

## GlobalSign's Cloud-based Digital Signing Service vs. HSM Deployments



### Digital Signature Deployments for Organizations Using Automated Document Generation, Workflow, or Management Software

For years, the most common option for organizations who wanted to integrate digital signatures into internally developed or off-the-shelf document workflows was to use an HSM (either on-premises or cloud) and configure the integration between the HSM, the document software, and the various cryptographic components needed to deploy signatures (e.g., signing certificates, key management, timestamping server, OCSP or CRL service). This required internal development resources with advanced cryptography knowledge.

Fortunately, GlobalSign has developed a new cloud-based Digital Signing Service (DSS) to simplify these types of integrations and make trusted, compliant digital signatures more accessible to organizations of all sizes. The biggest difference is that unlike HSM deployments, where you need to source the cryptographic components separately and set up your application to make separate calls to each service, DSS includes all of these components in one REST API, so there is minimal development and overhead needed.

Organizations currently using, or planning to use, an HSM-based digital signature deployment should consider migrating to the signing service to:

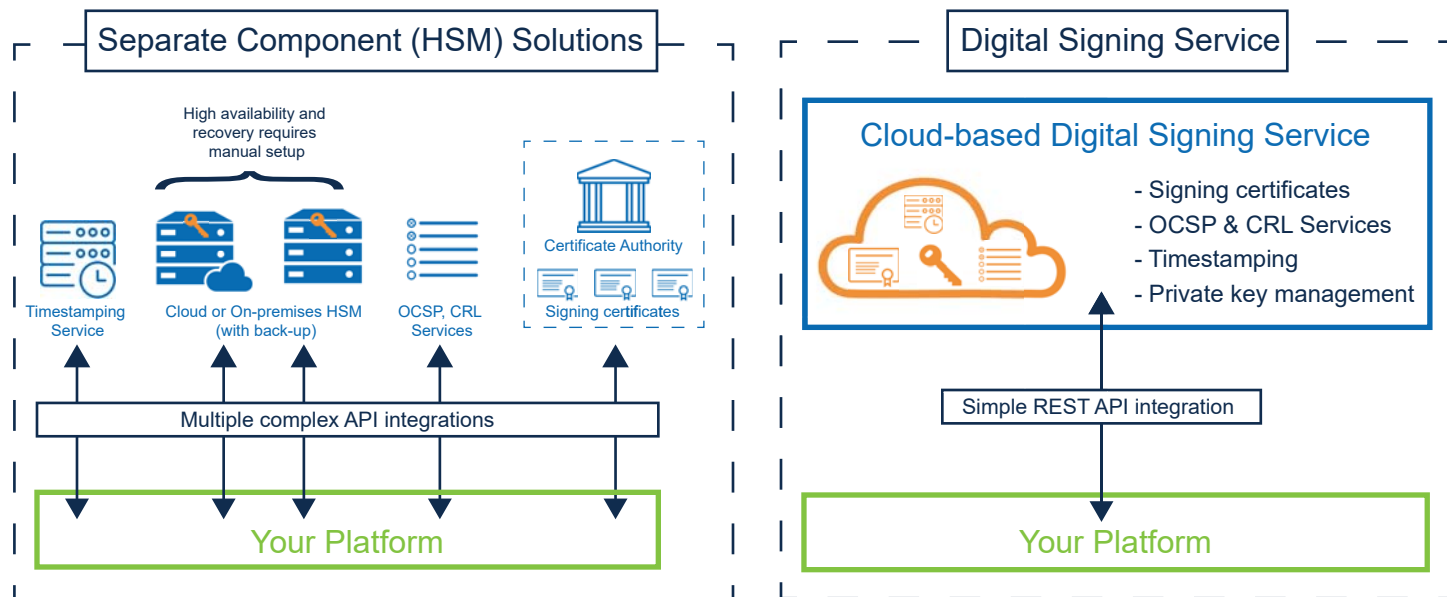
- Eliminate the need to invest in or maintain an HSM(s).
- Simplify the integration and development effort to deploy digital signatures into document software, removing the need for native connection to HSM, and other cryptographic components (i.e., save internal development resources and eliminate need for internal PKI expertise).
- Get more flexibility with signing identities (i.e., HSM solutions can only sign with organization-level identities; DSS supports individual identities).
- Make it easier to scale the deployment, if necessary (i.e., HSM deployments may require additional partitions or configuration to do so).
- Eliminate the need for internal private key management (this is handled by DSS API).
- Ensure high availability by default, without redundant HSM investment.

### FEATURES

- **SIMPLE INTEGRATION WITH DOCUMENT WORKFLOWS/ SOFTWARE**  
Cryptographic components needed for signatures are sourced via one simple REST API, as opposed to multiple calls for each component
- **NO INTERNAL PKI EXPERTISE NEEDED**  
Integration with document software is much simpler and private key management is handled by the service (i.e., GlobalSign)
- **FLEXIBILITY OF SIGNING IDENTITIES**  
Individual or organization-level identities are supported, unlike HSM deployments which generally only support organization-level
- **SAVE TIME AND RESOURCES**  
No need to invest in and maintain an HSM, plus simplified integration saves development resources and hardware costs

## Comparing HSM Deployments to GlobalSign's Digital Signing Service

	HSM Deployment	Digital Signing Service
Integration with document signing applications	Requires internal cryptographic expertise to configure and maintain	Via simple REST API
Signing identities	Only organization- or department-level identities are supported (e.g., Accounting, Finance)	Individual or department-level identities are supported (e.g., John Smith, Accounting)
Scalability	May require additional HSM partitions and configuration	No additional configuration or integration needed
Document workflow options	Integrate a custom built or existing signing workflow using PKCS#11	Easily integrate your signing workflow or use one of our partner's seamlessly integrated workflows
Private key management	Customer responsible for sourcing key management	Handled by REST API (no internal resources required)
Cryptographic signing components (e.g., certificates, OCSP, CRL, timestamping)	Sourced separately, require separate calls from application and internal development resources to configure	Included in one API, no advanced crypto knowledge or development resources needed



### 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).

US: +1 877 775 4562  
 UK: +44 1622 766766  
 EU: +32 16 89 19 00

[sales@globalsign.com](mailto:sales@globalsign.com)  
[www.globalsign.com](http://www.globalsign.com)

