KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger
March 31, 2022

# HYPR Passwordless and Phishing-resistant Authentication

Passwordless authentication is becoming the new normal, bypassing the need for users to maintain passwords, and thus bypassing the inherent security challenges of passwords. In the broad range of solutions that claim being passwordless, HYPR excels with its desktop and Microsoft Active Directory integration, and support for a broad range of specialized and complex use cases. HYPR provides a highly secure, phishing resistant approach on passwordless authentication.

By **Martin Kuppinger**
mk@kuppingercole.com

# Content

**1 Introduction** . . . . . 3

**2 Product Description** . . . . . 5

**3 Strengths and Challenges** . . . . . 8

**4 Related Research** . . . . . 10

**Content of Figures** . . . . . 11

**Copyright** . . . . . 12

# 1 Introduction

Passwords can easily be stolen, guessed, or compromised. Relying on passwords for security has become increasingly risky and problematic for organizations. End-user behavior and new attacks that take advantage of them can jeapordize the security of the computer, the data and information systems that run the organization. Numerous studies have shown that most data breaches involve the use of stolen credentials and compromised passwords, making them one of the weakest links in cybersecurity.

To understand why a passwordless solution has the potential to secure and enhance the IT systems of an organization, it is important to recognize why passwords are failing as an authentication system. In most cases, users use or reuse similar passwords across different applications. Moreover, new sophisticated methods of social engineering are being used to harvest heightened user credentials en-masse; and this increases not only risk and vulnerability but also the possibility of password-based threats such as brute force attacks, phishing, smishing and MitM (Man in the Middle) attacks.

As a result, organizations are continuously seeking to address this fundamental security risk. The IT security community has long known that passwords provide little or no security at all as a means of authentication. Therefore, as remote work becomes more prevalent and cyberattacks continue to increase, preventing a password compromise is one of the main challenges organizations face today. In response, investment into cybersecurity has soared but, in most cases, these efforts have not fully addressed the reliance on passwords and the vulnerabilities they present.

The main problem of passwords in the workforce is the security risk they pose to the entire digital ecosystem of an organization. Furthermore, managing existing passwords within an organization can be burdensome, time-consuming, and costly. Since password elimination is recognized as a fundamental goal for the IT security industry, passwordless options are increasingly gaining popularity and widespread adoption. To minimize the reliance on passwords and the associated risk, the industry has been working for a long time on different technical solutions and standards.

However, many solutions claiming to be passwordless do not fully eliminate passwords, but simply reduce the number of passwords at the frontend by hiding a password, or add another insecure factor for authentication. Various solutions are still password-bound such as password managers, and legacy multi-factor authentication (MFA) solutions, which utilize passwords as a factor in their authentication process. Solutions that are truly passwordless should employ secure factors such as biometrics and should adhere to industry standards , such as FIDO.

Passwordless authentication solutions should provide a consistent login experience across all devices, introduce a frictionless user experience, include an integrated authentication approach, support industry standards, support access management products that use SAML or OIDC, and eliminate the dependence on passwords or other easily phishable factors, as an authentication method.

To stay competitive, secure, and compliant, organizations must actively seek a more comprehensive way of assessing and managing security risk without disrupting the users and the business. By removing passwords as an authentication method, organizations will end up with a modern authentication system that does not rely on users remembering passwords. If successfully implemented, the passwordless solution will add a significant layer to the overall security posture of the organization while providing a frictionless experience to the users. It increases both the level of security and seamless user experience.

# 2 Product Description

HYPR is a provider of passwordless and phishing-resistant authentication solutions, enabling users a simple, convenient, and secure authentication. In contrast to many other solutions, HYPR integrates with the desktop authentication, securing initial access of users to their systems. Other solutions in this market segment only target access to, e.g., cloud services, but not the initial access. Thus, the entire path from initial access to a system such as a desktop PC, and forward to backend services, can be protected at multiple levels.

