Print this page

Mozilla - CA Program

Case Information

Case Number	00000233	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	GlobalSign	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Include GlobalSign Root CA - R6	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1390803

General information about CA's associated organization

CA Email Alias 1	rootembedding@globalsign.com		
CA Email Alias 2			
Company Website	https://www.globalsign.com	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Verified
Geographic Focus	USA, Global	**Verified?**	Verified
Primary Market / Customer Base	GlobalSign provides Businesses and Individuals with SSL, SMIME and code signing certificates as we have done for well over a decade.	**Verified?**	Verified
Impact to Mozilla Users	This is a root renewal request.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	1. Publicly Available CP and CPS: yes 2. Audit Criteria: CP/CPS section 8 3. Revocation of Compromised Certificates: CP/CPS section 4.9 4. Verifying Domain Name Ownership: CP/CPS section 3.2.5, 3.2.7 5. Verifying Email Address Control: CP/CPS section 3.2.8 6. DNS names go in SAN: CP/CPS section 3.2.4 7. OCSP: CP/CPS section 4.9.9 8. Network Security Controls: CP/CPS section 6.7	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: CP/CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CP/CPS section 3.2.7 3. Issuing End Entity Certificates Directly From Roots: No 4. Distributing Generated Private Keys in PKCS#12 Files: CP/CPS section 6.2. 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. 5. Certificates Referencing Local Names or Private IP Addresses: CP/CPS section 3.2.7 6. Issuing SSL Certificates for .int Domains: CP/CPS section 3.2.7 7. OCSP Responses Signed by a Certificate Under a Different Root: no 8. Issuance of SHA-1 Certificates: The Issuance of SHA-1 client certificates is being phased out. We expect to stop issuance in January 2018. 9. Delegation of Domain / Email Validation to Third Parties: 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	**Verified?**	Verified

transitioning all customers to hosted solutions.

Root Case Record # 1

Root Case Information

Root Certificate Name	GlobalSign	**Root Case No**	R00000421
Request Status	In Detailed CP/CPS Review	**Case Number**	00000233

Certificate Data

Certificate Issuer Common Name	GlobalSign
O From Issuer Field	GlobalSign
OU From Issuer Field	GlobalSign Root CA - R6
Valid From	2014 Dec 10
Valid To	2034 Dec 10
Certificate Serial Number	45e6bb038333c3856548e6ff4551
Subject	CN=GlobalSign, OU=GlobalSign Root CA - R6, O=GlobalSign, C=null
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	80:94:64:0E:B5:A7:A1:CA:11:9C:1F:DD:D5:9F:81:02:63:A7:FB:D1
SHA-256 Fingerprint	2C:AB:EA:FE:37:D0:6C:A2:2A:BA:73:91:C0:03:3D:25:98:29:52:C4:53:64:73:49:76:3A:3A:B5:AD:6C:CF:69
Certificate ID	33:FD:5F:C0:97:D4:72:DD:50:BB:C4:7E:DD:E8:54:E1:77:CB:33:DF:DB:E5:3E:41:9D:63:2E:AA:FD:61:87:8C
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	GlobalSign's root R6 is the next generation root certificate, and will	**Verified?**	Verified

	replace older, expiring roots that have smaller key sizes in the future.		
Root Certificate Download URL	http://secure.globalsign.com/cacert/root-r6.crt	**Verified?**	Verified
CRL URL(s)	http://crl.globalsign.com/root-r6.crl http://crl.globalsign.com/gsr6admincasha256g3.crl CP/CPS section 4.9.7 -- 7 days for end-entity CRL	**Verified?**	Verified
OCSP URL(s)	http://ocsp2.globalsign.com/rootr6 http://ocsp2.globalsign.com/gsr6admincasha256g3 CP/CPS section 4.9.9	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://valid.r6.roots.globalsign.com/	**Verified?**	Verified
Test Website - Expired	https://expired.r6.roots.globalsign.com/		
Test Website - Revoked	https://revoked.r6.roots.globalsign.com/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/valid.r6.roots.globalsign.com OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=18459&opt=cablint,zlint,x509lint&minNotBefore=2014-12-10 OK	**Verified?**	Verified
Test Website Lint Test	See above.	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	GlobalSign Root CA – R6 currently has the following internally-operated intermediate CAs: - GlobalSign R6 Admin CA – SHA256 – G3 - GlobalSign 4096 Administration CA All of GlobalSign's root and subordinate certificates are publically disclosed in CCADB.	**Verified?**	Verified
Externally Operated SubCAs	None in this CA Hierarchy. 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. CP/CPS section 1.1.	**Verified?**	Verified
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)	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CP/CPS section 1.3.2 Third party Issuing CAs who enter into a contractual relationship with GlobalSign CA may operate their own RA and authorize the issuance of Certificates. Third parties must comply with all the requirements of this CP and the terms of their contract which may also refer to additional criteria as recommended by the CA/BForum. RA's may implement more restrictive vetting practices if their internal policy dictates.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	**Verified?**	Verified
CA Document Repository	https://www.globalsign.com/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.globalsign.com/en/repository/GlobalSign-CP-v5.6_Released.PDF	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.globalsign.com/en/repository/GlobalSign-CA-CPS-v8-6_RELEASED.pdf	**Verified?**	Verified
Other Relevant Documents	Enterprise PKI Service Agreement: https://www.globalsign.com/repository/globalsign-epki-service-agreement.pdf Managed SSL (MSSL) Service Agreement: https://www.globalsign.com/repository/globalsign-subscriber-	**Verified?**	Verified

	agreement-managed-ssl-mssl.pdf		
Auditor (New)	BDO International Limited	**Verified?**	Verified
Auditor Location (New)	United States	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2287&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/26/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2338&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/22/2017	**Verified?**	Verified
EV SSL Audit	https://cert.webtrust.org/SealFile?seal=2288&file=pdf	**Verified?**	Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	7/26/2017	**Verified?**	Verified
BR Commitment to Comply	CP/CPS section 1.0	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8941595	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.2.7 CP section 3.2.7 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.	**Verified?**	Verified
EV SSL Verification Procedures	CPS sections 1.3.2.1, 3.2.3.3, 4.1.1, 6.8.2 CP section 3.2.3.3	**Verified?**	Verified
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CP/CPS sections 3.2.3, 3.2.8	**Verified?**	Verified

Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 6.5 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.	**Verified?**	Verified
Network Security	CP/CPS section 6.7 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.	**Verified?**	Verified