GlobalSign
GMO Internet Group

over **10 years** of securing
identities, web sites & transactions

GlobalSign Root Certificates – 2014+

Platform owners focusing on the lifecycle management of root certificates within their root stores should consider several key issues and trends that ultimately affect system performance and speed for relying parties noting that an incorrect choice could adversely affect brand perception. Root store owners should ideally be focused on the immediate needs of their relying parties as error messages today can lead to a loss of customers to an alternative product. However in saying this owners should also be mindful to ensure that Root Stores remain flexible in terms of overall capacity and technology choices. Restricting Certificate Authorities ability to embed sufficient choices could damage future platform flexibility. In the case of Root Certificates where Disaster Recovery planning is essential then less is most certainly not more! GlobalSign's Root Certificate Policy Authority 4 (From WebTrust 2.0) is directly responsible for the ongoing policy, procedure and control of the range of root certificates which GlobalSign offers. GlobalSign's 5 root certificates (together with a future 4096 bit RSA certificate due in Q2 2014) will provide the necessary longevity you need for your platform to be recognized by GlobalSign's ever expanding customer base. With one of the most ubiquitous 2048 bit SHA1 RSA roots in the industry, GlobalSign already secures many of the world's leading brands. A 2048 bit SHA256 RSA alternative was added in 2009 that is now present in the majority of the systems that support the SHA2 hashing algorithm. With two new ECC alternatives added in 2012, GlobalSign is poised to continue its ongoing strategy for root embedment.

Our current ubiquity is detailed here:- http://www.globalsign.com/resources/ssl_root_compatibility.pdf

Microsoft implemented a dynamic root store across their product range (desktop, server and mobile) and as such this offers the maximum flexibility to relying parties and future potential issues with Cryptography choices. i.e. It's possible to easily add new providers without relying parties needing to update to a complete new platform. Microsoft introduced their dynamic store capabilities with Vista allowing new root certificates to be dynamically downloaded by the OS at the point of reliance (SSL session. Encrypted e-mail receipt, code signed executable etc). Other providers such as Adobe are following suit. Their AATL (Adobe Authorized Trust List) for example, is also dynamic from 9.1.2 onwards.

GlobalSign's EV OID

GlobalSign provides Extended Validation SSL certificates with the following OID across all roots.

1.3.6.1.4.1.4146.1.1 http://www.oid-info.com/get/1.3.6.1.4.1.4146.1.1

Contact Details:-

For additional information and a root embedding agreements please contact our generic e-mail contact address rootembedding@globalsign.com. This e-mail address is monitored by the Policy Authority and serves as a single point of contact for all Root Embedding Issues

Expanded Information – GlobalSign's Roots:-

*GlobalSign Root CA **R1** (2048 bit RSA SHA1)*

The 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. All legal documents are located in the repository: http://www.globalsign.com/repository/. The root uses the same key material as the GlobalSign Root CA.

Key extensions

- basicConstraints: CA: true
- keyUsage: keyCertSign, cRLSign

Example SSL/TLS certificate

https://2028.globalsign.com

Example SSL/TLS certificate to support Extended Validation

https://2028ev.globalsign.com

Subject DN

CN = GlobalSign Root CA
OU = Root CA
O = GlobalSign nv-sa
C = BE

Serial Number

04 00 00 00 00 01 15 4b 5a c3 94

Subject KeyID

60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b

Validity time

Valid from : 01 September 1998 12:00:00
Valid to : 28 January 2028 12:00:00

Fingerprints

SHA1 = B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

URL to online CRL repository

http://crl.globalsign.net/root.crl

URL to secure online location of the root

https://secure.globalsign.net/cacert/Root-R1.crt

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----
```

GlobalSign Root CA R2 (2048 bit RSA SHA1)

The 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. All legal documents are located in the repository: http://www.globalsign.com/repository/.

Key extensions

- basicConstraints: CA: true
- keyUsage: keyCertSign, cRLSign

Example SSL/TLS certificate
https://2021.globalsign.com
Subject DN
CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA - R2
Subject KeyID
9b e2 07 57 67 1c 1e c0 6a 06 de 59 b4 9a 2d df dc 19 86 2e
Serial Number
04 00 00 00 00 01 0f 86 26 e6 0d
Validity time
Valid from : 15 December 2006 08:00:00
Valid to : 15 December 2021 08:00:00
Fingerprints
SHA1 = 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE
URL to online CRL repository
http://crl.globalsign.net/root-r2.crl
URL to secure online location of the root
https://secure.globalsign.net/cacert/Root-R2.crt

```
-----BEGIN CERTIFICATE-----
MIIDujCCAqKgAwIBAgILBAAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDAwWhcNMjExMjE1
MDgwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEG
A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAKbPJA6+Lm8omUVCxKs+IVSbC9N/hHD6ErPL
v4dfxn+G07IwXNb9rfF73OX4YJYJkhD10FPe+3t+c4isUoh7SqbKSaZeqKeMWhG8
eoLrvozps6yWJQeXSpkqBy+0Hne/ig+1Anwblrj FuTosvNYSuetZfeLQBoZfXklq
tTleiDTsvHgMCJiEbKjNS7SgfQx5TfC4LcshytVsW33hoCmEofnTlEnLJGKRILzd
C9XZzPnqJworc5HGnRusyMvo4KD0L5CLTfuwNhv2GXqF4G3yYROIXJ/gkwpRl4pa
zq+r1feqCapgvdzZX99yqWATXgAByUr6P6TqBwMhAo6CygPCm48CAwEAAaOBnDCB
mTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUm+IH
V2ccHsBqBt5ZtJot39wZhi4wNgYDVR0fBC8wLTAroCmgJ4YlaHR0cDovL2NybC5n
bG9iYWxzaWduLm5ldC9yb290LXIyLmNybDAfBgNVHSMEGDAWgBSb4gdXZxwewGoG
3lm0mi3f3BmGLjANBgkqhkiG9w0BAQUFAAOCAQEAmYFThxxol4aR7OBKuEQLq4Gs
J0/WwbgcQ3izDJr86iw8bmEbTUsp9Z8FHSbBuOmDAGJFtqkIk7mpM0sYmsL4h4hO
291xNBrBVNpGP+DTKqttVCL1OmLNIG+6KYnX3ZHu01yiPqFbQfXf5WRDLenVOavS
ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/N5GJG79G+dwfCMNYxd
AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7
TBj0/VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==
-----END CERTIFICATE-----
```

GlobalSign Root CA R3 (2048 bit RSA SHA256)

The 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. All legal documents are located in the repository: http://www.globalsign.com/repository/.

Key extensions

- basicConstraints: CA: true
- keyUsage: keyCertSign, cRLSign

Example SSL/TLS certificate
https://2029.globalsign.com

Signature Algorithm
sha256WithRSAEncryption

Subject DN
CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA – R3

Serial Number
04 00 00 00 00 01 21 58 53 08 A2

Subject KeyID
8f f0 4b 7f a8 2e 45 24 ae 4d 50 fa 63 9a 8b de e2 dd 1b bc

Validity time
Valid from : 18th March 2009 10:00:00
Valid to : 18th March 2029 10:00:00

Fingerprints
SHA1 = D6 9B 56 11 48 F0 1C 77 C5 45 78 C1 09 26 DF 5B 85 69 76 AD

URL to online CRL repository
http://crl.globalsign.net/root-r3.crl

URL to online location of the root
http://secure.globalsign.net/cacert/Root-R3.crt

```
-----BEGIN CERTIFICATE-----
MIIDXzCCAkegAwIBAgILBAAAAAABIVhTCKIwDQYJKoZIhvcNAQELBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjMxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDkwMzE4MTAwMDAwWhcNMjkwMzE4
MTAwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMzETMBEG
A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMwldpB5BngiFvXAg7aEyiie/QV2EcWtiHL8
RgJDx7KKnQRfJMsuS+FggkbhUqsMgUdwbN1k0ev1LKMPgj0MK66X17YUhhB5uzsT
gHeMCOFJ0mpiLx9e+pZo34knlTifBtc+ycsmWQ1z3rDI6SYOgxXG71uL0gRgykmm
KPZpO/bLyCiR5Z2KYVc3rHQU3HTgOu5yLy6c+9C7v/U9AOEGM+iCK65TpjoWc4zd
QQ4gOsC0p6Hpsk+QLjJg6VfLuQSSaGjlOCZgdbKfd/+RFO+uIEn8rUAVSNECMWEZ
XriX7613t2Saer9fwRPvm2L7DWzgVGkWqQPabumDk3F2xmmFghcCAwEAAaNCMEAw
DgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFI/wS3+o
LkUkrk1Q+mOai97i3Ru8MA0GCSqGSIb3DQEBCwUAA4IBAQBLQNvAUKr+yAzv95ZU
RUm7lgAJQayzE4aGKAczymvmdLm6AC2upArT9fHxD4q/c2dKg8dEe3jgr25sbwMp
jjM5RcOO5LlXbKr8EpbsU8Yt5CRsuZRj+9xTaGdWPoO4zzUhw8lo/s7awlOqzJCK
6fBdRoyV3XpYKBovHd7NADdBj+1EbddTKJd+82cEHhXXipa0095MJ6RMG3NzdvQX
mcIfeg7jLQitChws/zyrVQ4PkX4268NXSb7hLi18YIvDQVETI53O9zJrlAGomecs
Mx86OyXShkDOOyyGeMlhLxS67ttVb9+E7gUJTb0o2HLO02JQZR7rkpeDMdmztcpH
WD9f
-----END CERTIFICATE-----
```

GlobalSign ECC Root CA R4 (SHA256 256bit ECC)

The 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. All legal documents are located in the repository: http://www.globalsign.com/repository/. The root is based on Elliptic Curve Cryptography.

Key extensions

- basicConstraints: CA: true
- keyUsage: keyCertSign, cRLSign

Example SSL/TLS certificate
https://2038r4.globalsign.com
Subject DN
CN = GlobalSign
O = GlobalSign
OU = GlobalSign ECC Root CA – R4
Serial Number
2a 38 a4 1c 96 0a 04 de 42 b2 28 a5 0b e8 34 98 02
Subject KeyID
54 b0 7b ad 45 b8 e2 40 7f fb 0a 6e fb be 33 c9 3c a3 84 d5
Validity time
Valid from : 13 November 2012 00:00:00
Valid to : 19 January 2038 03:14:07
Fingerprints
SHA1 = 69 69 56 2e 40 80 f4 24 a1 e7 19 9f 14 ba f3 ee 58 ab 6a bb
URL to online CRL repository
http://crl.globalsign.com/root-r4.crl
URL to secure online location of the root
https://secure.globalsign.net/cacert/Root-R4.crt

