**Bugzilla ID:** [**1390803**](https://bugzilla.mozilla.org/show_bug.cgi?id=1390803)

**Bugzilla Summary:** Add “GlobalSign Root CA – R6” root certificate

**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | GlobalSign |
| Website URL | www.globalsign.com |
| Organizational type | Private Company |
| Primary Market / Customer Base | GlobalSign is a subsidiary of GMO CLOUD K.K. in Japan and serves customers worldwide. |
| Impact to Mozilla Users | Please supply the below information: |
| *Why does the CA need to have their root certificate directly included in Mozilla’s products, rather than being signed by another CA’s root certificate that is already included in NSS?* | GlobalSign already has root certificates included in NSS. GlobalSign’s root R6 is the next generation root certificate, and will replace older, expiring roots that have smaller key sizes in the future. Adding this latest root to NSS/Mozilla products will enable Mozilla and GlobalSign customers to benefit from the use of a root with 4096 bit RSA keys. |
| *Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not?* | Chrome, Firefox, Internet Explorer, iOS |
| *Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.* | Mozilla users who browse secure websites and/or send/receive secure email messages will likely encounter GlobalSign certificates issued under this root certificate. GlobalSign’s root R6 will be used to issue EV SSL, DV SSL, OV SSL, S/MIME, ClientAuth, EV Code Signing, Non-EV Code Signing, Timestamping, Document Signing, and Encrypted File System certificates. |

**CA Primary Point of Contact (POC)**

|  |  |
| --- | --- |
| POC Full Name (First, Last) | Julie Olson |
| POC Direct Phone Number | 1-603-570-7060 |
| POC Direct E-mail Address | julie.olson@globalsign.com |
| CA E-mail Alias | rootembedding@globalsign.com |
| CA Phone Number | Americas Support Line: 1-877-467-7543 |
| Title/Department | Project Manager |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| 1. Certificate Name
 | GlobalSign Root CA - R6 |
| 1. Certificate Issuer Field
 | CN = GlobalSignO = GlobalSignOU = GlobalSign Root CA - R6 |
| 1. Certificate Summary
 | GlobalSign Root R6 is GlobalSign’s next generation root certificate, with longer keys and signing algorithms to ensure future security of GlobalSign roots. This is the first GlobalSign root with a RSA 4096 bit key and SHA-384 signature. |
| 1. Root Certificate URL
 | http://secure.globalsign.com/cacert/root-r6.crt |
| 1. SHA1 Fingerprint
 | ‎80 94 64 0e b5 a7 a1 ca 11 9c 1f dd d5 9f 81 02 63 a7 fb d1 |
| 1. Valid from (YYYY-MM-DD)
 | 2014-12-09 |
| 1. Valid to (YYYY-MM-DD)
 | 2034-12-09 |
| 1. Certificate Version
 | 3 |
| 1. Certificate Signature Algorithm
 | SHA-384 With RSA Encryption |
| 1. Signing key parameters
 | 4096 bit RSA |
| 1. Test website URL
 | Root URL:* http://secure.globalsign.com/cacert/root-r6.crt

Test URLs:* <https://valid.r6.roots.globalsign.com/>
* <https://revoked.r6.roots.globalsign.com/>
* <https://expired.r6.roots.globalsign.com/>
 |
| 1. Example certificates
 | N/A |
| 1. Certificate Revocation Lists (CRLs)
 | URL:* <http://crl.globalsign.com/root-r6.crl>

Nextupdate:* 7 days from generation

CP Nextupdate reference:* 4.9.7
 |
| 1. OCSP
 | URI:* <http://ocsp2.globalsign.com/rootr6>

Response time:* <https://certificate.revocationcheck.com/valid.r6.roots.globalsign.com>

