

**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](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](https://wiki.mozilla.org/CA:Recommended_Practices).

| General Information            | Data   |
|--------------------------------|--|
| CA Name                        | GlobalSign   |
| Website URL (English version)  | <a href="http://www.globalsign.com/">http://www.globalsign.com/</a>  |
| Organizational type            | Public corporation   |
| Primary market / customer base | GlobalSign is a commercial CA based in Portsmouth NH and serving customers worldwide.  |
| CA Contact Information         | CA Email Alias: <a href="mailto:legal@globalsign.com">legal@globalsign.com</a><br>CA Phone Number: 44 1622 766 766<br>Title / Department: Business Development |

**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 new root 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.<br>The Root has been created (A ceremony to WebTrust audited standards witnessed by E&Y). However, this root is not yet active, so full CRL and OCSP support have not yet been provided for it. GlobalSign will be supporting a new certificate hierarchy in 2010 based on this SHA256 root. |
| The root CA certificate URL | <a href="http://secure.globalsign.net/cacert/Root-R3.crt">http://secure.globalsign.net/cacert/Root-R3.crt</a>  |
| 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                | <a href="https://2029.globalsign.com">https://2029.globalsign.com</a>  |
| CRL URL                     | <a href="http://crl.globalsign.net/Root-r3.crl">http://crl.globalsign.net/Root-r3.crl</a> (Not yet published)<br><a href="http://crl.globalsign.net/SHA256ExtendVal1.crl">http://crl.globalsign.net/SHA256ExtendVal1.crl</a> (NextUpdate 30 days)<br>CPS section 4.9.1 CRL: A CRL is issued each 3 hours.  |

|   |  |
|---|--|
| OCSP Responder URL                        | <p>OCSP is not yet provided for this root.</p> <p>For the EV root already in NSS the OCSP responder URL is : <a href="http://evssl-ocsp.globalsign.com/responder">http://evssl-ocsp.globalsign.com/responder</a></p> <p>OCSP will be provided on an 'as needed' basis. So any certificate hierarchy that requires OCSP will have it. The root itself will be used to sign OCSP responder certificates. OCSP responses for EV end entity certificates will be compliant with CABForum guidelines.</p>   |
| CA Hierarchy                              | <p>GlobalSign will be supporting a new certificate hierarchy in 2010 based on this SHA256 root. The plan for this root will be very similar to the current product range. i.e. specific separate intermediate issuing CAs for each product type, including EV.</p> <p>For reference, hierarchy of the root currently in NSS: 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.</p>  |
| Subordinate CAs operated by third parties | <p>In the future, it is possible that this root will sign an externally operated sub-CAs. If this does happen then the rules followed today will apply.</p> <p>Subordinate CA requirements are described in the CPS, including following CPS and audits.</p> <p>See CPS section 1.10.7.3.</p>  |
| Cross-Signing                             | There no plans to cross sign another CA with this root.  |
| Requested Trust Bits                      | <p>Websites</p> <p>Email</p> <p>Code</p>   |
| SSL Validation Type                       | DV, IV/OV, EV  |
| EV policy OID                             | 1.3.6.1.4.1.4146.1.1   |
| CP/CPS                                    | <p>All of these documents are in English.</p> <p>Repository of All Legal Documents: <a href="http://www.globalsign.com/repository/">http://www.globalsign.com/repository/</a></p> <p>GlobalSign Certification Practice Statement: <a href="http://www.globalsign.com/repository/GlobalSign_CPS_v6.5.pdf">http://www.globalsign.com/repository/GlobalSign_CPS_v6.5.pdf</a></p> <p>The CPS is the primary document describing verification procedures</p> <p>GlobalSign's CPS - Digitally signed: <a href="https://bugzilla.mozilla.org/attachment.cgi?id=398640">https://bugzilla.mozilla.org/attachment.cgi?id=398640</a></p> <p>Revision 6.4 to 6.5 adds support for SHA256 as a cryptographic technology in GlobalSign's WebTrust approved product range.</p> <p>GlobalSign CA Certificate Policy: <a href="http://www.globalsign.com/repository/GlobalSign_CA_CP_v3.4.pdf">http://www.globalsign.com/repository/GlobalSign_CA_CP_v3.4.pdf</a></p> <p>GlobalSign's Certificate Policy - Digitally Signed: <a href="https://bugzilla.mozilla.org/attachment.cgi?id=398634">https://bugzilla.mozilla.org/attachment.cgi?id=398634</a></p> <p>Revision 3.3 to 3.4 adds the SHA256 based R3 root under GlobalSign's WebTrust approved certificate hierarchy.</p> |
| AUDIT                                     | <p>Audit Type: WebTrust for CA</p> <p>Auditor: Ernst &amp; Young</p>   |

