DATA SHEET

Securing E-signatures and Digital Documents for Remote Online Notarization (RON) in the U.S.

Use Entrust hardware security modules (HSMs) and digital signing solutions to align technological requirements for digital seals and online notary services.

Remote Online Notarization (RON) is now accepted in more than 40 U.S. states

Since January 2011, legislation has authorized notaries in the U.S. to conduct online remote notarization. The state of Virginia, via House Bill 2318/Senate Bill 827, led the way, enabling the use of secure e-signatures and e-seals thereby permitting the notarization without the signer needing to be physically present. Interest in RON accelerated rapidly during the COVID-19 pandemic due to the challenges of a face-to-face notarization. Today the state-by-state roll out continues.[1]

Certificate-based seals ensure a high level of document and signature assurance

Digital signing (or digital sealing when the signature represents an organization) provides strong proof of authenticity and helps to ensure non-repudiation.

Digital signing is based on public key infrastructure (PKI) technology, which relies on cryptographic keys. The cryptographic keys must be protected on a secure hardware device like an HSM, a physical device that securely generates, stores, and manages these keys.

Benefits

Improved document security

A digital signature or seal acts like a digital padlock on a PDF document: once it's in place, any modification of the content will invalidate the seal, leaving visual proof of document tampering.

Embedded proof of signing/sealing for independent verification

Digital seals and timestamps on PDF documents that use long-term validation (LTV) give strong proof of the existence of the document from the exact date and time it was timestamped. This proof sits within the document and can be checked by anyone using a compatible PDF reader such as Adobe Acrobat Reader.

Alignment with global standards

- Entrust nShield HSMs are certified to:
  - National Institute for Standards and Technology (NIST) FIPS 140-2/FIPS 140-3
  - Common Criteria EAL4+
- Entrust is a public Certification Authority and an eIDAS qualified trust service provider. We provide publicly trusted digital certificates under the Adobe Approved Trust List (AATL) and the European Union Trusted Lists (EUTL).

[1] Check with the National Notarization Association nationalnotary.org if your U.S. state permits remote online notarization. Different states often have different requirements before you can legally conduct RON so it is always best to do your research and due diligence in advance.

ENTRUST
SECURING A WORLD IN MOTION

Use cases: E-signatures and digital document security

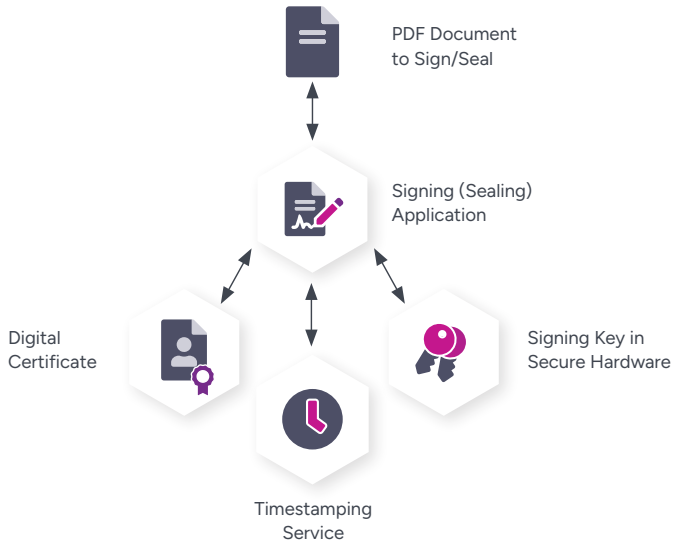
There are two main use cases for digital document sealing:

- **Document authenticity:** Establishing integrity and non-repudiation
- **Electronic signature process:** While e-signatures must be recorded in an audit trail, you can also add a digital seal on top of the e-signature(s) of your documents as a way to "close" the document when all signatories have signed

How it works

Document sealing is a cryptographic operation on a document. It requires the following elements:

- **An application or toolkit** to generate the signature (or seal)
- **A digital signing certificate**, also called document signing certificate, issued by public Certification Authorities (CAs) such as Entrust
- **Secure hardware** such as HSMs, where the cryptographic keys associated with each digital signing certificate must be generated and stored
- **A timestamping service**, based on timestamping certificates which are also issued by CAs



Entrust has all the components, expertise, and services to help you build your sealing process