```
-----BEGIN CERTIFICATE-----
MIIB4TCCAYegAwIBAgIRKjikHJYKBN5CsiilC+g0mAIwCgYIKoZIzj0EAwIwUDEk
MCIGA1UECxMbR2xvYmFsU2lnbiBFQ0MgUm9vdCBDQSAtIFI0MRMwEQYDVQQKEwpH
bG9iYWxTaWduMRMwEQYDVQQDEwpHbG9iYWxTaWduMB4XDTEyMTExMzAwMDAwMFoX
DTM4MDExOTAzMTQwN1owUDEkMCIGA1UECxMbR2xvYmFsU2lnbiBFQ0MgUm9vdCBD
QSAtIFI0MRMwEQYDVQQKEwpHbG9iYWxTaWduMRMwEQYDVQQDEwpHbG9iYWxTaWdu
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEuMZ5049sJQ6fLjkZHAOkrprlOQcJ
FspjsbmG+IpXwVfOQvpzofdlQv8ewQCybnMO/8ch5RikqtlxP6jUuc6MHaNCMEAw
DgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFFSwe61F
uOJAf/sKbvu+M8k8o4TVMAoGCCqGSM49BAMCA0gAMEUCIQDckqGgE6bPA7DmxCGX
kPoUVy0D7O48027KqGx2vKLeuwIgJ6iFJzWbVsaj8kfSt24bAgAXqmemFZHe+pTs
ewv4n4Q=
-----END CERTIFICATE-----
```

GlobalSign ECC Root CA R5 (SHA384 384bit ECC)

The 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. All legal documents are located in the repository: http://www.globalsign.com/repository/. The root is based on Elliptic Curve Cryptography.

Key extensions

- basicConstraints: CA: true
- keyUsage: keyCertSign, cRLSign

Example SSL/TLS certificate
https://2038r5.globalsign.com
Subject DN
CN = GlobalSign
O = GlobalSign
OU = GlobalSign ECC Root CA – R5
Serial Number
60 59 49 e0 26 2e bb 55 f9 0a 77 8a 71 f9 4a d8 6c
Subject KeyID
3d e6 29 48 9b ea 07 ca 21 44 4a 26 de 6e de d2 83 d0 9f 59
Validity time
Valid from : 13 November 2012 00:00:00
Valid to : 19 January 2038 03:14:07
Fingerprints
SHA1 = 1f 24 c6 30 cd a4 18 ef 20 69 ff ad 4f dd 5f 46 3a 1b 69 aa
URL to online CRL repository
http://crl.globalsign.com/root-r5.crl
URL to secure online location of the root
https://secure.globalsign.net/cacert/Root-R5.crt

```
-----BEGIN CERTIFICATE-----
MIICHjCCAaSgAwIBAgIRYFlJ4CYuu1X5CneKcflK2GwwCgYIKoZIzj0EAwMwUDEk
MCIGA1UECxMbR2xvYmFsU2lnbiBFQ0MgUm9vdCBDQSAtIFI1MRMwEQYDVQQKEwpH
bG9iYWxTaWduMRMwEQYDVQQDEwpHbG9iYWxTaWduMB4XDTEyMTExMzAwMDAwMFoX
DTM4MDExOTAzMTQwN1owUDEkMCIGA1UECxMbR2xvYmFsU2lnbiBFQ0MgUm9vdCBD
QSAtIFI1MRMwEQYDVQQKEwpHbG9iYWxTaWduMRMwEQYDVQQDEwpHbG9iYWxTaWdu
MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAER0UOlvt9Xb/pOdEh+J8LttV7HpI6SFkc
8GIxLcB6KP4ap1yztsyX50XUWPrRd21DosCHZTQKH3rd6zwzocWdTaRvQZU4f8ke
hOvRnkmSh5SHDDqFSmafnVmTTZdhBoZKo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUPeYpSJvqB8ohREom3m7e0oPQn1kwCgYI
KoZIzj0EAwMDaAAwZQIxAOVpEslu28YxuglB4Zf4+/2a4n0Sye18ZNPLBSWLVtmg
515dTguDnFt2KaAJJiFqYgIwcdK1j1zqO+F4CYWodZI7yFz9SO8NdCKoCOJuxUnO
xwy8p2Fp8fc74SrL+SvzZpA3
-----END CERTIFICATE-----
```