![GlobalSign GMO Internet Group]

GlobalSign Intermediate Root CA Certificates

All customers installing a GlobalSign SSL Certificate will need to install the appropriate Intermediate root CA onto their web servers. The installation needs to only be conducted once. Once installed, all browsers, applications and mobiles that recognize GlobalSign will trust GlobalSign SSL Certificates. If customers do not install the appropriate Intermediate root CA certificate, browsers, applications and mobiles will not be able to recognize GlobalSign SSL Certificates as being trusted. The Intermediate root CA certificates need only be installed on the web server and are NOT needed to be installed by visitors to your web site.

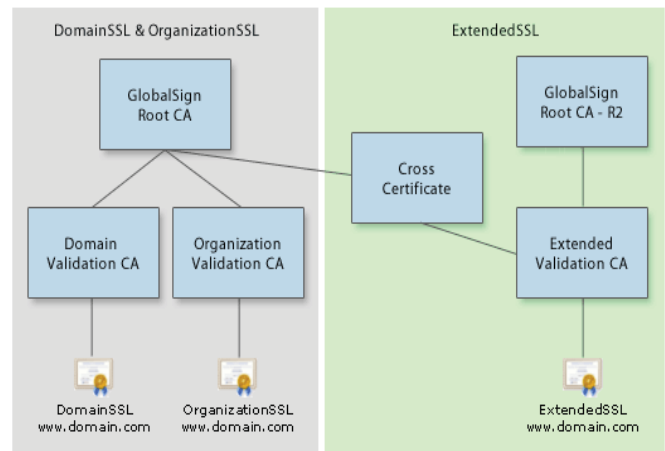## Why does GlobalSign use Intermediate Root CA Certificates?

GlobalSign has always adopted a high security model when issuing digital certificates. We use a trust chain that ensures that the primary GlobalSign root CA (i.e. the certificate that is pre-installed with all browsers, applications and mobiles) is "offline" and kept in a highly secure environment with stringently limited access. This means the root CA is not used to directly sign end entity SSL Certificates, as such GlobalSign employs a best practices approach for its Public Key Infrastructure therefore protecting against the major effects of a "key compromise". For example, a key compromise of the Root CA would render the root and all certificates issued by the root untrustworthy, and because we keep our root offline this (somewhat unlikely event) is significantly less likely to happen.

The use of Intermediate root CAs is utilized by all major Certification Authorities because of the extra security level they provide. Both GlobalSign and VeriSign have long adopted the use of Intermediate root CA certificates

The GlobalSign Intermediate root CA Certificates for SSL products differ depending on your SSL Certificate. GlobalSign uses a number of Intermediate root CAs, for example:

○ For DomainSSL customers, you must install your DomainSSL Certificate and the Domain Validation CA Certificate (the Intermediate Root CA) onto your web server.

○ For OrganizationSSL customers, you must install your OrganizationSSL Certificate and the Organization Validation CA Certificate (the Intermediate Root CA) onto your web server.

○ For ExtendedSSL customers, you must install your ExtendedSSL Certificate and BOTH the Extended Validation CA Certificate (the Intermediate Root CA) and the Cross Certificate onto your web server.

Graphical Representation of the GlobalSign SSL Root CA Certificate Hierarchy

The diagram shows the high security CA root hierarchy (Public Key Infrastructure) deployed by GlobalSign. Note that the Domain Validation CA, Organization Validation CA and Extended Validation CA are all unique Intermediate Root CAs linked either directly, or via the Cross Certificate to the trusted GlobalSign Root CA and the newer GlobalSign Root CA - R2 (used at present only for issuing Extended Validation SSL Certificates).

Learn More

For further information about installing GlobalSign Intermediate Root CA Certificates please visit
http://www.globalsign.com/support/intermediate-root-install.html
or contact support@globalsign.com

SSL Certs
Code Signing
Doc Signing
Digital IDs

A Leader in Online Security & Authentication Solutions for over 10 years