wildcard DV SSL certificates
    - Not found
- Delegation of Domain / Email validation to third parties

- **CP section 2.3.2 GlobalSign Registration Authorities**
    - The GlobalSign CA reaches its subscribers through a designated Registration Authorities. An RA requests the issuance and revocation of a certificate under this CP. An RA submits the necessary data for the generation and revocation of the certificates to the CA.
    - The GlobalSign RA acts locally on approval and authorisation by the GlobalSign CA. The GlobalSign RA acts in accordance with the approved practices and procedures of the GlobalSign CA including this CP and documented GlobalSign RA procedures.
    - Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of GlobalSign RAs.

- Issuing end entity certificates directly from roots
  - No, GlobalSign has an offline root which only signs subordinate CAs.
- Allowing external entities to operate unconstrained subordinate CAs
  - Subordinate CAs are required to follow CPS and be audited
  - CPS section 1.10.7.3, Root CA Indemnification**:**
    - In cases where the Subordinate CA and the Root CA are different legal entities and the Root CA specifically enables the Subordinate CA to issue ExtendedSSL Subscriber Certificates, the Root CA shall also be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA‟s compliance with the EV Guidelines, and for all liabilities and indemnification obligations of the Subordinate CA under the EV Guidelines, as if the Root CA was the Subordinate CA issuing the ExtendedSSL Certificates.
    - However, this Section shall not apply to cases where a Root CA, Root CA "A", from a different legal entity, cross-certifies Root CA "B" to enable certificates issued by "B" to be trusted in older, non-EV enabled browsers. The cross certificate issued by "A" to "B" does not enable EV according to these guidelines. Certificates issued by "B" are EV enabled only when an EV enabled browser can build a certificate chain to the root certificate of "B".
- Distributing generated private keys in PKCS#12 files
  - GlobalSign does provide the option for generating the private key.
    - CPS: If GlobalSign issues both the public certificate and the GlobalSign generated private key to the applicant, then it will be protected by the strong password provided by the applicant during the registration process. GlobalSign will then delete all instances of the Applicant‟s private key.
- Certificates referencing hostnames or private IP addresses
  - CPS: DomainSSL certificates may also be used to secure Intranet Servers or Unified Communications Servers, however, any non-publically resolvable domain names, server names or IP addresses may only be incorporated as a Subject Alternative Name extension.
- OCSP Responses signed by a certificate under a different root
  - ?
- CRL with critical CIDP Extension
  - ?

- Generic names for CAs