Out-of-the-box deployment

Use an out-of-the-box cloud-based document sealing service

No expertise required | Pay per use | Scalable | Very quick deployment

Custom deployment

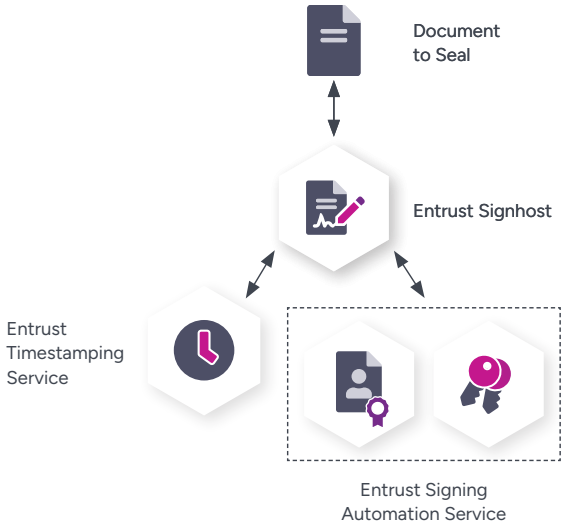
Leverage your existing e-signing solution

Limit change | Keep control of your core infrastructure | Leverage Entrust's public trust services and HSMs

Out-of-the-box deployment

Entrust provides a cloud document sealing service using our own signing application, as well as our trusted certificates and timestamps.

- **Sealing workflow:** Entrust Signhost
- **Digital certificate:** Issued by Entrust, stored in Entrust Signing Automation Service
- **Signing key storage:** Managed by Entrust Signing Automation Service
- **Timestamping:** Provided by Entrust public timestamping service

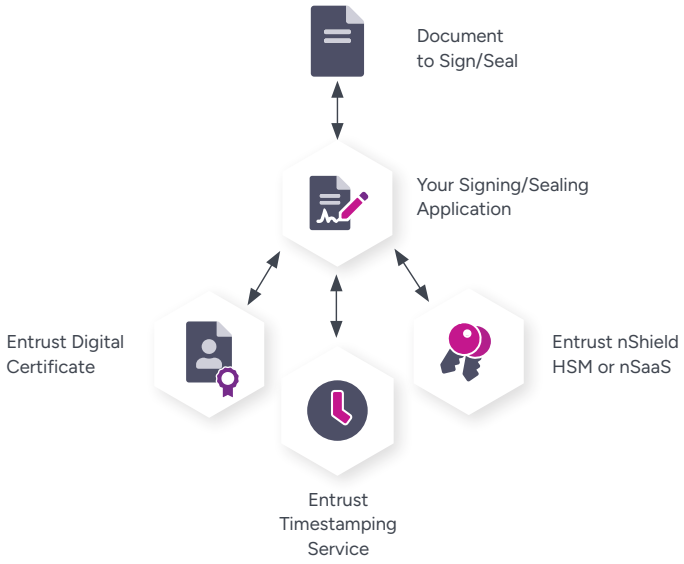


Features and Options	
Access to the Service	Documents can be submitted manually via Signhost's web portal, or automatically via Signhost's REST API. Alternatively, third-party workflows can submit document hashes to be signed directly to Signing Automation Service using a PKCS #11 connector or a REST API.
Digital Certificate Type	By default, Signhost comes with a generic Adobe-trusted certificate for document sealing issued under the name of Entrust. We offer the option to use an Adobe-trusted certificate (AATL) certificate issued under your organization's legal name via Entrust Signing Automation Service. Signhost can be configured to use your custom certificate for sealing.
Seal Type	All digital seals are generated based on the PAdES and LTV standards. They are trusted by Adobe and considered advanced seals under the EU eIDAS regulation.
Timestamping Service	Timestamps are issued by Entrust. We offer a "standard" public timestamping service, as well as an EU eIDAS-qualified timestamping service.

Custom deployment

You may prefer a custom deployment if you already have a signing portal or application, and you're just looking for trusted certificates and secure key storage to generate digital seals.

- **Sealing workflow:** Your own solution or any third-party solution that is able to generate digital signatures and connect to HSMs
- **Digital certificate:** Issued by Entrust
- **Signing key storage:** Entrust nShield HSM (on-premises hardware) or nShield as a Service (cloud HSMs)
- **Timestamping:** Provided by Entrust public timestamping service



Features and Options	
Sealing Process	Managed by your signing application (in-house or third-party). The application must be able to generate digital signatures, to connect to the Entrust HSM solution you'd like to use (on-premises HSM or cloud HSM), and to connect to Entrust's timestamping service.
Digital Certificate Type	We offer Adobe-trusted certificate (AATL) issued under your organization's name, whose private key can be generated in the Entrust HSM solution you choose.
Seal Type	Managed by your signing application (in-house or third-party).
Timestamping Service	Timestamps are issued by Entrust. We offer a public timestamping service based on RFC 3161 with all our digital signing certificates.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION