THE FUTURE IS DECENTRALIZED

A HYPR published study on Decentralized Authentication and its impact on the Identity and Access Management landscape.

Jointly written by Sean Connolly of HYPR and Alan Goode of Goode Intelligence.

CONTENTS

CENTRALIZATION IS THE PROBLEM

DECENTRALIZED AUTHENTICATION AS A SOLUTION

EMPOWERING DECENTRALIZATION WITH HYPR

INTRODUCTION

Now more than ever, the world is watching how companies manage consumers' data. We believe this creates a unique opportunity for you to stand out from the crowd, protect your customers and be a leader in cyber security. Large-scale data breaches are avoidable. The technology exists, and it is ready to implement.

This white paper, jointly written by Sean Connolly of HYPR and Alan Goode of Goode Intelligence, details why decentralized authentication is the way forward for enterprises wanting to solve a critical security challenge.

THE FUTURE IS DECENTRALIZED

CYBER SECURITY IS NOW A C-SUITE CHALLENGE AND OPPORTUNITY

As identity theft and identity related breaches increase at staggering rates, the world is turning its attention to how organizations manage user authentication. According to Verizon, in its 2017 Data Breach Investigations Report (DBIR), 80% of hacking related breaches are the result of weak or stolen passwords.

80%

80% of hacking related breaches are the result of weak or stolen passwords.

Source Verizon - 2017 Verizon Data Breach Investigations Report

Yahoo, LinkedIn, Sony and Equifax are just some of the large global companies that have been hit with hacks that have led to widespread identity theft long after the initial breach.

A combination of poor security management and weak password protection, often a result of poorly implemented hashing and encryption techniques, is leading to the recent rise in identity related breaches. Referred to as credential stuffing, criminals will attempt to use the stolen identities, along with their decrypted passwords, in an attempt to take over other accounts used by the same user.

CEOs must make cyber safety a top priority to protect their customers, their share prices and themselves. The European Union has established legislation to that effect. Any company that does business in the EU and has EU citizens as customers will have to adhere to The European Union's General Data Protection Regulation (GDPR). This regulation may prove to be the blueprint for data protection and privacy legislation around the world. Non-compliance with the GDPR may lead to hefty fines of up to 4% of a company's annual revenue (up to about $24 million).

THE NEED FOR DECENTRALIZED CREDENTIALS

Centralized authentication models, which store identity credentials including user IDs and passwords in a central database, are one of the biggest factors in the rise of identity theft and identity related breaches. If a central database is breached, thousands or even millions of identity credentials could be compromised.

That's what happened with the LinkedIn breach. The user IDs and passwords of 100 million members were stolen because LinkedIn was poorly protecting them – with unsalted SHA-1 hashing – and because all 100 million were centrally stored. LinkedIn initially claimed that the breach only affected six million identities, but four years after the first notification, they had to inform more than 117 million users to reset their passwords after reports that cyber criminals were offering to sell 117 million stolen records.

Storing, securing and maintaining a centralized repository of passwords carries high costs for what is essentially a prime target for hackers.

The 2017 breach of Equifax may be the most severe example of the dangers of centralization. Over 143 million consumers potentially had their social security numbers compromised. Additionally the 2015 U.S. Office of Personnel Management (OPM) breach saw over 5 million fingerprint records compromised and shined a spotlight on the risks of centrally storing biometric data.

