Trusted Root

Global acceptance and trust for your Microsoft CA or Inhouse CA

What is Trusted Root?

Trusted Root enables Enterprises to setup their own internal Certificate Authority that is chained to the GlobalSign root, giving full global acceptance by all browsers, mail clients, and devices. TrustedRoot certifies the root of an existing CA (or PKI infrastructure) to extend the certification path to GlobalSign's root, hence allowing immediate inherited trust, providing an easy way for certificates issued by the enterprise to be transparently accepted in all popular applications, thereby eliminated the costly support issues.

Who should use TrustedRoot?

Enterprises interested in having their own internal CA or using Microsoft CA

Enterprises interested in having their own internal CA or using Microsoft CA that want to avoid untrust messages or having to incur the increased support cost of having self-signed certificates inserted into all operating systems, browsers, and applications.

Enterprises currently using self-signed Certificates

Self-signed root Certificates are not automatically trusted by operating systems (such as Microsoft Windows), browsers (such as Microsoft Internet Explorer), or email clients (such as Outlook). Therefore, enterprises using self-signed root certificates would have to be forced to accept the increased support to have the self-signed root CA Certificate distributed to all clients and inserted into all operating systems, browsers, and applications.

Such a program is expensive and labor intensive, using Trusted Root from GlobalSign allows you to use a root certificate that is already trusted in all operating systems, browsers, applications, and devices.

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 in-house CA is not found in the Trusted Root Certificate store and will cause error messages when browsers, mobiles, devices and applications encounter the Certificates issued by the Microsoft CA or in-house CA.

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

Because GlobalSign's Root Certificate is 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.

Supported Browsers, Applications & Mobile Devices

Extended Validation Browsers
- Microsoft Internet Explorer 7+ (Vista)
- Microsoft Internet Explorer 7+ (XP)*
- Opera 9.5+
- Firefox 3+
- Google Chrome 0.3.154.9 +
- Apple Safari 3.2 +
- Apple iOS 4.0 +

Web Browsers (SSL/TLS enabled)
- Microsoft Internet Explorer (IE) 5.01+
- Mozilla Firefox 1.0+
- Opera 6.1+
- Apple Safari 1.0+
- Google Chrome
- AOL 5+
- Netscape Communicator 4.51+
- Red Hat Linux Konqueror (KDE)
- Microsoft WebTV
- Camino
- Konqueror (KDE) 2.0.0 +

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

Mobile, OSs, Micro Browsers, Handsets & Game Consoles
- Apple iPhone, iPod Safari
- Microsoft Windows Mobile 5/6
- Microsoft Windows CE 4.0
- Microsoft Internet Explorer Pocket PC 2003
- Microsoft Internet Explorer Smartphone 2003
- RIM Blackberry 4.3.0
- NTT / DoCoMo
- SoftBank Mobile
- KDDI
- Brew
- PalmOS 5.x
- Netfront 3.0+
- Opera 4.10+
- Openwave mobile browser 6.20+
- Major Operators inc. Vodafone, Orange, AT&T
- Major Handset providers SonyEricsson, Nokia, Alcatel & Palm (S40/S60/S80/OSSO) based Handsets from 2002
- Sony PlayStation Portable
- Sony PlayStation 3
- Nintendo Wii

Document Security Platforms
- Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath)

Application Suites
- Microsoft Authenticode & Visual Basic for Applications (VBA)
- Adobe AIR
- Sun Java JRE (1.4.2 Update 16+, 5.0 Update 13+,6 Update 3+)
- Mozilla Suite v0.9.8+
- SeaMonkey
- OpenSSL.org's OpenSSL v0.9.5+
- Google Checkout

Major Operating Systems
- Microsoft Windows XP, Vista and 7 (all versions inc 32/64 bit)
- Apple MAC OS 9.0+ (circa 2002), includes 10.5.X and 10.6.X
- All Major Linux Distributions (Debian, Ubuntu etc)

Default API Support within Hosting Control Panels
- WHMCS
- Ubersmith

1-877-775-4562
www.globalsign.com