

# Client Authentication

Prevent unauthorized access & protect business assets

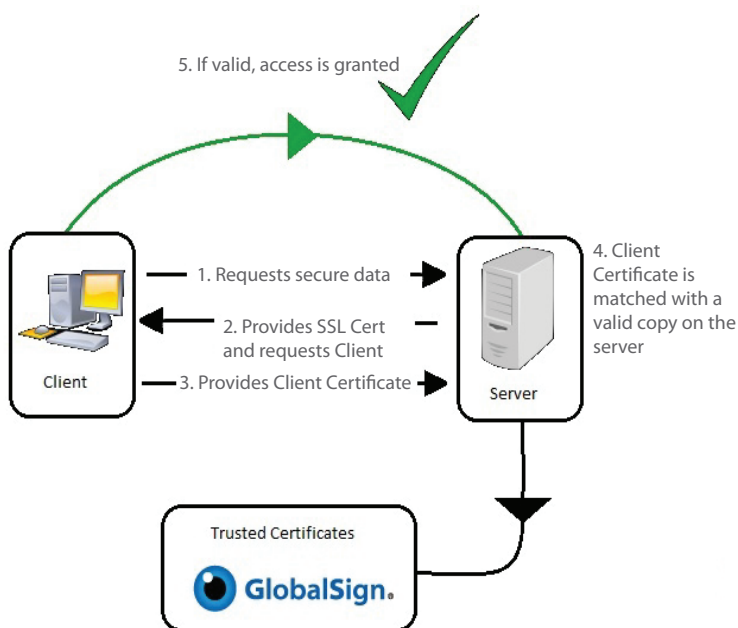
## What is Client Authentication?

Client Authentication is the process by which users securely access a server or remote computer by exchanging a Digital ID. The Digital ID is used to cryptographically bind a customer, employee, or partner's identity to a unique Digital ID (typically including the name, company name and location of the Digital ID owner). The Digital ID can then be mapped to a user account and used to provide access control to network resources or web services and websites.

Prevent unauthorized access or simply add a second layer of security to your current username and password combination. Client Authentication and Access Control helps organizations meet regulatory and privacy compliance 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 listed 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 authorization or accountability of a user is required. Coarse-grained systems may be preferred in situations where partial user anonymity is desired.

For more information about GlobalSign solutions, please call 1-877-755-4562

Visit [www.globalsign.com](http://www.globalsign.com) for more information

## Client Authentication products

GlobalSign offers a range of Client Certificates with varying trust levels.

### PersonalSign 2

Used for individuals (not representing organizations) to secure email (S/MIME), authenticate to enterprise online services and digitally sign Microsoft Office documents. The individual's identity is verified. Issued to `firstname.lastname@email.com` + Firstname Lastname

### PersonalSign 2 Pro

Used for individuals representing organizations to secure email (S/MIME), authenticate to enterprise online services and digitally sign Microsoft Office documents. The individual's identity and company existence are verified. Issued to `firstname.lastname@company.com` + Firstname Lastname + Company Name

### PersonalSign 2 Department

Used for departmental "identities" (such as Marketing or Legal) to secure email (S/MIME), authenticate to enterprise online services and digitally sign Microsoft Office documents. The individual's identity and company existence are verified. Issued to `department@company.com` + Department Name + Company Name

### Enterprise PKI (ePKI)

Managed service model that provides administrators the essential tools for full control of Digital IDs issued and managed.

## Deployment options

### Browser-based workflows

A trusted digital credential is issued to an individual or departmental identity and stored on a user application, e.g. PC/laptop key management system for added protection. The credential is used by the user application to apply the digital signature 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

- Prevents unauthorized 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 Virtual Private Networks (VPN) and high performance SSL VPNs
- Cost effective for businesses large to small