Get Verified, Secure Passwordless Multi-Factor Authentication With ID Dataweb and HYPR

Users Demand Frictionless Authentication, Enterprises Require Uncompromising Authentication Security

Users want easy and expect secure. Today's enterprise is forced by default to use shared secrets, namely passwords, as the foundational factor for authentication into workstations, identity platforms, clouds and other applications. This presents productivity friction for users as well as massive security challenges and password-related costs for the enterprise itself. Despite the intent to improve security around authentication, user friction concerns mean legacy MFA has mostly been limited to VPN and remote access, leaving workstations wide open. Moreover, legacy MFA has been deployed in a fragmented manner, overwhelming most enterprise users who need to manage multiple MFA methods to access VPN, identity platforms, clouds and applications.

When an enterprise deploys passwordless multi-factor authentication (PMFA), they offer convenience and usability without sacrificing security. However, a vulnerability exists early in this process when pairing the credential with the user, either for credential issuance or recovery. If the credential pairing is compromised by an attacker, that secure and convenient authentication factor makes malicious activity even easier. Identity verification during this critical phase is needed to ensure that the user pairing the phone is legitimate.
HYPR and ID Dataweb combine to solve this problem with verified secure passwordless credentials.

Easy for Users, Secure for Enterprises

With True Passwordless MFA, the use of shared secrets such as passwords is replaced with public key cryptography and FIDO open standards. HYPR's decentralized architecture allows enterprises to eliminate passwords across Windows, MacOS, and Linux machines, as well as virtual desktops (VDI), closing the desktop MFA gap once and for all. Utilizing ID Dataweb's AXN Verify service to assure that the correct user is receiving the credential, an enterprise is able to establish

Key Benefits

- **Easy Standards-Based Integration:**
  Deploy HYPR & ID Dataweb's solutions in tandem with simple configuration to unlock the full power of verified passwordless authentication.
- **Scale and Reliability:**
  Rely on the cloud-based infrastructure with built in redundancy and failover.
- **Proven in the Enterprise:**
  Keep company with the largest financial and healthcare organizations in the world, utilizing these solutions to verify and authenticate their users.

the match between the user's physical identity, digital identity and mobile device being used for authentication. Users have a simple, frictionless and secure method of authentication.

Identity verification during credential issuance and recovery ensures that the user pairing the phone is the correct user. Depending on the security needs, this can be a simple mobile match (the identity is the user who owns this phone) or KBA challenge (does the user pairing know what they should) or a government ID match (does the user pairing have an ID and matching biometrics for the identity). The important part is that you establish the match between the physical identity, the digital identity and the mobile device being used as an authenticator.

PMFA is the wave of the future both for workforce and consumers. It is easier for the user, more secure for the enterprise, and intuitive and fast for authentication. The important part is that you establish the match between the physical identity, the digital identity and the mobile device being used as an authenticator at the initial point of vulnerability.

Initial Onboarding

During initial onboarding, the most stringent identity verification template should be used — MobileMatch and BioGovID. Verify the user's possession and ownership of the mobile device being used for the credential, then verify their identity with a government issued ID and matching selfie — you hit the two most secure factors (what you have and what you are) in one flow.

Credential Recovery

During credential recovery, an enterprise has already established the identity of the user during onboarding, now they can use a more streamlined template and just check MobileMatch. Determine that the user is indeed the legal owner of the phone, that it hasn't been used for fraud, and that the user has actual possession of that phone. Only then will an enterprise re-issue the credential.

Why HYPR

- Replace passwords and legacy MFA with Passswordless MFA
- Solve the Desktop MFA gap with Passwordless MFA starting at the desktop
- Extend Passwordless MFA to IdP, VPN, clouds and more, providing users with a simple unifield authentication experience

Why ID Dataweb

- Robust Orchestration of hundreds of attribute feeds
- Single interface to initiate identity verification workflows
- Policy Engine designed to easily create the perfect identity verification workflow

ID Dataweb is the leader in identity verification, matching a user's digital to their physical identity for ongoing trust with a user. The AXN™ is the only platform that ties top identity verification, multi-factor authentication, and login services together through a single cloud interface. The easy to use dashboard enables creation of custom verification and authentication policies to create full life-cycle, self-healing trust with your users.

THE PASSWORDLESS COMPANY

Email: info@hypr.com
Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's true passwordless multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.