DIGITAL CERTIFICATES with HID® Approve™

EPCS Prescribing – HID® Approve™ IGC Prescribing | Basic Assurance | Individual Identity Certificates

Trusted Identity –
Increase your customer's trust and reduce fraud with a state of the art secured mobile solution

Seamless Experience –
Push notification provides a simple yet secure way for users to validate access and transaction requests

Simplified Compliance –
HID Approve meets requirements for compliance with the PSD2, FFIEC, and PCI-DSS 3.2 regulations

Push notification authentication –
Convenience and security unite with mobile push notifications and public key cryptography

Flexible Policy Customization –
Fine-grained security policies enable organizations to strike the appropriate balance between security and usability

Robust Security –
Runtime Application Self-Protection to detect and prevent real-time attacks

Product Summary

HID® Approve™ allows you to authenticate requests to Approve or Decline your prescription(s) via a mobile device in a flexible and secure manner using state-of-the-art cryptographic protocols, providing a straightforward and easy user experience. HID Approve's security posture is second to none, built following industry-defined security best practices and is backed by third-party penetration tests and independent audit reviews.

IGC | Basic Assurance | Individual Identity | Software Storage certificates and IGC | Basic Assurance | Individual Identity | Hardware Storage certificates are issued under the IdenTrust Global Common Certification Authority Policy program and are cross-certified under the U.S. Federal PKI Common Policy Framework.

The IGC Federal Bridge Certified certificates are accepted by government agencies and used by individuals who are not affiliated with a sponsoring organization to securely conduct business in a digital world.

The Software Storage certificate is safely stored in the browser certificate store on your local PC or laptop and can only be used on a single device. The Hardware Storage certificate is bound and stored on a FIPS 140-2 compliant hardware device (USB token or Smart card), and can be used with multiple PCs or laptops if they have the ActivID software installed.

Identity Authentication Method:	Your identity is verified by IdenTrust via an automated process
Identity Proofing Requirements:	Provide personally identifying information
Forms Packet Required:	No – You do not need to submit forms for this certificate type
Trust Model:	This certificate is publicly and government trusted
Assurance Level:	Basic Assurance
Certificate Type:	This is an individual certificate that is issued to you
Validity Periods:	Available up to a three (3) year validity period. EPCS and Hardware-based certificates are offered for two (2) years only.
Storage Type:	Software certificate is stored on a single PC or laptop. Hardware certificate is stored on a FIPS 140-2 compliant device.
Available to Non-U.S. Residents:	No – This certificate is offered to residents of the U.S. only

Specifications
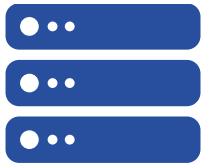
Authentication methods:
- Mobile push with public key cryptography
- One-time password – OATH HOTP Event, TOTP Time-based, OCRA
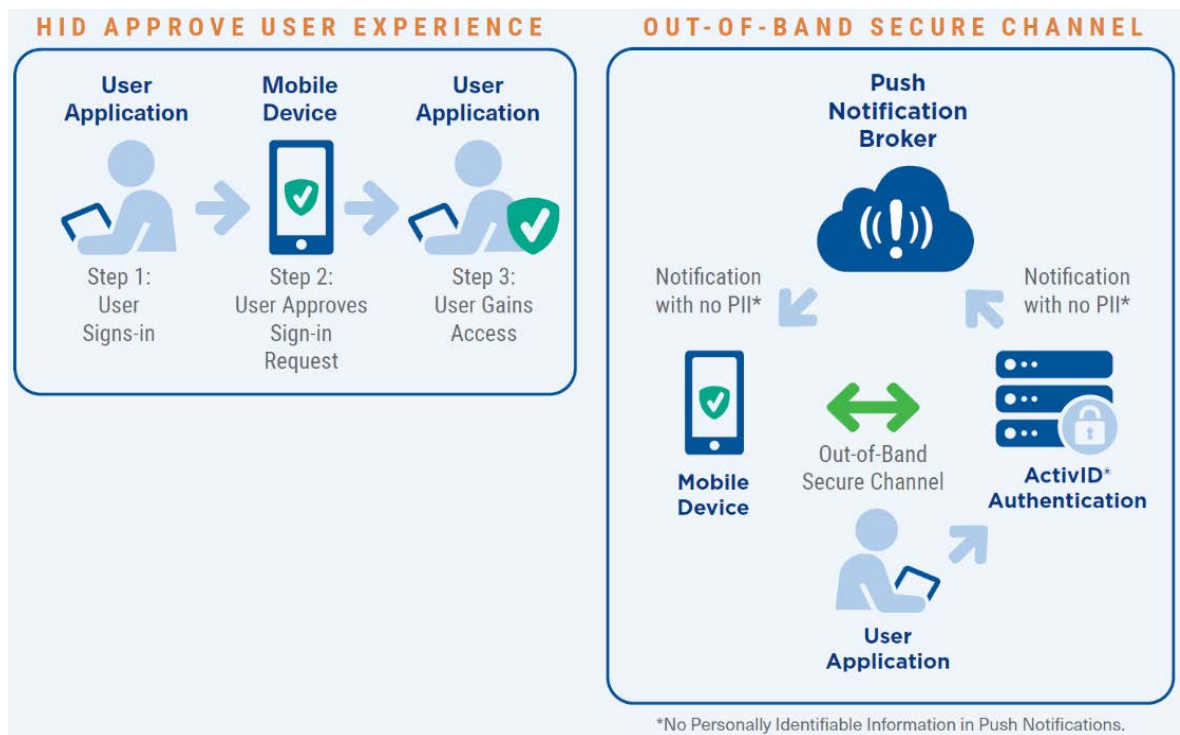
Protocol and cryptography standards:
- OIDC/OAuth2
- ECDH
- ECC
- ADFSv3
- SAMLv2
- TLS v1.2x509
- 800-56 KDF
- RSA2048
- RADIUS
- HPKP RFC 7469
- PKC#5
- Oath
- HMAC-SHA2
- SAMLv2

Platforms:
- iOS 8.0+ (mobile and tablet in portrait mode)
- Android 4.1+ (mobile and tablet in portrait mode)

Secure Key Generation and Storage:
- iOS KeyChain (hardware backed)
- Android KeyStore (hardware backed on version 4.3 and later)

HID APPROVE USER EXPERIENCE

User Application
Mobile Device
User Application

Step 1: User Signs-in
Step 2: User Approves Sign-in Request
Step 3: User Gains Access

OUT-OF-BAND SECURE CHANNEL

Push Notification Broker

Notification with no PII*

Notification with no PII*

Mobile Device

Out-of-Band Secure Channel

ActivID* Authentication

User Application

*No Personally Identifiable Information in Push Notifications.

Certificate Usage

This certificate can be used for:
- Non-Repudiation
- Two-Factor Authentication
- HID Approve
- Data and Email Encryption
- Digital Document and Email Signing

Software certificates are exportable and can be backed up. Hardware certificates are portable and can be used on any computer where the middleware is installed.

Related information:
- Acceptable Forms of Identification
- IGC Forms, Agreements and Policies
- IGC FAQs

2022-05-17-identrust-igc-hidapprove-cert- ds-en

For IdenTrust Sales inquiries: +1 (866) 763-3346 | sales@identrust.com

An ASSA ABLOY Group brand

ASSA ABLOY™

identrust.com