|                                    |   |
|------------------------------------|---|
|                                    | <p>Auditor Website: <a href="http://www.ey.com/be">http://www.ey.com/be</a><br/> Audit: <a href="https://cert.webtrust.org/SealFile?seal=928&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=928&amp;file=pdf</a> (2009.03.31)</p> <p>Audit Type: WebTrust for EV<br/> Auditor: Ernst &amp; Young<br/> Auditor Website: <a href="http://www.ey.com/be">http://www.ey.com/be</a><br/> Audit: <a href="https://cert.webtrust.org/SealFile?seal=929&amp;file=pdf">https://cert.webtrust.org/SealFile?seal=929&amp;file=pdf</a> (2009.03.31)</p> <p>Both audits are for the root CAs: “GlobalSign Root CA”, GlobalSign Root CA – R2” and “GlobalSign CA for Adobe”... The next audits will include this GlobalSign Root CA – R3 root.</p>   |
| Organization Identity Verification | <p>CPS section 1.2.2, Server Certificates</p> <p>GlobalSign offers several types of certificates for servers/hardware which may be used for web based transactions. In all cases, a licence is granted by GlobalSign to the subscriber to create a backup of both the certificate and associated private key pair for business continuity purposes. No licence is granted to transfer or duplicate the certificate and associated key pair for any other purpose unless specifically indicated during the purchasing process by virtue of a suitable offer or promotion which may or may not be advertized on the appropriate GlobalSign web site:</p> <ul style="list-style-type: none"> <li>· OrganizationSSL: OrganizationSSL is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web- based businesses engaging in commercial and financial transactions. The identity of the certificate-holder is fully authenticated by GlobalSign.</li> <li>· DomainSSL: DomainSSL is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions. The identity of the certificate-holder is not authenticated by GlobalSign, only the ownership of the domain or the capability to use the domain as represented by the Domain Name System.</li> <li>· ExtendedSSL: ExtendedSSL is meant for entities that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in commercial and financial transactions. The identity of the certificate-holder is fully authenticated by GlobalSign in accordance with the CA/browser forum Guidelines for Extended Validation Certificates.</li> <li>· Educational ServerSign: Educational ServerSign is meant for entities within the education and research space that wish to verify their identity and participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based education and research institutes.</li> </ul> <p>CPS section 1.10.1.4 ExtendedSSL Subjects</p> |

|                                    |  |
|------------------------------------|--|
|                                    | <p>ExtendedSSL certificates may be issued to private organizations, government entities Business Entities and International Organizations, provided they are either duly incorporated in the jurisdiction of incorporation where GlobalSign acts as a CA, or the principle individuals and the legal existence of the business have been verified in accordance to the <a href="#">guidelines</a> incorporated into this document by reference.</p> <p>GlobalSign may not issue ExtendedSSL certificates to individuals (natural persons).</p> <p>The period retention for records fulfils professional records requirements of the Laws of the United States.</p>   |
| Domain Name<br>Ownership / Control | <p>GlobalSign verifies domain ownership/control as specified in the CPS in sections 1.8 (OrganizationSSL), 1.9 (DomainSSL), 1.10 (ExtendedSSL), 1.11 (Educational ServerSign), and 3.3.1 (Documents used for subscriber registration).</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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: <ul style="list-style-type: none"> <li>• 1 Applicant's existence and identity, including where applicable:</li> <li>• (a) Applicant's legal existence and identity (as established with an Incorporating</li> </ul> </li> </ul> |

