Bugzilla ID: 825954
Bugzilla Summary: Add GlobalSign's ECC Roots to Mozilla's root store

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	GlobalSign NV/SA
Website URL	https://www.globalsign.com
Organizational type	GlobalSign is a Privately owned Organization, issuing certificates to the Public.
Primark Market / Customer Base	GlobalSign provides Businesses and Individuals with SSL, SMIME and code signing certificates as we have done for well over a decade.
Impact to Mozilla Users	In the event of a security issue with RSA or a need to move to ECC for speed or compatibility reasons GlobalSign would like to move to products based around our 2012 ECC roots (We already have 3 2048 bit RSA roots embedded). Embedding these new roots prior to any known issues offers Mozilla users a better experience in the future should any issues happen requiring GlobalSign's current global customer base to update their certificates.
CA Contact Information	CA Email Alias: legal@globalsign.com CA Phone Number: 44 1622 766 766 Title / Department: Business Development

Technical information about each root certificate

Certificate Name	GlobalSign ECC Root CA - R4	GlobalSign ECC Root CA - R5
Certificate Issuer Field	CN = GlobalSign O = GlobalSign OU = GlobalSign ECC Root CA - R4	CN = GlobalSign O = GlobalSign OU = GlobalSign ECC Root CA - R5
Certificate Summary	SHA-256 ECC root that will sign internally-operated intermediate certificates.	SHA-384 ECC root that will sign internally-operated intermediate certificates.
Root Cert URL	https://secure.globalsign.net/cacert/Root-R4.crt	https://secure.globalsign.net/cacert/Root-R5.crt
SHA1 Fingerprint	69:69:56:2E:40:80:F4:24:A1:E7:19:9F:14:BA:F3:EE:58:AB:6A:BB	1F:24:C6:30:CD:A4:18:EF:20:69:FF:AD:4F:DD:5F:46:3A:1B:69:AA
Valid From	2012-11-13	2012-11-13
Valid To	2038-01-19	2038-01-19
Certificate Version	3	3
Certificate Signature Algorithm	SHA256	SHA384
Signing key parameters	ECC NIST Curve P-256	ECC NIST Curve P-384
Test Website URL (SSL)	https://2038r4.globalsign.com/	https://2038r5.globalsign.com/

CRL URL	http://crl.globalsign.com/gs/root-r4.crl CPS 4.9.7: online CAs have CRLs, published every 3 hours and are valid for 1 week.	http://crl.globalsign.com/gs/root-r5.crl CPS 4.9.7: online CAs have CRLs, published every 3 hours and are valid for 1 week.
OCSP URL	http://ocsp2.globalsign.com/ecadminca1sha2g2	http://ocsp2.globalsign.com/ecadminca2sha2g2
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	1.3.6.1.4.1.4146.1.1	1.3.6.1.4.1.4146.1.1

CA Hierarchy information for each root certificate

CA Hierarchy	Roots certs are offline and will sign internally operated intermediate certificates. No plans have been made for these roots regarding specific products or services. In a worst case scenario where RSA is deemed insecure then ECC products will need to replace all current products. It is unlikely that this root will be used to sign 3rd parties as the ubiquity will not be sufficient for several years.
Externally Operated SubCAs	None. None planned.
Cross-Signing	None.

Verification Policies and Practices

Policy Documentation	All GlobalSign's documentation is in English and is here: https://www.globalsign.com/repository/
Audits	Auditor: Ernst & Young WebTrust for CA: https://cert.webtrust.org/SealFile?seal=1511&file=pdf (2013.06.19) WebTrust for BR: https://cert.webtrust.org/SealFile?seal=1515&file=pdf (2013.06.19) WebTrust for EV: https://cert.webtrust.org/SealFile?seal=1514&file=pdf (2013.06.19) These new roots will be included in the 2014 audit, which are expected to be available at the end of July 2014.
Baseline Requirements (SSL)	CPS section 1.0: GlobalSign CA conforms to the latest version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at www.cabforum.org. In the event that a discrepancy arises between interpretations of this document and Baseline Requirements, the Baseline Requirement shall govern.
SSL Verification Procedures	The domain verification is in section 3.2.2 We confirm that we have automatic blocks in place for high value brands and domains. For OV vetting details are in section 3.2.2 In order to understand our processes as a whole then section 3.2 must be reviewed EV practices are provided in the CABForum EV guidelines and are not therefore duplicated into the GlobalSign CPS. Section 3.2.2.3 makes this statement.
Organization Verification Procedures	CPS section 3.2.2
Email Address Verification Procedures	Section 3.2.3 relates to e-mail products. The Applicant is required to demonstrate control of any email address to be included within a certificate.

