

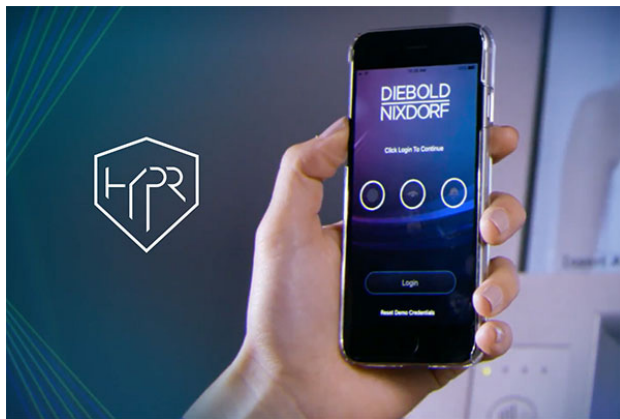


TRUST ANYONE

FRAUD-PROOF ATM EXPERIENCES WITH TRUE CARD-LESS SECURITY

Card skimming and ATM malware have forced banks to rethink consumer fraud protection. When ATM cards, PINs and passwords are stored in one place, hackers can commit widespread account fraud by attacking a single point of failure – the ATM. **The solution is to move authentication keys to the user’s mobile device and enable fully card-less security.** This approach - known as Decentralized Authentication - has enabled banks and ATM manufacturers to provide customers a secure mobile-first banking experience that’s immune to card skimming and account fraud.

- STOP CARD SKIMMING & CREDENTIAL REUSE
- ELIMINATE ACCOUNT TAKEOVER FRAUD
- NEUTRALIZE ATM MALWARE ATTACKS
- ACCELERATE TRANSACTION SPEEDS
- ENHANCE CUSTOMER EXPERIENCE
- ENABLE MOBILE-FIRST BANKING



MOBILE-FIRST ATM AUTHENTICATION BUILT ON OPEN FIDO STANDARDS

HYPR is a FIDO-Certified Decentralized Authentication Platform. FIDO standards enabling PKI authentication have been adopted by the world’s largest banks, enterprises, and even ATM manufacturers. In 2017, Diebold-Nixdorf and HYPR unveiled the first card-less security solution powered by FIDO authentication.

[Watch the video at HYPR.com/biometric-atm.](https://www.hypr.com/biometric-atm)



TRUE CARD-LESS
SECURITY



MOBILE-INITIATED
ATM ACCESS



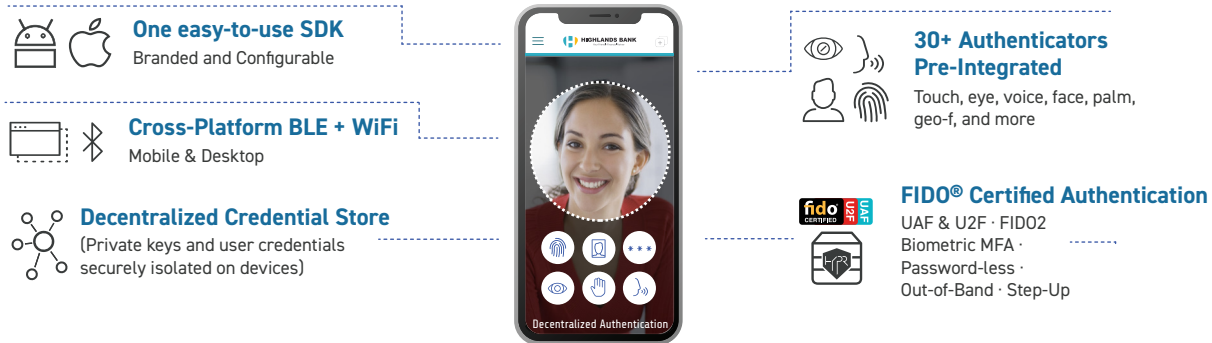
DECENTRALIZED
MOBILE BIOMETRICS



BLE, NFC & QR
SUPPORTED

INTEGRATE THE HYPR SDK INTO YOUR APPS AND SAY GOODBYE TO CARD SKIMMING

With HYPR, your users can authorize ATM transactions from their mobile device without having to remember pins or passwords. The HYPR SDK allows you to provide a secure card-less authentication for your cardholders with a simple app update. With HYPR, your ATM does not require additional hardware to enable card-less authentication and communicates with the mobile device via HTTPS, WiFi, BLE or NFC. By decentralizing user authentication, HYPR stops mass ATM breaches, eliminates card skimming, and sets the foundation for secure card-less transaction.



DEPLOY HYPR'S FIDO-CERTIFIED ARCHITECTURE TO ACHIEVE PSD2 COMPLIANCE

PKI Authentication is critical to addressing the PSD2 compliance requirements designed to mitigate theft of payment service credentials by all known attacks that successfully harvest “shared secret” credentials (such as PINs and passwords). HYPR provides asymmetric cryptography out-of-the-box by leveraging a FIDO-Certified architecture to enable PKI authentication and secure ATM credentials.

At the time of registration, a user’s private key is generated from a biometric such as a fingerprint or face. This key always remains on their personal device and is used to sign ATM transactions. HYPR can be configured to interact with the ATM via BLE, NFC, or QR codes. User keys are never sent over the wire and the user never needs to interact with the ATM again.

Decentralized ATM Authentication

1. Transaction Request
2. User Validity Check
3. OOB Authentication Request
4. Authentication Challenge
5. FIDO Signed Response
6. Authentication Complete
7. Approved Session