ENTERPRISES ARE TRANSITIONING AWAY FROM CENTRALIZATION OF BIOMETRICS, PINs AND PASSWORDS

PASSWORDS ARE NOT THE PROBLEM

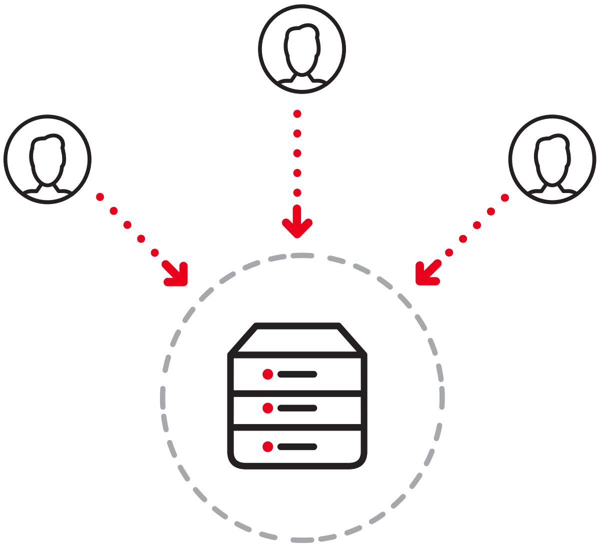
Commentators often accuse passwords of being the root of the problem are recommending the death of password-based authentication. With eye-catching headlines about massive data breaches, it becomes easy to put the blame on passwords. It's true, the password is far from perfect. Its biggest downside is that it is difficult to maintain integrity when users are responsible for creating and remembering their own passwords. But weak, stolen, or re-used passwords are not solely responsible for the large-scale breaches we're seeing today. They are a symptom of a much bigger problem. The primary issue is centralized storage of poorly protected personal credentials – including passwords, PINs, biometrics, credit card numbers, and other personal information.

Passwords have proven to be an effective method of authenticating users for decades. Password based authentication used in either single or two-factor authentication solutions are engrained in technology. It would take a monumental effort to completely eliminate them – if in fact that was the most pragmatic way to improve the security of authentication systems.

Passwords and PINs are still included as part of two-factor or multi-factor regulation and technology standards including those issued by the National Institute of Standards and Technology (NIST) and included by the European Banking Authority (EBA) as part of its Strong Customer Authentication (SCA) technology standards for the PSD2 payment regulation. The EBA's standards provide clear guidance on how consumers must be authenticated and requires the use of at least two independent elements from Knowledge (passwords and PINs), Possession (token or mobile) and Inherence (biometric). Strong passwords are part of the solution here for a modern authentication standard generated with industry input.

CENTRALIZATION IS THE PROBLEM

- USER CREDENTIALS STORED CENTRALLY
- SINGLE POINT OF FAILURE
- HIGH RISK OF BREACHES
- RISING IT COSTS



IS TWO FACTOR AUTHENTICATION THE SOLUTION?

Two factor authentication (2FA) combines two or multiple factor authentication methods – such as knowledge-based authentication (KBA) and generation and receipt of one-time passwords (OTP) – to create an additional layer or two of protection. There has been a steady rise in the adoption of 2FA with many of the leading digital service providers including Apple, Google, Facebook, and Twitter giving users the option to activate 2FA – or two-step verification (2SV) as it is often called. When 2FA is implemented well – meaning it does not create too large of a barrier to entry – and consumers choose to use it, it can add an extra layer of security.

The issue is that 2FA is often deployed alongside a centralized authentication scheme. Like passwords, 2FA can be an effective part of the solution, but it alone does not prevent or protect against the fallout of the massive data breaches we're seeing today. One of the largest breaches to date, the 2016 Uber "mega-hack," impacted all users and drivers. Even though the company had implemented a 2FA solution, hackers were able to steal the personal information of 57 million Uber users and drivers. Such breaches are reminders that additional layers of security do not solve the underlying issue of centralized credential storage.

THE RISE OF BIOMETRICS

Biometric authentication has shaken the industry and helped solve the security versus convenience conundrum, but does it really solve the centralized authentication challenge?

Since Apple introduced Touch ID on its iPhone 5S in 2013, we have witnessed wide-scale adoption of biometric authentication primarily on smart mobile devices. According to industry analysts, there are more than two billion devices including mobile phones, tablets, desktops, laptops, and wearables that support biometrics.

Biometrics offer convenient, frictionless user authentication and work well with the prominent endpoint, the smartphone. But as with passwords, their effectiveness in preventing identity theft and data breaches is tied to how well they are designed and implemented. Centralized biometric databases are prone to the same threat as centralized password repositories in that they can be stolen and re-used. In the 2015 OPM breach, millions of fingerprints were stolen because they were centrally stored.

