GlobalSign
GMO INTERNET GROUP

DATASHEET

Certificate-based Authentication

Keep the Right Users and Devices In; Keep the Wrong Ones Out

Passwords are no longer a reliable method of user authentication. The growing threat of rogue machines from malicious parties and employee's who desire to bring-your-own-device (BYOD) has many in IT wondering how they can control which users and machines can access and operate on their networks. Using Digital Certificates as an authentication factor allows IT to identify endpoints and restrict access to only approved users, machines and devices.

What is Certificate-based Authentication?

Certificate-based authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc. In the case of user authentication, it is often deployed in coordination with traditional methods such as username and password. One differentiator of certificate-based authentication is that unlike some solutions that only work for users, such as biometrics and one time passwords (OTP), the same solution can be used for all endpoints – users, machine, devices and even the growing Internet of Things (IoT).

BENEFITS

- EASE OF DEPLOYMENT AND ONGOING MANAGEMENT
  GlobalSign's cloud-based certificate management platform and optional Active Directory and MDM integrations make it easy for administrators to issue and revoke certificates as needed
- ONE SOLUTION FOR ALL ENDPOINTS
  Certificates can be issued to all endpoints, including users, machines and devices
- NO ADDITIONAL HARDWARE
  Saves on costs, alleviates token management pains and is easy for users (note: for higher assurance use cases, certificates can be part of cryptographic hardware)
- MUTUAL AUTHENTICATION
  All parties (users, machines, devices) involved in a communication can identify themselves
- LEVERAGE EXISTING ACCESS CONTROL POLICIES
  Use existing group policies and permissions to enable role-based access and control which endpoints can access different applications and networks
- EXTEND TO EXTERNAL USERS
  Outside users (e.g. partners, independent contractors, freelancers) can access your networks without requiring additional software on their local machine or extensive training

Certificate-based Authentication

DATASHEET

Example Use Cases

User Authentication

Replace passwords or add a second authentication factor to control access to:

- Windows Logon
- Corporate email, internal networks, or intranets
- Cloud-based services and applications (e.g. Google Apps, Office 365, SharePoint, Salesforce)

Machine and Device Authentication

Protect against rogue machine and device access by:

- Identifying on-location/in-field machines that need to communicate with back-end services (e.g. payment kiosks located in convenience stores)
- Identifying all employee laptops and mobile devices before allowing access to WiFi networks, VPNs, Gateways, Web Services, etc.
- Identifying all servers within the enterprise to enable mutual authentication

Certificate Provisioning and Management

GlobalSign's Authentication Certificates scale to accommodate businesses of all sizes, from small and mid-sized business to large enterprises, with certificate lifecycle management and automation technologies to simplify high volume deployments.

Managed PKI Platform

GlobalSign's Managed PKI (MPKI) platform simplifies certificate management, offers significant volume discounts compared to purchasing individual certificates, centralizes billing information and enables administrators to efficiently issue, renew and revoke certificates as needed.

Active Directory Integration

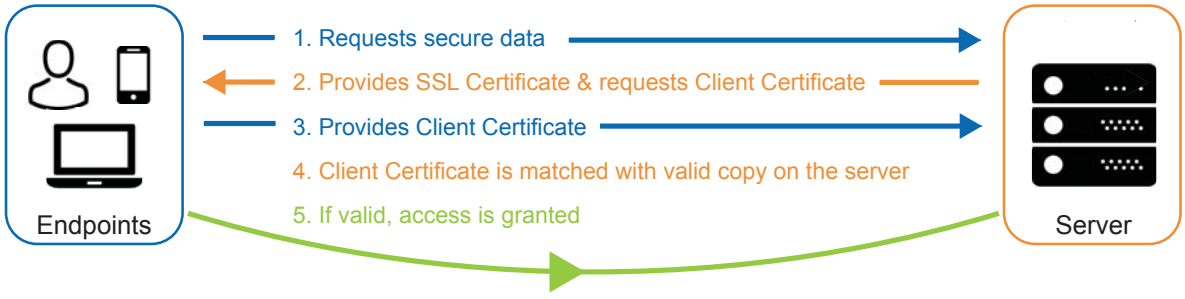
Automate deployments by leveraging existing Active Directory architecture and Group Policy to provision and silently install certificates for domain-joined Windows and Apple OSX endpoints.

Mobile Device Management (MDM) Integration

GlobalSign's integration with MDM platforms, such as AirWatch and MobileIron, eliminate the need for IT staff to manually install certificates on each employee device. As soon as a new device is enrolled with the MDM platform, a GlobalSign Digital Certificate will be issued to the device.

How It Works

The server requests a Digital Certificate from the client to verify that they are who they claim to be. The certificate must be an X.509 certificate and must be signed by a trusted Certificate Authority (CA) as the server will check it against its listed of trusted certificates and only then a secure session will be established.



About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

USA: +1 603 750 7060 or +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign GMO INTERNET GROUP