Mobile ID

A mobile device integration module for Entrust Remote Signing Engine

Market Challenge

A Remote Signing deployment provides a convenient digital signing service for individuals, with signing keys managed in a centralized service and actioned upon request. To ensure the best user experience possible, the user's own mobile device should be used for signature approvals.

Solution

The optional Mobile ID module for Entrust Remote Signing Engine enables signature activation from any smartphone.

- Signing is performed in Remote Signing Engine; users approve from their device
- Two-factor authentication (2FA) with integrated fingerprint or facial recognition
- Web push notifications for signature requests
- Available as an app and SDK (software development kit)

BENEFITS

- Simple activation – as easy as downloading an app and reading a QR code
- Secure identity – the module requires a fingerprint or PIN to use the activation key on the mobile device where it's installed; credentials are linked to the device to safeguard against the cloning of private keys
- Standard integration – performed using current web standards; also available in SDK format for integration into app
- Multi-device support - users can start signing transaction from any device with a browser; the signature is authorized via a push notification on the user's smartphone
- Customized branding - customizable design allows you to add corporate branding elements to the app

Learn more about Remote Signing Engine at entrust.com

Mobile ID for Entrust Remote Signing Engine

Mobile ID at a glance

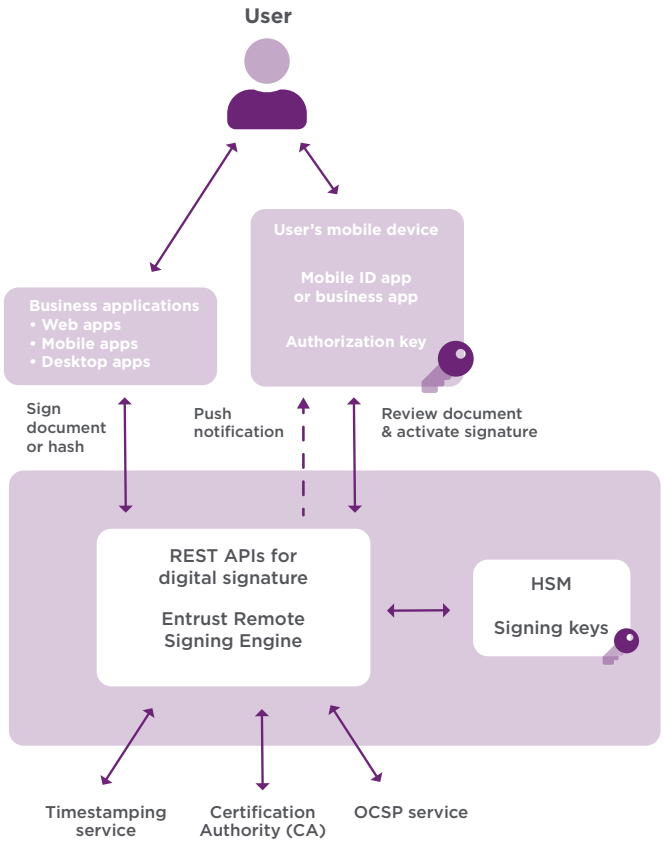
When the user downloads the Mobile ID from Apple's App Store or the Google Play Store, the identity activation process starts with entering a registration code on the mobile device. During this process, the user establishes their key protection (biometric or PIN), and the credentials are generated and activated transparently.

From that point on, the app is automatically invoked in web pages and other devices via notifications when authorization or document signing is required.

Architecture

The diagram at right illustrates the interactions between Entrust's Mobile ID, the user applications, and the infrastructure components.

- Entrust Remote Signing Engine provides remote signing functionality that requires two-factor authentication
- The PKI service provides the keys used for authentication
- Business applications include web browsers, third-party apps, and other applications run from other devices
- the PKI authentication keys can be software- or hardware-protected (Secure Element/Trusted Execution Environment)



Technical Specifications

- Operating systems: iOS and Android; branded app or SDK
- Electronic signature service: Entrust Remote Signing Engine
- External PKI services: Entrust's PKI or third-party PKI using the provided mechanism of custom connectors

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
EMEA Phone: +44 (0) 118 953 3000
info@entrust.com