The solution delivers three levels of SSO:

- Single Sign-On: Based on the integration with the desktop authentication and a primary login to Microsoft Active Directory, HYPR achieves a comprehensive Single Sign-On experience across all applications. There is no need for a second, separate authentication to SSO and Identity Provider solutions or applications such as Microsoft 365.
- Simple Sign-On: The authentication process for the user becomes simplified. Depending on the approach chosen, users can unlock their smartphone and use the HYPR app, or they can use hardware built-in FIDO authenticators such as TouchID or Windows Hello Camera, when web-based authentication is required
- Secure Sign-On: Finally, HYPR also works in a highly secure manner. By initiating each authentication from the smartphone, via the HYPR app, there is no push of sensitive information to the smartphone involved. This provides a significant level of phishing resistance.

In combination, the approach, being passwordless, provides protection against password-based attacks, which still are the most common cyber-attacks. It is easy to use and relies on authentication steps that are common to every user today. Not being dependent on passwords also reduces help desk cost, which is significantly affected by the cost involved with resetting passwords.

While the advantage for the average user is in the simplicity of modern, passwordless authentication, administrators also benefit for privileged access, by avoiding long and complex passwords and, instead, leveraging the HYPR app on their smartphone, a hardware security key such as a YubiKey, or their desktop-native biometric authenticator.

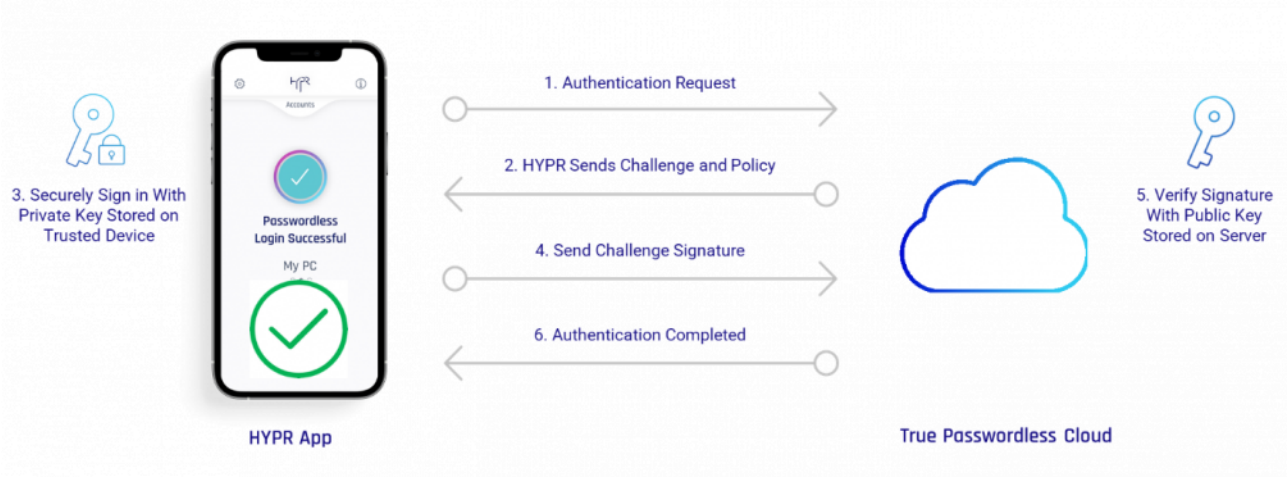


Figure 1: The HYPR authentication flow is initiated from the smartphone [Provided by HYPR]

In contrast to other solutions, the HYPR authentication flow is initiated from the smartphone of the user, via the HYPR app. It sends an authentication request to the HYPR cloud, which returns a cryptographic challenge and information about the authentication policy. The policies are managed centrally via the HYPR cloud. Thus, every policy change becomes immediately effective at the next authentication of a user. HYPR then uses the private key that is stored on the trusted, registered device in a secure element such as the Apple iPhone Secure Enclave. The HYPR app delivers a challenge signature back, which is verified via the public key that is stored on the server side. If this is a verified user, authentication is completed. By building on proven concepts such as strong and established cryptographic methods (RSA 2048 bit, ECC 128 bit and ECC 256 bit), and the secure elements on the device, HYPR delivers a very high level of security.

The authentication flow supports a wide range of use cases. For Windows desktop authentication, as for every authentication, the HYPR app is the starting point. Users select the workstation and initiate login. The authentication flow then is, when looking more into details, based on the FIDO and X.509 standards. The private key is stored either on the smartphone, the hardware security key, or the device trusted platform module (TPM).

For every authentication, two factors are used: most commonly a smartphone in combination with biometrics or a YubiKey in combination with a decentralized PIN. In some scenarios such as VDI (Virtual Desktop Integration) authentication, a QR code is generated by the HYPR authentication server, which a user will scan with the HYPR app on their smartphone in order to initiate the passwordless login. And even without connection to the internet, the HYPR app is providing public key encrypted offline PINs for a safe yet simple authentication.

Enrollment of the HYPR app commonly is done via an EMM / MDM (Enterprise Mobility Management / Mobile Device Management) solution, or it can simply be downloaded from the app store. The app can be rebranded to the customer's design. Additionally, the client must be installed on the Windows or MacOS device, and Active Directory Certificate Services (ADCS) must be enabled for obtaining a smartcard logon user certificate.

The management runs centrally via the HYPR control center, which also provides full FIDO2 support. HYPR also is a board member of the FIDO Alliance, helping to drive innovation. Here, the deployment of HYPR to users can be managed, also supporting full integration to Microsoft Active Directory for the user accounts. The policies also are managed centrally, and fraud analytics based on factors such as geo-location and user behavior analytics is performed centrally. This enables, based on the defined policies, also to block users or take other actions. The HYPR cloud has SOC 2 Type 2 and ISO 27001 as well as ISO27017 and ISO 27018 certifications.

Some of the specific features include support for roaming users, which allows multiple users to authenticate to the same device (for shared devices), but also users to authenticate to multiple devices easily. A side-effect of this is that there is a "run as administrator" approach, which allows users to authenticate as both administrator and standard user on a device, and switch between these two without the need for logging off and on again.

# 3 Strengths and Challenges

HYPR provides a well thought out and secure solution for passwordless and phishing-resistant authentication. Their strength is derived from the support for the entire flow from desktop authentication to backend applications, and the utilization of the established FIDO2 standards as well as strong cryptographic algorithms.

A differentiator is, aside of the integration to Active Directory/Windows desktop authentication, the fact that HYPR also supports a range of common use cases such as kiosk mode (multiple users for one device) or run as administrator mode (one smartphone and device used to authenticate multiple users), as well as support for VDI and RDP (Remote Desktops).

The solution is easy to install and use, backed by a secure cloud for the central management and configuration. Policies are managed centrally and enforced automatically at next login.

The Microsoft Active Directory integration of HYPR is both a strength and a challenge. For organizations that rely on Active Directory authentication -- still most organizations -- this provides excellent integration. However, it requires deployment of Active Directory Certificate Services, and HYPR is rather neatly integrated with Active Directory, which limits the use for other customers.

In sum, HYPR counts amongst the leading-edge solutions for passwordless authentication. Customers must analyze their use cases and existing environment. Specifically for complex use cases with the requirement for strong desktop authentication or remote authentication, HYPR should be evaluated.

## Strengths

- Delivers truly passwordless, phishing-resistant authentication.
- Easy to setup via app, client software, and the use of a secure and certified cloud backend.
- Strong integration with Microsoft environments, specifically Microsoft Active Directory and Kerberos.
- Full support for FIDO standards.
- Utilizes strong cryptographic algorithms and secure elements on the smartphone or desktop device, but also allows for storing the private key on a hardware security key (YubiKey).
- Delivers protection from the desktop authentication on, not just at the application level.
- Support for both MacOS and Windows environments.
- Strong support for common use cases such as roaming users / kiosk mode / offline mode
- Full support for VDI/RDP.

## Challenges

- Lack of support for legacy systems that continue to rely on passwords.
- Reliance on existing Microsoft Active Directory infrastructures as need to deploy AD Certificate Services.
- Azure-only joined devices not supported yet.

# 4 Related Research

Leadership Brief: How to Get Rid of Passwords - Today
Leadership Compass: Access Management

# Content of Figures

Figure 1: The HYPR authentication flow is initiated from the smartphone [Provided by HYPR]

# Copyright



**KuppingerCole Analysts** support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

**KuppingerCole**, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.