Client Authentication
Prevent unauthorised access and protect business assets

What is Client Authentication?

Client Authentication is the process by which users securely access a server or remote computer by exchanging a Digital ID. A Digital ID is an individual’s identity (typically including the name, company name and location of the Digital ID owner) bound to a unique cryptographic credential. Networks and web services can be configured to only allow access to particular Digital IDs.

Two Factor Authentication

Prevent unauthorised access or simply add a second layer of security to your current username and password combination. Client Authentication and Access Control helps organisations meet regulatory and privacy compliancy as well as fulfill internal security policies using PKI based two factor authentication – something you have (a GlobalSign Digital Certificate) and something you know (an internally managed password).

How Does it Work?

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 list of trusted certificates and only then a secure session will be established.

Server Security Requirements

Different levels of authentication can be set up depending on the strength and granularity of authentication required.

Granularity refers to the fact that some servers identify individual users throughout a session, while others identify users only during the first request. A fine-grained system is useful if specific authorisation or accountability of a user is required. Coarse-grained systems may be preferred in situations where partial user anonymity is desired.

Client Authentication Use Cases

GlobalSign Client Authentication solutions can be used to access a variety of business services, including:

- Enterprise Email
- Google Apps
- Salesforce
- Sharepoint
- Networks

Deployment Options

Browser-based workflows

A trusted digital credential is issued to an individual or departmental identity and stored on a device (i.e. PC or mobile). The credential is then used by the device to authenticate to the server. The certificate can only be used from one specific browser, machine, laptop, desktop, or server.

FIPS-based workflows

To avoid being tied to one machine, a secure USB token can also be used. A trusted digital credential is issued to an individual departmental identity and stored securely on a cryptographic device, a SafeNet FIPS 140-1 level 2 cryptographic USB token, which is portable and password-secured. The token can be plugged into any USB port without the need for costly reader devices.

Features and Benefits

- Prevent unauthorised access and enhances current security
- Helps meet company email security policies and regulatory compliance
- Cryptographically encapsulates an identity within a Digital ID
- Can be used for in-browser client authentication, VPN’s, smartcard technology, cloud applications and mobile devices
- Cost effective for businesses large to small

For more information about GlobalSign solutions, please call
UK: +44 1622 766766 or EU: +32 16 891900
Visit www.globalsign.co.uk or www.globalsign.eu for more information