Code Signing Subscriber Verification Procedures	Verification of organization and authorization is covered in section 3.2.
Multi-factor Authentication	CPS section 6 GlobalSign uses multi factor authentication systems for it's own internal processes. GlobalSign's end customers are provided with an account that is locked to a specific domain/e-mail address that will have been verified prior to any initial issuance of a certificate. Re-issuance (Re-Key within the operating period of an issued certificate) is covered in the CPS with authentication into the account via a user name and password. Re-new is currently not supported. Full validation is necessary.
Network Security	CPS section 6.7

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	See above
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	IDN not currently supported
Revocation of Compromised Certificates	Yes
Verifying Domain Name Ownership	Yes
Verifying Email Address Control	Yes
Verifying Identity of Code Signing Certificate Subscriber	Yes
DNS names go in SAN	Comment #3: The FQDN is always placed into the SAN. • CPS section 3.1.1: In the case of SSL certificates, whilst the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field, it may also be duplicated into the Subject Alternative Name extension along with a www version of the DNS-ID. Subject Alternative Names are marked non critical in line with RFC5280. • Comment #3: I'll ask the Policy Authority to address the language here. The FQDN is "always" placed into the SAN. It's a www version which may also be included and this should be the language in the CPS. Thanks for highlighting it's not clearly written.
Domain owned by a Natural Person	Not applicable. SSL certs are only issued to organizations.
OCSP	See above

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	GlobalSign meets the needs of the Base requirements on Certificate duration.
Wildcard DV SSL certificates	**GlobalSign currently issues Wildcard DV certificates. We currently do not share the same concern as Mozilla on this point and therefore do not plan to deprecate this product type.** CPS section 3.1.1: Wildcard SSL Certificates include a wildcard asterisk character. Before issuing a

	certificate with a wildcard character (*) GlobalSign CA follows best practices to determine if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix". (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation.) and if it does, it will reject the request as the domain space must be owned or controlled by the subscriber. e.g. *.globalsign.com
Email Address Prefixes for DV Certs	GlobalSign meets the needs of the Base requirements for e-mail challenges
Delegation of Domain / Email validation to third parties	GlobalSign does it's own verification for all products. This includes managed services for SSL and SMIME on behalf of enterprise clients. (Section 3.2.3.4 of our CPS discusses this in detail)
Issuing end entity certificates directly from roots	GlobalSign does not issue from it's roots unless a test is needed such as these ECC test certificates.
Allowing external entities to operate subordinate CAs	GlobalSign's program for external entities (RootSign) has been in operation for 10+ years and as highlighted by the responses above, the program is migrating to a new policy of Name Constraints or 3rd party audit under the title Trusted Root.
Distributing generated private keys in PKCS#12 files	GlobalSign provides pfx files to customers. We created and reviewed the process with our auditors in 2007 (Deloitte) and again when we moved to E&Y in 2008. **GlobalSign's solution for SSL is known as AutoCSR and is covered in our CPS in section 6.1.2 on page 45.**
Certificates referencing hostnames or private IP addresses	**GlobalSign provides OV certificates which may include Internal IP address and/or hostnames**. Section 3.2.4 covers these non verifiable items. Our application systems prevent applicants from using Internal IP addresses and Hostnames within DV certificates. Issuing SSL Certificates for Internal Domains - GlobalSign provides OV certificates which may include Internal domains. Section 3.2.4 covers these non verifiable items. Our application systems prevent applicants from using Internal domains within DV certificates.
Issuing SSL Certificates for Internal Domains	See above
OCSP Responses signed by a certificate under a different root	Not applicable as we use the same keys for OCSP and CRL as for the issuance of the certificate.
CRL with critical CIDP Extension	Not applicable as we use full CRLs
Generic names for CAs	Our Roots are names as GlobalSign. GlobalSign is a global brand and has presence in >10 countries so we choose to use the global brand name.
Lack of Communication With End Users	GlobalSign tries to be responsive to users and relying parties. This offers a crowd sourcing capability that helps to identify problems. i.e. this issue is not applicable.