MEET PSD2 & SCA REQUIREMENTS WITHIN DAYS

Your organization is committed to meeting regulatory requirements for Strong Customer Authentication (SCA), and you are tasked with achieving PSD2 authentication compliance. We’ll show you how industry leaders such as Mastercard have deployed HYPR’s Decentralized Authentication Platform to enable payment security that meets and exceeds the European Banking Authority’s (EBA) PSD2 requirements.

ACHIEVE PSD2 WITH TRUE PASSWORD-LESS SECURITY

HYPR provides a secure and convenient approach to meet the authentication requirements as defined in the EBA’s final draft Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA). The RTS describes the principles of multi-factor authentication and authentication code generation to support strong consumer authentication for PSD2.

With HYPR, your PSD2 needs are addressed by solving the underlying problems of credential reuse and fraud that are caused by centralized passwords. By eliminating centralized passwords, HYPR provides a fast and easy way for you to achieve PSD2 compliance for strong authentication of user logins and cryptographically signed transactions.

Deploy true password-less security with HYPR to immediately meet several key PSD2 requirements. Your enterprise will save significant time to market and millions of dollars versus building your own PSD2-compliant solution, and you’ll never have to worry about future changes to authentication security standards. HYPR will always offer payment service providers the most advanced, compliant and user-friendly authentication experience.
**REQUIREMENT #1 - USE OF CRYPTOGRAPHIC SIGNATURES TO AUTHORIZE TRANSACTIONS WITH LINK TO AMOUNT AND PAYEE BEING APPROVED BY USER**

**What it means** - This requirement describes the use of transaction signatures for payment approval. Your users must be able to authorize a specific transaction, amount, and receiving party using asymmetric cryptography.

**SOLUTION - DEPLOY HYPR’S DECENTRALIZED CLIENT & SERVER**

HYPR meets this requirement by enabling **Decentralized Biometric Transaction Approvals**. Integrate the HYPR SDK into your applications, and your customers will instantly be able to use their mobile device to approve web and mobile transactions, including amounts and payees. Decentralized authentication is critical to enabling PSD2 compliance by ensuring a user’s credentials are always stored safely on their personal mobile device.

**FIDO-CERTIFIED ARCHITECTURE**

Asymmetric cryptography is the foundation of the security model addressing the RTS security requirement designed to mitigate theft of payment service credentials by all known attacks that successfully harvest “shared secret” credentials like passwords, effectively mitigating the techniques that are behind 81% of all data breaches.

HYPR provides you asymmetric cryptography out-of-the-box. The solution leverages a FIDO-Certified PKI architecture to enable decentralized authentication, and secure payment tokens. At the time of registration, a user’s private key is generated from a biometric such as a fingerprint or face and is used to sign transactions initiated by a relying party. This key always remains on their personal device.
REQUIREMENT #2 - PROTECTION OF USER’S CRYPTOGRAPHIC MATERIAL FROM UNAUTHORIZED DISCLOSURE.

What it means - This requirement describes the protection of users’ private keys and payment tokens of by way of mobile security controls, such as Trusted Execution Environments, Secure Enclave, and ARM TrustZone.

SOLUTION - INTEGRATE HYPR’S ADVANCED DEVICE PROTECTION INTO MOBILE APPS

HYPR meets this requirement by enabling Advanced Device Protection (ADP). HYPR’s ADP solution ensures that your users’ cryptographic material is protected from malware and stored below the operating system level. This approach to PSD2 compliance goes above and beyond the requirements set forth by the RTS by simultaneously enabling GDPR-compliant decentralized authentication. Rather than storing credentials centrally, you will store each user’s cryptographic material – including biometrics, PINs, passwords and private keys – on their trusted mobile device where HYPR encrypts, isolates and secures it.

Encrypt and store decentralized credentials in the most secure environment on any trusted user device. With Advanced Device Protection powered by HYPR, you will stop malware on mobile devices by securing user credentials below the operating system level. ADP supports RSA 2048-bit, ECC 128-bit & 256-bit Encryption, Secure Data Storage and White Box Encryption.
REQUIREMENT #3 - ABILITY TO AUTHENTICATE USERS BASED ON TWO OR MORE OF THE FOLLOWING ELEMENTS: POSSESSION, KNOWLEDGE, AND/OR INHERENCE.

What it means - This requirement describes the need for multiple authentication factors - including but not limited to - Something You Have, Something You Are, and Something You Know.

SOLUTION - DEPLOY HYPR’S FIDO CONTROL CENTER

HYPR meets this requirement by enabling advanced multi-factor policy management with the industry’s first FIDO Control Center. Achieve PSD2 compliant authentication by combining biometric modalities with transaction policies and business logic – all without writing a single line of code. HYPR features dozens of pre-integrated authenticators including fingerprint, voice, face, eye, palm, decentralized PIN, and more.

We’re proud to have innovated and deployed Control Center - the first FIDO Management Console. Manage, provision, and deploy millions of users. Respond to adversary tactics in real-time without making code-level changes, and achieve unprecedented control over the user authentication experience. Experience it all in one simple, intuitive user interface.

Advanced Capabilities

- Manage decentralized apps & access points
- Fully API-Driven, plug-ins for IAM/IdP systems
- Real-time control, analytics, & reporting
- Authenticator & Policy Management
- Biometric Orchestration

“HYPR’s technology is a smart way to keep critical data where it belongs – close to the consumer.”

- Bob Reany, EVP Global Products & Services for Identity Solutions, Mastercard