|  |   |
|--|---|
|  | <p>Agency),</p> <ul style="list-style-type: none"> <li>• (b) Applicant's physical existence (business presence at a physical address), and</li> <li>• (c) Applicant's operational existence (business activity) and where applicable to the Business Category type,</li> <li>• (d) The principle individual(s)</li> <li>• 2 Applicant's exclusive control of the domain name and applicable Subject Alternative Name domains to be included in certificate;</li> <li>• 3 Applicant's authorization for the ExtendedSSL certificate, including;</li> <li>• (a) Contract Signer, certificate Approver and certificate Requester name, title, and authority</li> <li>• (b) Subscriber Agreement signing by Contract Signer</li> <li>• (c) Approval by the certificate Approver of the certificate Request.</li> </ul>  |
| Email Address<br>Ownership / Control   | <p>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)</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> |
| Identity of Code Signing<br>Subscriber | <p>GlobalSign verifies that the entity submitting the certificate signing request is the same entity referenced in the certificate. (CPS section 1.12)</p> <ul style="list-style-type: none"> <li>• ObjectSign certificates are used for the signing of software objects, such as software packages or</li> </ul>   |

|                                   |   |
|-----------------------------------|---|
|                                   | <p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>   |
| Potentially Problematic Practices | <p><a href="http://wiki.mozilla.org/CA:Problematic_Practices">http://wiki.mozilla.org/CA:Problematic_Practices</a></p> <ul style="list-style-type: none"> <li>• <a href="#">Long-lived DV certificates</a> <ul style="list-style-type: none"> <li>○ OrganizationSSL certificates (OV) validity period is between one and five years according to the choice of the applicant.</li> <li>○ <b>DomainSSL certificates (DV) validity period is between one and five years.</b></li> <li>○ ExtendedSSL certificates validity period is between one year and 27 months.</li> <li>○ Educational ServerSign certificates validity period is between one and three years.</li> </ul> </li> <li>• <a href="#">Wildcard DV SSL certificates</a> <ul style="list-style-type: none"> <li>○ Not found</li> </ul> </li> <li>• <a href="#">Delegation of Domain / Email validation to third parties</a> <ul style="list-style-type: none"> <li>○ <b>CP section 2.3.2 GlobalSign Registration Authorities</b> <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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.</li> <li>▪ Some RA functions are sometimes carried out by Local Registration Authorities (LRAs). LRAs act under the supervision and control of GlobalSign RAs.</li> </ul> </li> </ul> </li> <li>• <a href="#">Issuing end entity certificates directly from roots</a> <ul style="list-style-type: none"> <li>○ No, This root will be offline and will only sign subordinate CAs.</li> </ul> </li> <li>• <a href="#">Allowing external entities to operate unconstrained subordinate CAs</a> <ul style="list-style-type: none"> <li>○ Subordinate CAs are required to follow CPS and be audited</li> </ul> </li> </ul> |

|  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>○ CPS section 1.10.7.3, Root CA Indemnification: <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ 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".</li> </ul> </li> <li>• <a href="#">Distributing generated private keys in PKCS#12 files</a> <ul style="list-style-type: none"> <li>○ GlobalSign does provide the option for generating the private key. <ul style="list-style-type: none"> <li>▪ 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.</li> </ul> </li> </ul> </li> <li>• <a href="#">Certificates referencing hostnames or private IP addresses</a> <ul style="list-style-type: none"> <li>○ 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.</li> </ul> </li> <li>• <a href="#">OCSP Responses signed by a certificate under a different root</a> <ul style="list-style-type: none"> <li>○ OCSP will be provided on an 'as needed' basis. So any certificate hierarchy that requires OCSP will have it. The root itself will be used to sign OCSP responder certificates again every 6 months as with above. OCSP responses for EV end entity certificates will be compliant with CABForum guidelines.</li> </ul> </li> <li>• <a href="#">CRL with critical CIDP Extension</a> <ul style="list-style-type: none"> <li>○ CRL for the current sub-CA imported into Firefox browser without error.</li> </ul> </li> </ul> |
|--|---|