HID Approve™

SIMPLE, SECURE MOBILE PUSH AUTHENTICATION AND VERIFICATION SOLUTION

Benefits

- 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, but 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

- Lower Cost of Ownership - Out-of-the-box customization enables organizations to keep their brand at the forefront of the user experience without the need to build and maintain a custom mobile app

- Flexible Deployment – The functionality is available as a turn-key application or a Software Development Kit for integration into existing corporate apps

- **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

- **Easy rebranding –** Organizations can easily brand the user interface with their own logo and color schemes

- **Robust security -** Runtime Application Self-Protection to detect and prevent real-time attacks

HID Approve™ is a next-generation two-factor authentication solution. By combining public key-based cryptography with mobile push notifications, HID Approve delivers a simple and secure way for users to authenticate and validate their transactions. With a simple swipe gesture, your customer's confidence increases in the security of your digital channel and you get proof-of-possession for "something a user has" to achieve strong two-factor authentication.

HID Approve offers a comprehensive range of security policy customizations, suited to each organization's unique risk-profile. This enables organizations to strike a better balance between security and usability.

Additionally, organizations can easily and securely customize the HID Approve user interface with their own logo and color schemes via server-side configuration. This ensures your users understand who is asking for verification.

The flexible and secure activation process of HID Approve ensures that each user's

device is securely personalized using state-of-the-art cryptographic protocols, provided through a straightforward and easy user experience. Users may securely register HID Approve with multiple user accounts, and service providers, thus eliminating the need to manage multiple tokens or mobile apps for their two-factor authentication needs.

HID Approve's security posture is second to none. It was built following industry-defined security best practices and is backed by third-party penetration tests and independent audit reviews.

HID Approve is a new addition to the broad range of authentication products and services offered by HID Global that enables organizations to achieve a maximum return on investment for all their authentication needs. It works in conjunction with HID Global's Authentication Server Products. More information about these solutions can be found on www.hidglobal.com.

SYSTEM FEATURES:

- Mobile push notification, and public key cryptography-based authentication and transaction validation
- Confidential and anonymous data in push notifications
- Fully customizable and fine grained security policies – for example, independent and optional password protection on mobile credentials
- Easy server-side configuration for mobile app branding
- Runtime Application Self-Protection (RASP) to detect and prevent real-time app attacks
- User device Integrity detection capabilities, such as: tamper detection, anti-cloning, Jailbreak and root detection
- Mobile SDK option for integration into corporate apps
- Protect web apps, cloud apps and VPN
- On-premise deployable
- FIPS 140-2 L1 compliant (when deployed in FIPS mode)

USER/CUSTOMER FEATURES:

- Secure channel out-of-band activation and authentication
- Easy and flexible user activation with QR codes or manual entry
- Optional use of TouchID or Fingerprint for mobile key protection
- Users can register multiple devices for their convenience
- Users can register multiple accounts with multiple service providers in a single app
- Secure Code (One Time Password) option for mobile offline scenarios in case of connectivity challenges
- Reliable Digital Signatures – the content of signed messages cannot be changed, by accident or intent, balancing security and convenience
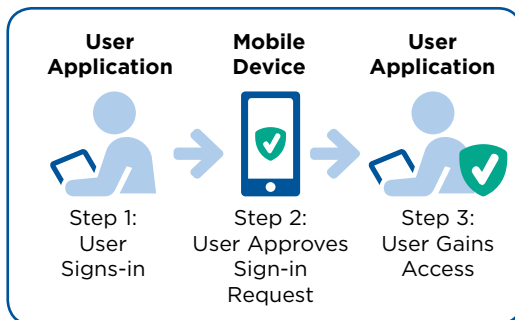- Support for 15 languages out-of-the-box

SPECIFICATIONS

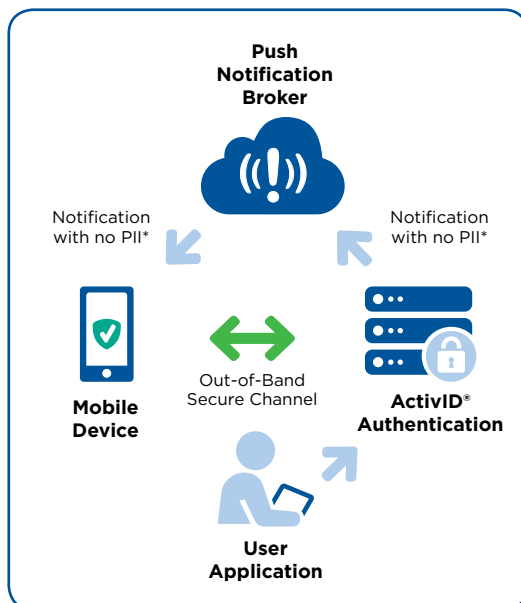|	
Authentication Methods	• Mobile push with public key cryptography • One Time Password: OATH HOTP Event, TOTP Time-based, OCRA
Protocol and Cryptography Standards	OIDC/OAuth2, TLS v1.2, x509, HPKP rfc7469, ECDH, 800-56 KDF, PKCS#5, ECC, RSA2048, AES256, OATH, HMAC-SHA2, FIPS 140-2 L1 compliant
Platforms	• iOS 9.0 and up (mobile and tablet in portrait mode) • Android 4.4 and up (mobile and tablet in portrait mode) • Windows 10 (PC and tablet)
Secure Key Generation and Storage	• Android KeyStore (hardware backed on versions 4.3 later) • iOS KeyChain (hardware backed)

HID Professional Services

Technical expertise and project management resources are available to assist in the complete design and implementation of your customized HID Approve solution, or to integrate our Software Development Kit into your own app. Visit www.hidglobal.com/professional-services to learn more.

HID Approve User Experience

User Application — Step 1: User Signs-in
Mobile Device — Step 2: User Approves Sign-in Request
User Application — 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.