Mobile ID

A mobile device integration module for the TrustedX eIDAS Platform

Market Challenge

A TrustedX eIDAS 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 the TrustedX eIDAS Platform enables signature activation from any smartphone.

- Signing is performed in the TrustedX eIDAS Platform; 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 – 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 - user can start signing transaction from any device with a browser; signature is authorized via a push notification on user's smartphone
- Customized branding - customizable design allows you to add corporate branding elements to the app

Mobile ID

Mobile ID at a glance

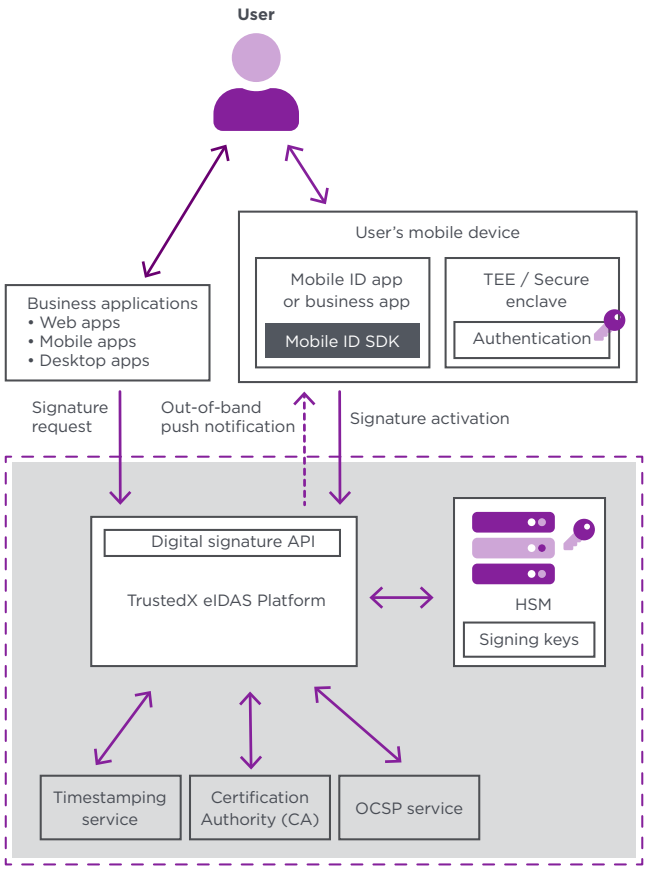
When the user downloads Mobile ID from Apple's App Store or the Google Play Store, the identity activation process starts with entering a registration code on the mobile device. During this process, the user establishes their key protection (biometric or PIN), and the credentials are generated and activated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

- The TrustedX eIDAS Platform 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 authentication PKI 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: TrustedX eIDAS Platform
- 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
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact