



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



GlobalSign Trusted Root™

Global acceptance and trust for your Microsoft CA or Inhouse CA

In recent years many enterprises and major organisations have established their own Enterprise Certificate Authority (CA) such as the Microsoft CA with the primary goal of enhancing security for an ever increasing number of diverse web based business processes. For an enterprise to establish their own Enterprise CA it must self-sign a CA Root Certificate, which is then used to issue digital certificates to employees, extranet users and even machines and services. Such certificates can then be used to digitally sign and encrypt communications and also to control access to web resources. However this self-signed Root CA Certificate is not automatically trusted by main-stream operating systems (such as Microsoft Windows), browsers (such as Microsoft Internet Explorer, Mozilla Firefox) or email clients (such as Microsoft Outlook). This inability to trust causes warning messages to be displayed, resulting in a lack of confidence by staff and increased cost for support and training.

To avoid these warnings the enterprise would be forced to either accept the increased support costs or to undertake a Root Embedding program to have the self-signed Root CA Certificate inserted into all operating systems, browsers and applications. Such a program is expensive and labour intensive, taking many years before the enterprise's Root CA Certificate is sufficiently

ubiquitous to be used without support issues. The time and cost associated with an Embedding Program massively outweigh any advantage that would be associated with implementing an Enterprise CA solution.

Today, there is no need for such CAs to have their Root Certificate directly embedded in browsers to create the necessary feeling of trust. GlobalSign has made available a simple solution for CAs to chain themselves under GlobalSign's embedded Root Certificate: Trusted Root™.

As a leading WebTrust accredited Certification Authority, GlobalSign has maintained its own pioneering Root Embedding program GlobalSign Ready for over 10 years and now the GlobalSign Root CA Certificate is trusted by practically all mainstream browsers and applications. With GlobalSign's Trusted Root there is no need for individual Enterprise CAs to have their own Embedding program, instead GlobalSign allows use of its own ubiquitous Root CA certificate to give the customer its own set of new, but highly trusted, Root CA certificates. The customer then immediately inherits the trust associated with the GlobalSign Root CA which provides an easy way for certificates issued by the enterprise to be transparently accepted in all popular applications, thereby eliminating the costly support issues.

Features & Benefits

Global Recognition & Acceptance

Trusted Root permits Certification Authorities operated by enterprises to be accepted by all browser and mail client software dating back many years. Consequently, all certificates issued to the enterprises community through the Microsoft CA or inhouse CA will gain the inherent trust provided by 10 years plus of GlobalSign's own root embedding program - GlobalSign Ready.

Greatly reduces support costs

Rolling out a PKI with an untrusted root certificate is costly - administrators are needed to install the enterprise's own root certificate on each machine within the community (employees, extranet users etc). This activity is costly and inconvenient. Trusted Root removes the need to install any enterprise root certificates as Trusted Root causes all certificates to be inherently trusted.

Trusted & Independent CA Deployment

By having its Root Certificate accepted and trusted by all standard browser software, the Microsoft CA or inhouse CA can easily perform:

Certificate Management

The Microsoft CA or inhouse CA is able to issue, publish & revoke trusted certificates completely independently from GlobalSign or any other trusted CA.

Independent Policies

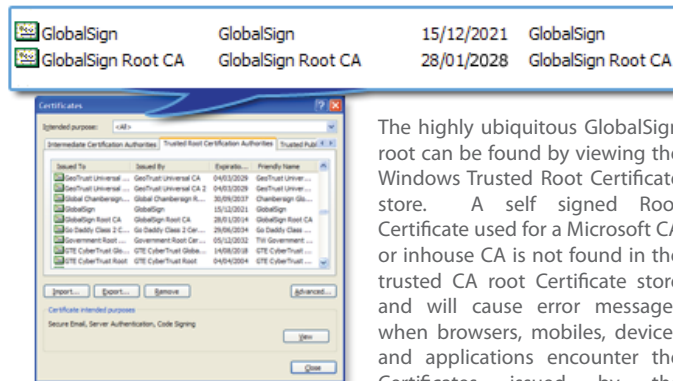
This signifies that the enterprise determines Key Management Policies, Secure Infrastructure Policies & Organizational Policies independently from but approved by GlobalSign.

Brand Name Management & True Certificate White Labeling

The Microsoft CA or inhouse CA uses its own brand name for the certificate issuing, management & revocation as the certificates will not be GlobalSign branded or co-branded.

The Strongest SSL Security

Every GlobalSign SSL Certificate is capable of 256 bit strong SSL, and includes step-up SGC technology that forces weak 40 bit browsers to connect at stronger 128 bit encryption strength.



The highly ubiquitous GlobalSign root can be found by viewing the Windows Trusted Root Certificate store. A self signed Root Certificate used for a Microsoft CA or inhouse CA is not found in the trusted CA root certificate store and will cause error messages when browsers, mobiles, devices and applications encounter the Certificates issued by the Microsoft CA or inhouse CA.

Who Should Use Trusted Root?

Public Certification Authorities

- Where the use of of Public Key Infrastructure to support standards, regulation and internal security policies - incorporating verticals such as education, notary, industry specific, financial, etc.

Enterprise Certification Authorities, where drivers include

- Compliance requirement for strong authentication to extranets
- Passwords no longer acceptable Partner management / customer management
- eProcurement procedures and new workflow processes drive the need for digital signatures

GlobalSign Ready™

Ensuring the highest recognition for Trusted Root users

GlobalSign is a focused enterprise and Internet security company and has been operating a dedicated root embedding program for over a decade. The GlobalSign Ready program ensures the GlobalSign root is present in all known browsers, Operating Systems, applications and mobile devices around the world. The GlobalSign Ready program is managed by all the International GlobalSign offices (US, UK, Continental Europe, Japan & China). The advantage of multiple International offices is simple - each region ensures extensive support

for GlobalSign certificates in region specific new devices and applications. This approach ensures GlobalSign certificates deliver the highest level of support for our customers, even "niche" new devices and applications, wherever the device manufacturer or software vendor may be based. This unique global approach ensures the best customer experience and sets GlobalSign valuable ubiquity points ahead of other Certification Authorities.

Supported Browsers, Applications & Mobile Devices

Extended Validation Browsers

- Microsoft Internet Explorer 7 (Vista)
- Microsoft Internet Explorer 7* (Windows XP)
- Opera 9.5

Web Browsers (SSL/TLS enabled)

- Microsoft Internet Explorer (IE) 5.01+
- Netscape Communicator 4.51+
- Mozilla Firefox 1.0+
- AOL 5+
- Opera 6.1+
- Apple Safari 1.0+
- Red Hat Linux Konqueror (KDE)
- Microsoft WebTV
- Camino

Email Clients (S/Mime)

- Microsoft Outlook 99+
- Microsoft Entourage (OS/X)
- Netscape Communicator 4.51+
- Mozilla Thunderbird 1.0+
- Qualcomm Eudora 6.2+
- Lotus Notes (6+)

Micro Browsers & Handsets (SSL/TLS enabled)

- Netfront 3.0+
- Opera 4.10+
- Apple iPhone Safari
- Microsoft Windows Mobile 5/6
- Microsoft Internet Explorer Pocket PC 2003
- Microsoft Internet Explorer Smartphone 2003
- Sony PlayStation Portable
- Sony PlayStation 3
- RIM Blackberry 4.3.0
- Brew
- PalmOS 5.x
- Openwave mobile browser 6.20+
- Major Network Operators inc. Vodafone, Orange, AT&T
- Major Handset providers SonyEricsson, Nokia, Alcatel & Palm
- (S40/S60/S80/OSSO) based Handsets from 2002

Application Suites

- Mozilla Suite v0.9.8+
- Sun Java SE (1.4.2 Update 16+, 5.0 Update 13+, 6 Update 3+)
- SeaMonkey
- OpenSSL.org's OpenSSL v0.9.5+
- Adobe AIR



GlobalSign has been a WebTrust compliant Certification Authority since 2002 - representing one of the longest serving WebTrust compliant Certification Authorities worldwide. WebTrust compliancy assures customers that GlobalSign has successfully been audited against the highest levels of practice for customer authentication procedures, physical, network and logical security surrounding the certificate issuance infrastructure, handling of customer data and business continuity planning.

Contact us today to discuss your specific requirements on Trusted Root for Microsoft CA and other inhouse CAs.

GlobalSign N.V.

UbiCenter, Philipssite 5
 3001 Leuven, Belgium
 TEL: +32 16 89 19 00 FAX: +32 16 28 74 04

<http://eu.globalsign.com>



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