CP Response time reference:* 4.9.9
 |
| 1. Test Results
 | * Revocation test successful – no errors
* Certificate does not violate CA/Browser Forum Baseline Requirements
* crt.sh test successful – no errors
* PSM EV Testing successful – no errors
 |
| 1. Requested Trust Bits
 | GlobalSign is requesting the following trust bits for this root certificate:* Websites (SSL/TLS)
* Email (S/MIME)
 |
| 1. SSL Validation Type
 | The following levels of SSL validation will be used for certificates within this root’s hierarchy:* DV
* OV
* EV
 |
| 1. EV Policy OIDs
 | * CA/B: 2.23.140.1.1
* GlobalSign: 1.3.6.1.4.1.4146.1.1
 |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| * 1. CA Hierarchy
 | GlobalSign Root CA – R6 currently has the following internally-operated intermediate CAs:* GlobalSign R6 Admin CA – SHA256 – G3
* GlobalSign 4096 Administration CA
 |
| * 1. Sub CAs Operated by 3rd Parties
 | None |
| * 1. Cross-Signing
 | Cross-signed by Microsoft for CodeSigning (93:9c:69:75:32:9f:e9:e7:77:b5:80:70:4f:af:98:03:27:58:9b:b3) |
| * 1. Technical Constraints or Audits of Third-Party Issuers
 | All of GlobalSign’s root and subordinate certificates are publically disclosed on the Mozilla CCADB: http://ccadb.org/. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| 1. Documentation: CP, CPS, and Relying Party Agreements
 | * GlobalSign Document Repository: <https://www.globalsign.com/en/repository/>
	+ GlobalSign Certificate Policy: https://www.globalsign.com/en/repository/GlobalSign-CP-v5.6\_Released.PDF
	+ GlobalSign CA Certificate Practice Statement (CPS): https://www.globalsign.com/en/repository/GlobalSign-CA-CPS-v8-6\_RELEASED.pdf
* GlobalSign’s “Commitment to Comply” can be found in the Introduction section of both the CP and CPS.
 |
| 1. Audits
 | Audit report information for this root certificate is provided in the Mozilla CCADB: http://ccadb.org/.All of GlobalSign’s root and subordinate certificates are publically disclosed on the Mozilla CCADB: http://ccadb.org/.Published, non-confidential statement from WebTrust: <https://cert.webtrust.org/ViewSeal?id=2287> This report was published July 2017. |
| 1. SSL Verification Procedures
 | GlobalSign Repository: <https://www.globalsign.com/en/repository/>For the purposes of this application, CP v5.6 and CPS v8.6 were used.Domain Verification* GlobalSign CPS, Section 3.2.7, page 37
* GlobalSign CP, Section 3.2.7, page 28

Challenge Response Verification (via email):* webmaster@domain.com
* postmaster@domain.com
* admin@domain.com
* administrator@domain.com
* hostmaster@domain.com
* Any address listed as a contact field of the WHOIS record

GlobalSign has automatic blocks in place for high-profile domain names. GlobalSign flags high-risk URLs through our automated DV process, using a robust keyword database. The database is used to determine sites that are related to financial organizations or other common trade names that are likely to be targeted by Phishing scammers. If a “hit” is recorded, further manual processes are employed prior to issuing the certificate.OV Verification* GlobalSign CPS, Section 3.2.2, page 32
* GlobalSign CP, Section 3.2.2, page 24

EV Verification* GlobalSign CPS, Section 1.3.2.1, page 18; Section 3.2.3.3, page 34; Section 4.1.1, page 40; Section 6.8.2, page 61
* GlobalSign CP, Section 3.2.3.3, page 25
 |
| 1. Email Address Verification Procedures
 | GlobalSign Repository: <https://www.globalsign.com/en/repository/>For the purposes of this application, CP v5.6 and CPS v8.6 were used.GlobalSign CPS, Section 3.2.8, page 38GlobalSign CP, Section 3.2.8, page 28GlobalSign CPS, Section 3.2.3, page 33GlobalSign CP, Section 3.2.3, page 24 |
| 1. Code Signing Subscriber Verification Procedures
 | Read and understood. |
| 1. Multi-factor Authentication
 | GlobalSign uses multi-factor authentication for all accounts capable of directly causing certificate issuance. Our log-in procedures include username/password, certificate, smart card/password, and/or biometric/password authentication techniques. |
| 1. Network Security
 | GlobalSign has done, and will continue to do the following network security activities on a regular basis, according to the guidelines issued by the CA/Browser Forum:* Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.
* Check for mis-issuance of certificates, especially for high-profile domains.
* Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
* Ensure Intrusion Detection Systems and other monitoring software is up-to-date.
* Shut down certificate issuance quickly if we are alerted of intrusion.
 |

