Bugzilla ID: 406794
Bugzilla Summary: Refresh the GlobalSign Root CA cert (will be EV)

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.

General Information	**Data**
CA Name	GlobalSign
Website URL (English version)	http://www.globalsign.com/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Public corporation
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	GlobalSign is a commercial CA based in Portsmouth NH and serving customers worldwide. It currently has two root CA certificates preloaded in Mozilla. The first root has two subordinate CAs (for domain-validated and organizationally-validated certificates respectively) and the second root has one subordinate CA (for extended validation certificates). (There is also a valid chain from the EV subordinate to the first root via a cross-signing certificate.)

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

Info Needed	**Data - 406794**	**Status / Notes**
Certificate Name	GlobalSign Root CA	COMPLETE
Cert summary / comments	Note that a version of this root CA certificate with the same public key but an earlier expiration date (2014-01-28) is already included in the Mozilla list. The present request is to replace the older certificate with this certificate and then enable this CA certificate for EV.	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://secure.globalsign.net/cacert/Root-R1.crt	COMPLETE

SHA-1 fingerprint.	B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C	COMPLETE
Valid from	9/1/1998	COMPLETE
Valid to	1/28/2028	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	http://crl.globalsign.net/root.crl CRL's for end-entity certificates are issued every 3 hours.	COMPLETE
OCSP (if applicable) • OCSP Responder URL • 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."	Comment #11 from related bugzilla #406794 (6/26/2008): OCSP will be implemented later this week as we can't now wait for the OCSP bug (https://bugzilla.mozilla.org/show_bug.cgi?id=413997) to be fixed.	Will need the OCSP Responder URL.
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	The personal certificate subordinate CAs are all being changed to move to a 3 tier hierarcy in August/September. At the moment we have a 4 certificate hierarchy for our product range with separate issuing CA's for PersonalSign Class 1,2,3 and ObjectSign. We already have a 3 certificate hierarchy for our Server Certificates. DomainSSL, OrganizationSSL and EntendedSSL.	COMPLETE
For subordinate CAs operated by third parties, if any:	With the exception of one extremely well known brand, all CA issuing certificates are signed such that	COMPLETE

General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	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.	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. (see text below)
List any other root CAs that have issued cross-signing certificates for this root CA	GlobalSign is not cross signed by or with any other certification authorities.	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLETE
. If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	DV, IV/OV, EV	COMPLETE

If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	1.3.6.1.4.1.4146.1.1	COMPLETE
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • *Note: mainly interested in SSL, so OK if no email example.*	The root key material is the same as the previous root it replaces so https://www.globalsign.com will work.	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	http://www.globalsign.com/repository/GlobalSign_CA_CP_v3.0.pdf http://www.globalsign.com/repository/GlobalSign_CPS_v6.0.pdf	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the “audit report and management assertions” document available from the webtrust.org site or elsewhere.)	The WebTrust audit is due to be completed this week with a report being published on the 20th June. The auditor has been changed from Deloitte to Ernst & Young.	Need : WT/EV audit – ETA June early July

Review CPS sections dealing with subscriber verification (complete)

- Verify domain check for SSL
    - “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 and independent verification through telephone.”
- 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.
    - From Steve Roylance on 6/6/08: We instigated a change to the CPS to make it more obvious. Version 6.1 will be published next week. Both for http based and API based requests we do a challenge response to the e-mail. The HTTP method does not specifically state to date so this is

what we changed, however the API method in section 1.5.2 specifically states:- "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."

- Verify identity info in code signing certs is that of subscriber
- Make sure it’s clear which checks are done for which context (cert usage)

Flag Problematic Practices (complete)

- Long-Lived Domain-Validated SSL certs (not found)
- Wildcard DV SSL certs (not found)
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA (not found)
- Allowing external entities to operate subordinate CAs (yes, but subordinates required to follow CPS and be audited)
    - **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 GlobalSign 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 GlobalSign ExtendedSSL Certificates.

Verify Audits (Need WT/EV audit)

- Validate contact info in report, call to verify that they did indeed issue this report.
- For EV CA’s, verify current WebTrust EV Audit done.
- Review Audit to flag any issues noted in the report