Entrust Remote Signing Engine

Entrust Remote Signing Engine is an on-premises solution for the deployment of a legally-compliant cloud-based signing service, easily accessible through a web API.

HIGHLIGHTS

Provide advanced and qualified signatures as defined by eIDAS

Entrust Remote Signing Engine performs signing operations on a Qualified Signature Creation Device (QSCD). When managed by a Qualified Trust Service Provider (QTSP) issuing qualified digital signing certificates, the service can provide advanced and qualified signatures compliant with the eIDAS regulation.

- Signing keys are centrally protected within an HSM
- Document signatures are approved remotely by users from their device, without the need for a hardware or software token

KEY FEATURES & BENEFITS

Follow globally accepted signing standards

Entrust Remote Signing Engine is based on the ETSI and CEN standards, which guarantee:

- A very high level of trust
- Broad interoperability with the industry products that require digital signatures, regardless of whether your organization operates in Europe or not

Remove the key management burden from your users

Entrust Remote Signing Engine was built with user experience in mind. The onboarding and signing process is:

- Transparent
- Does not require specific knowledge
- Can be done from any device

The signing service operates in your premises with keys securely stored in an HSM, and users authorize each signature request from their computer or device.

Ensure adequate authentication for each digital signature type

User authentication can be done with your existing service, ensuring that access is managed via an identity provider (IdP) that you control.

When a signature is required, Entrust Remote Signing Engine can raise the authentication assurance level by sending an additional challenge such as:

- An SMS/email OTP
- Entrust Remote Signing Engine Mobile ID app notifications

Learn more about Remote Signing Engine at entrust.com

Entrust Remote Signing Engine

HOW IT WORKS

Operation

Entrust Remote Signing Engine acts as a server-based signature provider, allowing users to authenticate in order to activate their keys and authorize the signature of documents or document hashes.

Electronic signature provider (eSigP)

PKI material for enrolled users is managed as identity attributes in a secure HSM-based repository. Each user can have one or more digital certificates to sign documents remotely once authenticated.

Signing functions are available through a web API or optionally via the Entrust Remote Signing Engine Desktop Virtual Card (VC) component.

Identity provider (IdP)

The platform is designed to leverage an existing federated identity provider, but it can also act as an IdP for some use cases. Consult us for more information about supported third-party IdPs.

Entrust Remote Signing Engine includes 2FA authentication methods such as SMS/Email OTP and Entrust Remote Signing Engine Mobile ID.

More authenticators can be incorporated thanks to the integration with Entrust Identity as a Service or Entrust Identity Enterprise, or with existing IdPs using our SAML 2.0 and OpenID Connect connector.

Modules

Entrust Remote Signing Engine comes with two optional modules that can be deployed according to your needs:

Mobile ID

An optional module that enables signature activation using a mobile device. It comes either as a dedicated app or as an SDK to integrate to your own app.

The module implements a PKI-based authentication requiring a fingerprint or a PIN to use the authentication key on the mobile device where it is installed.

Desktop VC

An optional module for signatures and web authentication processes from a local computer.

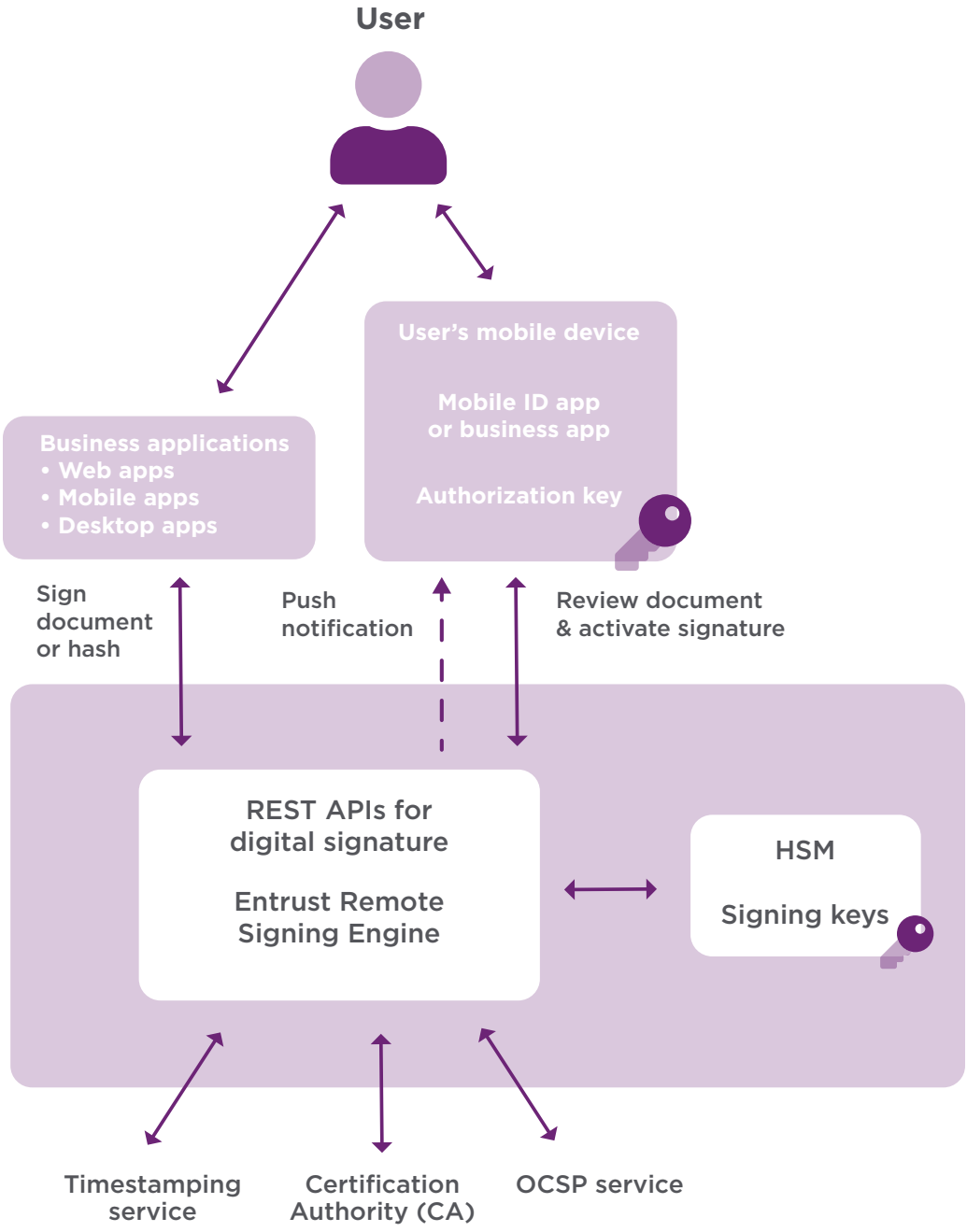
A light plug-in is installed on the user's computer, which enables them to sign documents directly from the computer using remote keys securely stored in Entrust Remote Signing Engine.

Desktop VC can be leveraged for both TLS authentication in web browsers and in-application signatures.

Entrust Remote Signing Engine

Architecture

Entrust Remote Signing Engine provides remote signing and 2FA-based signature activation options via web services operated by a trust service provider. The following figure illustrates the interactions between Entrust Remote Signing Engine, the optional Mobile ID module, and your infrastructure – the IdP is not represented:



Learn more about Remote Signing Engine at entrust.com

Entrust Remote Signing Engine

TECHNICAL SPECIFICATIONS AND REQUIREMENTS

Format:
- Virtual or hardware appliance. Hardware appliance is required for the Signature Activation Module.

Signature Activation Module (SAM):
- Entrust Remote Signing Engine implements a SAM conforming to CEN EN 419 241-2: Protection Profile for QSCD for Server Signing.

Authentication standards:
- OASIS SAML 2.0 and OAuth 2.0/OpenID Connect.

Native authentication methods:
- Passwords, digital certificates, SMS/email OTP, Mobile ID.

Extending authenticators:
- Integration with Entrust Identity as a Service or Entrust Identity Enterprise, or with third-party IdP using the provided SAML 2.0 connector or a custom connector.

Authentication classification:
- eIDAS's levels of assurance (LoA), NIST's authenticator assurance levels (AALs), ITU-T X.1254, ISO/IEC 29115.

Electronic signature standards:
- PAdES (ETSI TS 103 172 and ETSI EN 319 142), XAdES (ETSI TS 103 171 and ETSI EN 319 132), CAdES (ETSI TS 103 173 and ETSI EN 319 122), RSA PKCS#1 and Cloud Signature Consortium/ ETSI TS 119 432.

External TSA and OCSPs:
- Entrust's TSA and OCSP products or IETF TSA and IETF OCSP compatible servers to create LTV signatures with extended lifetime up to TSA certificate validity.

External PKI services:
- Entrust's PKI or third-party PKI using the provided mechanism of custom connectors.

HSM support:
- nShield Connect+ and nShield Connect XC. The available functions may vary depending on the model chosen (nShield Connect XC is required for the SAM). We are currently working on nShield 5 support, please contact us to know more about the timelines.

Event monitoring:
- Simple Network Management Protocol (SNMP). Syslog and raw format for processing with an external SIEM.

Database systems:
- Oracle, Microsoft SQL Server, and PostgreSQL. Consult us for other databases support.

SMS/Email gateway:
- An SMS Gateway and/or SMTP server is required for OTP methods.

Learn more at
entrust.com

Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
SL24Q4-remote-signing-engine-ds

ENTRUST

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