**Baseline Requirements Self-Assessment** ([https://wiki.mozilla.org/CA:BRs-Self-Assessment](https://wiki.mozilla.org/CA%3ABRs-Self-Assessment))

|  |
| --- |
| GlobalSign’s BR Self-Assessment is included as an attachment to this bug report. |

**Response to Mozilla's CA Required or Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_Practices))

|  |
| --- |
| Required Practices |
| Publicly Available CP and CPS | * Available at <https://www.globalsign.com/en/repository/>
* CP/CPS available in PDF
* CP/CPS available in English only
* CP/CPS references to Mozilla Root Store Policy:
	+ Section 1.0 – Introduction
	+ Section 3.2 – Initial Identity Validation
	+ Section 3.2.7 – Authentication of Domain Name
	+ Section 4.2.1 – Multi-factor Authentication
	+ Section 4.5.1 – Extended Key Usage
	+ Section 4.9 – Certificate Revocation and Suspension
	+ Section 5.0 – Facility, Management, and Operational Controls
	+ Section 6.1.5 – Key Sizes (SHA-1)
	+ Section 6.1.7 – Key Usage Purposes (as per X.509 v3 Key Usage Field)
	+ Section 6.3.2 – Certificate Operational Periods and Key Pair Usage Periods
	+ Section 8.0 – Compliance Audit and Other Assessments
 |
| Audit Criteria | Refer to CP/CPS Section 8 |
| Revocation of Compromised Certificates | Refer to CP/CPS Section 4.9 |
| Verifying Domain Name Ownership | Refer to CP/CPS Section 3.2.7 & 3.2.5 |
| Verifying Email Address Control | Refer to CP/CPS Section 3.2.8 |
| DNS names go in SAN | GlobalSign is fully compliant with CA/B Forum’s BRs. Refer to CP/CPS Section 3.2.4. |

|  |  |
| --- | --- |
| OCSP | GlobalSign is fully compliant with CA/B Forum’s BRs. Refer to CP/CPS Section 4.9.9. |
| Network Security Controls | GlobalSign has done, and will continue to do the following network security activities on a regular basis, according to the guidelines issued by the CA/Browser Forum:* Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.
* Check for mis-issuance of certificates, especially for high-profile domains.
* Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
* Ensure Intrusion Detection Systems and other monitoring software is up-to-date.

Shut down certificate issuance quickly if we are alerted of intrusion. |
| Recommended Practices |
| CA Hierarchy | GlobalSign currently has only one Subordinate CA under this root, which is available in the CCADB and also via the test URLs. |
| Document Handling of IDNs in CP/CPS | Refer to CPS Section 3.1.3 |

**Response to Mozilla's list of Forbidden or Problematic Practices** (<https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices>)

|  |
| --- |
| Forbidden Practices |
| Long‐lived Certificates | Not applicableNot Applicable |
| Non-Standard Email Address Prefixes for Domain Ownership Validation | Not applicable |
| Issuing End Entity Certificates Directly From Roots | Not applicable |
| Distributing Generated Private Keys in PKCS#12 Files | GlobalSign currently distributes private keys in PKCS#12 Files according to our CP/CPS 6.2. We are phasing out this practice, and will cease distributing private keys for SSL certificates in this fashion by the end of March 2018. |
| Certificates Referencing Local Names or Private IP Addresses | Not applicable |
| Issuing SSL Certificates for .int Domains | Not applicable |
| OCSP Responses Signed by a Certificate Under a Different Root | Not applicable |
| Issuance of SHA-1 Certificates | The Issuance of SHA-1 client certificates is being phased out. We expect to stop issuance in January 2018. |
| Potentially Problematic Practices |
| Delegation of Domain / Email validation to third parties | Not applicable |
| Allowing External Entities to Operate Subordinate CAs | GlobalSign allows some customers to issue SSL certificates from CAs they operate. In the case of SSL CA certificates, all CAs are technically constrained in line with the BRs. GlobalSign is in the process of transitioning all customers to hosted solutions. |
| Generic Names for CAs | Not applicable |
| Lack of Communication with End Users | Not applicable |
| Backdating the notBefore Date | Not applicable |
| Issuer Encoding in CRL | Not applicable |