Hosted HSM Services

GlobalSign Cloud Key Management for Server-based PDF Signing

What is an HSM?

A Hardware Security Module (HSM) is a physical computing device that safeguards and manages digital keys for crypto-processing without revealing key material, while complying with FIPS level private key protection requirements. These modules traditionally come in the form of a plug-in PCI card, or a network attached security device that can be accessed directly by a server or workstation.

Server-based PDF Signing via an HSM allows organizations to digitally sign large volumes of PDF documents, e.g. 25,000+ signings per year, such as bank statements or financial reports. Used in conjunction with either an internally developed or off the shelf automated PDF signature software, such as Adobe LiveCycle, digital signatures can be instantly applied to documents on creation. Organizations use the HSM to manage and protect the private signing key to comply with Adobe Certified Document Services (CDS) requirements around private key protection.

Owned HSMs vs. Hosted HSMs

Compared to a hosted HSM, fully owned and operated HSMs can support larger capacity requirements and can more readily provide access to data for compliance auditing since it is onsite. However, HSMs can be costly to purchase, often requiring CAPX investment, and usually require expert PKI knowledge to implement and manage. Additionally, many organizations never fully utilize the scale of an HSM's storage capability, paying a steep premium for unused capacity.

A hosted HSM solution is recommended as an alternative to purchasing and managing a dedicated and privately owned HSM. The fast set-up, on-demand capability, and scalability to efficiently meet the organization's current needs (e.g., by allowing for increased or reduced storage capacity as required), make it more convenient for service provider and enterprise level deployment. A hosted HSM also eases the man hours and level of expertise required to maintain the secure signing process that often requires 24x7 availability to support mission critical applications.

GlobalSign's Hosted HSM Service

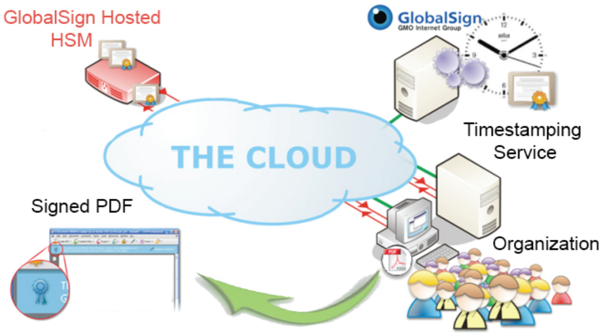
GlobalSign's Hosted HSM Service for PDF Signing offers the ability to host key storage and cryptographic operation materials within a GlobalSign managed HSM environment. By utilizing GlobalSign's Hosted HSM Service, which comprises of a virtual SafeNet Luna HSM partition capable of providing cryptographic storage provisioning, the organization can focus on its core competencies; leaving key management and cryptographic operations to the experts. GlobalSign can deliver Hosted HSM Service partitions within the cloud, tailored to meet your requirements, accessible over a fixed IP address.

Features & Benefits

- **High signing capacity**
- **Compatible with various signing solutions**
- **Reduced total cost of ownership compared to privately owned HSM**
- **Scalable and flexible solution to suit business requirements**
- **No in-house cryptographic expertise required**
- **Leverages GlobalSign and SafeNet technology**
- **High availability options available**
- **24x7 availability to support mission critical applications and meet SLAs**
- **Compliant with Adobe CDS min. FIPS 140-2 level 2 private key protection requirement**

How it Works

1. Install the Luna HSM Client drivers into your signing environment
2. Follow the client-side setup guide to connect your signing environment to the HSM
3. Generate Key material on the HSM and apply for a GlobalSign PDF Signing Certificate
4. Install your GlobalSign PDF Signing Certificate and associate with the Private Key on the HSM
5. Start signing PDF documents by sending the hash of the PDF to GlobalSign's Hosted HSM service (PDF never leaves enterprise environment)



Requirements and Recommendations

- Compatible signing solution to be used in conjunction with GlobalSign's PDF Signing Certificate. Options endorsed by GlobalSign include:
  - Adobe LifeCycle
  - Ascertia DSS
  - Eldos Secure Black Box
  - iText Java/C Sharp
- Single Signing Server with the ability to access to the Internet, for reasons such as:
  - Reaching out to the OCSP/Certificate Revocation List (CRL)
  - Reaching out to the HSM
  - Complete the certificate pick-up on the signing server
- Ability to open the TCP port 1792 at the signing server firewall
- At least one External fixed IP address is required at each location that will need to connect with the Hosted HSM
- Compatible operating systems including:
  - Windows Server 2008, 2008r2, 2012
  - Linux Red Hat or CentOS 5 +

Getting Started

Once you receive access to your Hosted HSM environment, GlobalSign will provide staging time and test certificates to ensure the platform is fully compatible within your organization's specific environment. Our team of Sales Engineers and Product Specialists will also be on hand to assist with any initial set-up questions you may have.

For more information about GlobalSign solutions please visit www.globalsign.com | www.globalsign.co.uk | www.globalsign.eu