

## Digital Signing Service

### Everything you need to deploy digital signatures in one scalable, cloud-based service

With GlobalSign's highly scalable, cloud-based Digital Signing Service (DSS), you can deploy digital signatures into any application with one simple REST API integration. This means all supporting cryptographic components, including signing certificates, key management, timestamping server, and OCSP or CRL service, are provided in one API call with minimal development or overhead needed and no on-premises hardware to manage.

DSS is the first solution on the market to do this. Other deployments require you to source these components separately and set up your application to make separate calls to each service, which requires internal development resources with advanced cryptography knowledge.

	Digital Signing Service	Traditional Digital Signature Deployments
Integration with document signing applications	Via simple REST API	Requires internal cryptographic expertise to configure and maintain
Cryptographic signing components (e.g., certificates, OCSP, CRL, timestamping)	Included in one API, no advanced crypto knowledge or development resources needed	Sourced separately, require separate calls from application and internal development resources to configure
Scalability	Highly scalable - no additional configuration or integration needed	May require additional hardware and configuration
High availability and disaster recovery	Delivered via GlobalSign's WebTrust-audited robust infrastructure with global data centers, redundancy, and world-class instrumentation protecting the network	Requires additional on premise hardware investment
Private key management and storage	Handled by REST API - no internal resources or hardware required	Customer responsible for sourcing key management and storage (i.e., via cloud or on-premises HSM)
Signing identities	Individual or department-level identities are supported (e.g., John Smith, Accounting)	Not all deployments support both types of identities

## FEATURES

- Build trusted digital signatures into existing document workflow solutions
- Outsource cryptography and PKI to a trusted third party CA
- All crypto components included – signing certificate issuance, timestamping, OCSP or CRL service
- Easy integration via API or SDK and high throughput scale to meet signature demand
- No on-premises hardware to manage
- Sign with individual or department-level identity
- GlobalSign is a member of Adobe's Approved Trust List (AATL) and Microsoft Root Trust program, so signatures are automatically trusted
- Meet national and industry-specific regulations, including US ESIGN, USE UETA, UN Model Electronic Signature Law, eIDAS (advanced signatures, eSeals, FDA CFR 21 Part 11, EMEA eSignature Capabilities, US State Professional Engineering (PE) Seals, and more

## Who Needs a Cloud-based Digital Signing Service?

The demand for trusted and legal digital signatures has never been greater. Fortunately, GlobalSign's DSS makes it easy to add digital signatures and seals to existing document workflows and applications. DSS is cloud-based, allowing organizations to benefit from long-lived, trusted digital signing – signer identity validation, content integrity, trusted timestamps, non-repudiation – without the need to manage any physical hardware or build any custom integrations.

### Adobe Sign Enterprise Users Who Want End-to-end Digital Signing

GlobalSign's Digital Signing Service is already integrated with Adobe Sign, making it the easiest way to add legally accepted and publicly trusted digital signatures to Adobe Sign workflows. Once an organization's DSS account is set up, employees can request signing certificates and start signing immediately within Adobe Sign.

- Sign with employee or department-level identity
- Multiple identity verification options, including integration with Active Directory and other enterprise authentication systems
- No hardware, PKI expertise, or development time needed

### Organizations with their own custom document workflows who want to enable internal and external individuals or departments to digitally sign

Many organizations have created their own electronic document workflows to help transition away from time- and resource-consuming paper processes (e.g., onboarding new clients, exchanging contracts, HR tasks, etc.). With the Digital Signing Service, companies have an easy-to-deploy and cost-effective way to add digital signatures to these processes, providing higher assurance around signer identity, signature authenticity, and content integrity compared to other types of electronic signatures.

- Protect documents with tamper-evident seal and provide higher assurance around who signed the document and when
- Signatures can be in the name of individuals or departments, internal employees or external users/customers (with pre-conditions)
- Integration between in-house document workflow and cloud-based DSS is handled via one simple REST API, minimizing burden on internal development teams and eliminating hardware investment

### Providers of document workflows or applications who want to protect the documents managed within their platforms with digital seals

More and more document workflow or management providers are building digital seals into their applications to increase document security and help meet compliance. Digitally sealing creates a timestamped, tamper-evident seal around document contents and adds assurance around who created it and when - all of which play a role in establishing audit trails, various regulatory compliance, and legal tenability.

The Digital Signing Service makes it easy to build digital seals into the service provider's platform with one simple REST API integration. DSS is the first solution on the market to include all supporting cryptographic components, including signing certificates, key management, time-stamping server, and OCSP or CRL service, in one API call, meaning there is minimal development or overhead needed and no on-premises hardware to manage.

- Digitally seal all documents managed within the platform to protect their contents, provide assurance about when and where documents originated, and help meet compliance
- Minimal development time needed - no complex integration, internal PKI expertise, or hardware investment
- Seals can be in the name of the service provider or the client company (option to add as premium offering)

### 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)



© Copyright 2019 GlobalSign  
gs-dss-2-19