Autenticación de Clientes

Evite accesos no autorizados y proteja los activos de su empresa

¿En qué consiste la autenticación de clientes?

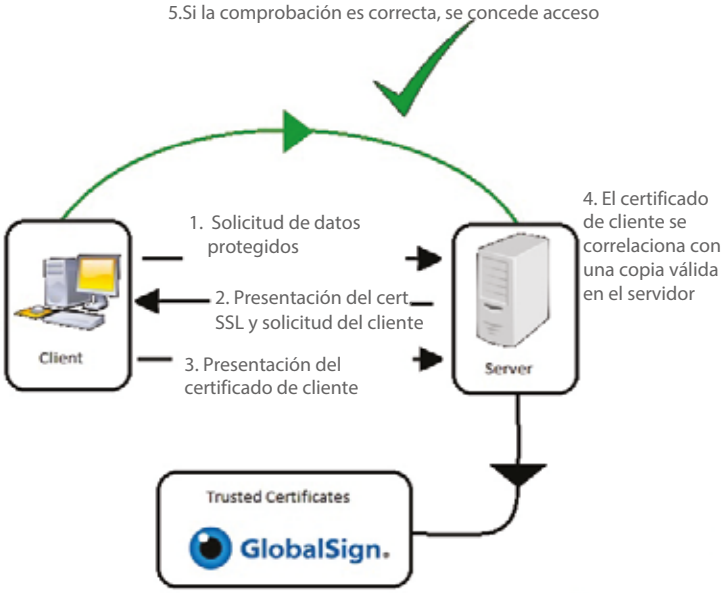
La autenticación de clientes es el proceso que permite a los usuarios acceder de forma segura a un servidor o computadora remota intercambiando una ID digital. Una ID digital es una identidad individual (que suele incluir el nombre, el nombre de la empresa empresa y la ubicación del propietario de la ID digital) vinculada a una credencial criptográfica única. Es posible configurar las redes y los servicios web de forma que solo se permita el acceso a determinadas ID digitales.

Autenticación de Dos factores

Evite accesos no autorizados o añada una segunda capa de seguridad a su actual combinación de nombre de usuario y contraseña. La autenticación de clientes y el control de accesos permite a las organizaciones cumplir los requisitos normativos y de privacidad y seguir las políticas de seguridad internas utilizando la autenticación de doble factor basada en PKI que utiliza algo que el usuario tiene (un certificado digital de GlobalSign) y algo que el usuario conoce (una contraseña gestionada de forma interna).

¿Cómo Funciona?

El servidor solicita un certificado digital al cliente para verificar su identidad. El certificado debe ser un certificado X.509 firmado por una Autoridad de Certificación de confianza, ya que el servidor lo comprobará consultando la lista de certificados de confianza y solo entonces permitirá iniciar sesión de forma segura.



Requisitos de Seguridad de Servidor

Es posible establecer distintos niveles de autenticación en función de la solidez y granularidad de la autenticación necesaria.
La granularidad hace referencia a la capacidad de determinados servidores de identificar a usuarios individuales durante toda la sesión o únicamente durante la primera solicitud. Un sistema muy granular resulta muy útil si es necesario contar con autorizaciones o asignación de responsabilidades específicas para cada usuario. Los sistemas menos granulares resultan más adecuados cuando se desea preservar el anonimato del usuario de forma parcial.

Ejemplos de Uso de Autenticación

Las soluciones de autenticación de clientes de GlobalSign permiten acceder a diversos servicios corporativos, como:

- Corrro Electrónico Corporativo
- Redes
- Sharepoint
- Google Apps
- Salesforce

Opciones de Implementación

Flujos basados en navegadores

Se emite una credencial digital de confianza para una identidad de individuo o departamento y se almacena en un dispositivo (por ejemplo, una computadora o celular). Posteriormente, el dispositivo utiliza la credencial para autenticar su acceso al servidor. El certificado solo puede utilizarse desde un navegador específico, máquina, computadora, portátil o servidor.

Flujos basados en FIPS

El uso de un dispositivo USB evita que la credencial quede vinculada a una única máquina. Se emite una credencial digital de confianza para una identidad de individuo o departamento y se almacena de forma segura en un dispositivo criptográfico, un dispositivo USB criptográfico de nivel 2 validado según FIPS 140-1 de SafeNet (una unidad portátil protegida). El dispositivo puede conectarse a un puerto USB sin necesidad de contar con un costoso lector.

Características y Beneficios

- Evita accesos no autorizados y mejora la seguridad existente
- Contribuye a cumplir las políticas de seguridad corporativas en materia de correos electrónicos y la legislación
- Es capaz de encapsular criptográficamente una identidad dentro de una ID digital
- Puede utilizarse para autenticar identidades en un navegador interno dentro de VPNs, en tecnologías de tarjetas inteligentes, aplicaciones en la nube y dispositivos móviles
- Solución rentable para empresas de todos los tamaños

Para obtener más información sobre las soluciones de GlobalSign:
1-877-755-4562 I www.globalsign.com I contacto@globalsign.com