# Entrust Signing Automation Engine

E-signature platform for automated processes

## HIGHLIGHTS

### Fully automate your electronic signature activities

The Entrust Signing Automation Engine is an on-premises solution for automated document signing integration. It allows your organization to:

- Fully implement and automate enterprise certificate-based document signing and verification processes into your business activities
- Benefit from a centralized signing system for your own applications and services

The Entrust Signing Automation Engine supports advanced electronic signature formats and multiple certification authorities (CAs), ensuring high compatibility and full integration into any environment.

## KEY FEATURES & BENEFITS

### Integrate document signing and verification into your applications

The Entrust Signing Automation Engine is a web services platform providing a complete set of signature-generation, signature-verification, and signature-augmentation features.

- Signature capabilities can be accessed from applications through web services (APIs), or through watched folders[1] on your network
- Application credentials and group-based rights assignment can be managed using your existing databases

### Leverage semantic interpretation of signatures

- The Entrust Signing Automation Engine is the most complete signature service of its kind
- Multiple CAs can be managed, all signature formats are supported, and the complexity related to managing trust is removed from your applications
- The incorporated semantic services allow you to obtain all signer/signature data along with a trust level indicated using discrete values (four levels) and labels (i.e., government, corporate, finance, etc.)

[1] Watched Folders is an optional module for the Entrust Signing Automation Engine. For more information, please consult our dedicated data sheet.

**Learn more about the Signing Automation Engine at entrust.com**

# Entrust Signing Automation Engine

## Maintain strong compliance and auditing levels

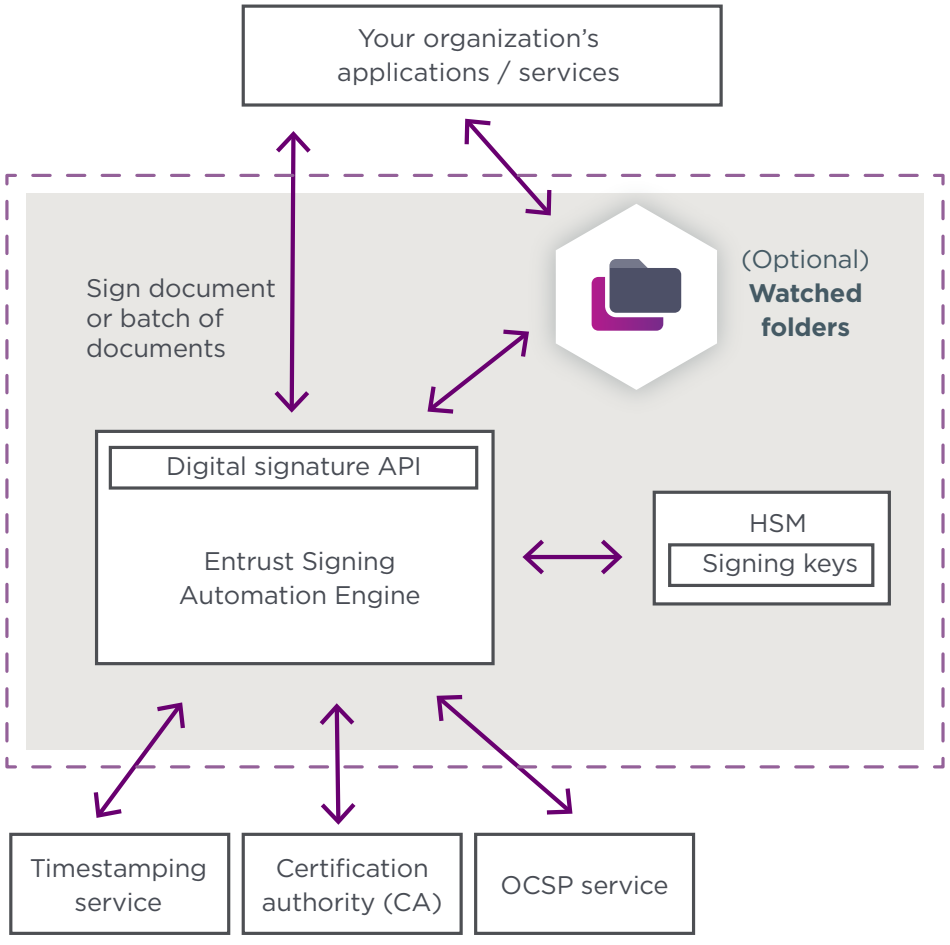
- The service can be deployed quickly, thanks to its compliance with standards and its multiple integration options
- Audit logs are generated for any changes in the configuration made by the administrators and for the services accessed by the applications
- These logs can be stored in a database or forwarded to a SIEM tool to generate reports

## Centralize key and policy management for signatures

- The Entrust Signing Automation Engine acts as a centralized certificate and key repository that your applications can leverage for signature processes, eliminating the need for in-app key storage and management
- The service also centralizes management of signature policies that lets you model different behaviors for groups of applications, such as trust in certain public or corporate CAs, or which method to use for certificate revocation status check

## Architecture

The following diagram illustrates a typical integration of the Entrust Signing Automation Engine into your organization.




**Learn more about the Signing Automation Engine at entrust.com**

# Entrust Signing Automation Engine

## HOW IT WORKS

## TECHNICAL FEATURES

The Entrust Signing Automation Engine incorporates functions that provide a set of security and trust mechanisms as services that can be used with different integration strategies:

- **SOAP/WS:** Using the OASIS DSS standard as an access protocol for web services
- **REST/WS, SOAP/WS:** Using the integration gateway, which supports configuring traffic and data processing with an XML pipeline language
- **Java SDK:** For easy integration of electronic signature services in native Java applications

Features are grouped into the following categories:

| | | | |
|---|---|---|---|
| **Authentication and Authorization** | Supports native authentication methods based on passwords and digital certificates. The validation can be delegated to LDAP/AD. | **Long-Term Validation (LTV)** | Extends a signature's validity up to the lifetime of the TSA certificate.<br>• Cryptographic reliability is preserved<br>• The certification chain is incorporated as well as certificate status information at the time of signing<br>• A timestamp is added<br>The signatures can be extended further by adding additional timestamps. |
| **Object and Entity Management** | Manages platform entities and objects. External repositories, such as user LDAP/AD, databases, files, and HSMs can be added for protecting private keys. | **Auditing and Accounting** | Logs are securely stored in a uniform and centralized way. It's also possible to forward log data to an external SIEM tool for processing and generating a report. |
| **Certificate Validation** | Provides PKI functions for validating certification chains and querying certificate status. Supports OCSP/CRL and customized mechanisms (e.g., databases). | **Optional Service: Watched Folders** | Monitors selected folders in your network (called "watched folders") and executes a series of signature-related actions (e.g., signing, verification, stamping, augmentation) on any file added to the folders. |
| **Signature Creation and Validation** | Creates and validates signatures compliant with the PAdES, XAdES, and CAdES standards; including document, email, and web services signatures. | **Optional Service: Data Encryption** | Provides document encryption and decryption functionalities. Supported formats are PKCS#7, CMS, XML-Enc, and S/MIME. Please contact us to learn more about this option. |

**Learn more about the Signing Automation Engine at entrust.com**

# Entrust Signing Automation Engine

## TECHNICAL SPECIFICATIONS

- **Format:** Software appliance (please contact us to learn more about supported hardware or virtual machines)
- **Event monitoring:** Simple Network Management Protocol (SNMP)
- **Security services:** OASIS WS-Security, DSS (Digital Signature Service) and SAML, SOAP, and SSL/TLS
- **Signature generation standards:** PKCS#7, CMS, CAdES (ETSI TS 103 173), XML-DSig, XAdES (ETSI TS 103 171), signature for PDF documents (IETF), PAdES (ETSI TS 103 172) and S/MIME
- **Signature validation and augmentation standards:** PKCS#7, CMS, CAdES (ETSI TS 103 173 and ETSI EN 319 122), XML-DSig, XAdES (ETSI TS 103 171 and ETSI EN 319 132), signature for PDF documents (IETF), PAdES (ETSI TS 103 172 and ETSI EN 319 142), and S/MIME
- **Encryption standards:** PKCS#7, CMS, XML-Enc, and S/MIME
- **Digital timestamping support:** IETF RFC 3161 and RFC 5816 compatible servers
- **Certificate validation support:** Using CRLs, IETF OCSP compatible servers and customized mechanisms (OCSP is required for LTV signatures)
- **Database and directory access:** Oracle, Microsoft SQL Server, PostgreSQL and MySQL, LDAP directory access protocol
- **Authentication and authorization:** Native authentication methods based on passwords and digital certificates. Password validation can be delegated to LDAP/AD
- **HSM support:** PKCS#11 devices approved by Entrust (a license is required for the HSM connector)
- **Network file systems supported:** SMB/CIFS and NFS

Learn more at
**entrust.com**



ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
+44 (0) 118 953 3000
**info@entrust.com**