Entrust Signing Automation Server

(Formerly TrustedX Electronic Signatures)

E-signature platform for automated processes

HIGHLIGHTS

Fully automate your electronic signature activities

Entrust Signing Automation Server 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

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

KEY FEATURES & BENEFITS

Entrust Signing Automation Server 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

- Entrust Signing Automation Server 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 Server. For more information, please consult our dedicated data sheet.

LEARN MORE AT ENTRUST.COM

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 Server 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 di erent behaviors for groups of applications, such as trust in certain public or corporate CAs, or which method to use for certificate revocation status check