As with 2FA, biometrics can improve security for the individual session, but they don't address the underlying challenge of centralized storage. Knowing this, service providers often implement biometrics as a convenience feature rather than a security control. Who wouldn't choose Touch ID over a 30 character password? **But if the user's fingerprint is linked to a password – as with many applications that leverage biometrics – then we are still dealing with the same centralized repository of credentials**. The user's password is still stored in a central repository, and there is no way of knowing if a specific trusted device is being used to authenticate the true account owner.

In theory strong passwords, 2FA and biometric security solutions should be more than enough, but they still fail to address the central storage of millions of valuable credentials. It's time to start focusing on the fundamentals.

It's time to decentralize.

THE FUTURE IS DECENTRALIZED

Decentralized authentication will become standard practice for securing digital experiences.

To prevent the types of massive data breaches we're seeing today, biometrics, PINs and passwords must not be tied to centralized credential stores. As part of a proactive strategy to prevent large-scale breaches and ensure public trust, business leaders and IT organizations are adopting decentralized authentication systems at a remarkable pace.

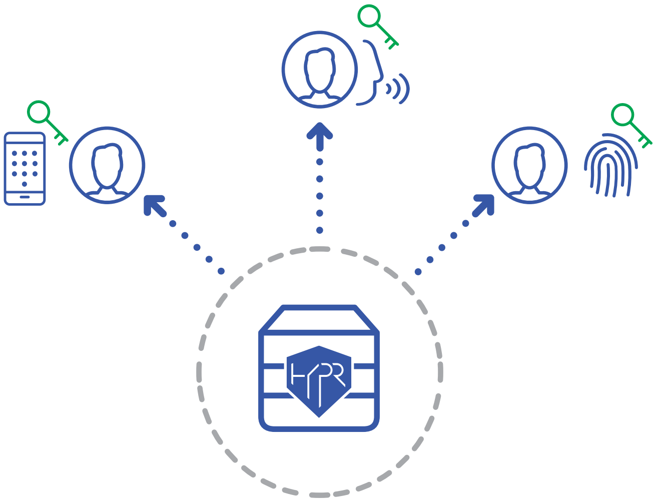
Why now?

The combination of open standards such as Fast Identity Online (FIDO) and the rapid adoption of mobile biometrics like Touch ID have made decentralized authentication possible at a global scale. FIDO standards are the most prominent open standarts for decentralized access. FIDO and standards like it will define how we build trust between a user and their service(s) of choice.

Now enterprises can use Touch ID and other biometric features to secure authentication from end-to-end. Notably, Bank of America was the first major financial institution to deploy FIDO authentication in a mobile app. From the technology sector, we already see wide adoption among industry leaders. Popular biometric sensors such as ones found on Samsung Galaxy devices and Microsoft's Surface tablets are making decentralized authentication possible by leveraging the FIDO standard. Samsung has implemented FIDO on device sensors and applications such as Samsung Pass. Microsoft has taken steps in this evolution with both the Windows Device Companion Framework and the Windows Hello PIN. As a FIDO-enabled credential, this PIN is decentralized. The PIN always remain safe on the user's device and is never centrally stored.

The Windows Hello PIN proves that the password is not dying, it is evolving; and with such an evolution the structure of authentication will change. We believe the industry is signaling a rapid paradigm shift away from centralized authentication.

DECENTRALIZED AUTHENTICATION MEANS CREDENTIALS ALWAYS REMAIN SAFELY STORED ON USERS' DEVICES



BENEFITS OF DECENTRALIZED AUTHENTICATION

- DECREASE SIZE OF THE ATTACK SURFACE
- PREVENT LARGE-SCALE BREACHES
- ENHANCE USER EXPERIENCE
- REDUCE IT COSTS
- ELIMINATE PASSWORD RESET COSTS
- PREVENT FRAUD AND CREDENTIAL RE-USE
- INCREASE CONTROL AND FLEXIBILITY

INDUSTRY TRENDS ARE ENABLING AND EMPOWERING DECENTRALIZATION AT A SCALE NEVER BEFORE POSSIBLE

STANDARDS adoption of pki-based standards to establish trust with applications

SENSORS integration of biometric sensors to authenticate users

SECURITY utilization of hardware security modules to store credentials on trusted devices

FIDO CALLS FOR CREDENTIALS TO BE STORED ON USERS' DEVICES

The FIDO Alliance provides the most prominent example of what a decentralized authentication framework should embody. FIDO protocols now seek to decentralize the process of authentication by storing a private key on a user's device. Only a public key is stored centrally by the service provider. This allows enterprises to shift credential storage from a centralized model to a decentralized model to protect themselves and their customers. Should there be any form of a database breach on a company's server infrastructure, there is nothing a hacker could use to impersonate its users. In fact, a true decentralized authentication implementation would possess no personally identifiable information at all.

PROLIFERATION OF BIOMETRIC SENSORS

The need for more advanced, secure hardware is increasing with the rise of biometrics and decentralization. With the device becoming our primary source of user verification, the sensitive information it contains must be properly protected. This shift in security is quickly becoming an industry standard. Apple implemented Touch ID which is built upon the Secure Enclave within their iOS devices; Android is pushing for hardware based security through the Trusted Execution Environment (TEE); Intel has introduced SGX; Qualcomm has introduced the SecureMSM and the list goes on. These technology leaders have embedded their devices into our lives. With these strides forward in hardware security, today's consumer is authenticating in a whole new way. Authentication credentials including private keys and biometric data always remain safe within the trusted environment on these devices and also offer a very difficult attack vector. Rather than target individual devices, there are easier, lower-hanging fruits for criminals to focus on such as centralized credential databases.

AVAILABILITY OF TRUSTED DEVICES

As service providers adopt decentralized standards, the role of trusted devices has never been so prominent or accessible. These devices are not only enhancing user experiences with biometrics, but when combined with open standards such as FIDO, they enable secure decentralized authentication at a mass scale.

From financial services to the healthcare sector, large enterprises are adopting decentralized systems at a remarkable pace. Now is the time to protect your enterprise and your customers.

SHOULD YOU BUILD OR BUY YOUR DECENTRALIZED ARCHITECTURE?

Building your own anything gives you a sense of ownership and more perceived control over the end product, but in this case there are several factors to consider.

Many large enterprises have calculated the benefits and costs of both options and have ultimately decided to purchase decentralized authentication. Purchasing a proven and reliable solution allows you to maintain a high level of control without the millions of dollars required to develop and maintain an in-house solution. Investing in a decentralized solution allows you to eliminate the likely astronomical costs of developing and maintaining your own system. It also enables you to benefit from:

- ACCELERATED TIME TO MARKET
- CONTINUOUS INTEROPERABILITY BETWEEN SYSTEMS AND DEVICES
- QUICK AND EASY ACCESS TO ALL THE LATEST SECURITY FEATURES
- YOUR PROVIDER'S DECENTRALIZED SOLUTION SHOULD INCLUDE 2FA, MULTI-FACTOR BIOMETRIC SECURITY, OMNI-ACCESS CONTROL, PLUS STEP-UP AND PASSWORD-LESS AUTHENTICATION

CONSIDER HYPR

The Solution Trusted by Enterprises to Secure Consumer, Employee and IoT Experiences

Consumer Authentication

- MOBILE
- WEB
- CALL CENTER
- PAYMENTS
- BRANCH & ATMs

Employee Access

- EMPLOYEE WORKSTATIONS
- VIRTUAL DESKTOP INFRASTRUCTURE (VDI)
- VIRTUAL PRIVATE NETWORKS (VPNs)
- APPLICATIONS ACCESS VIA SINGLE SIGN-ON (SSO)

IoT Security

- CONNECTED CARS
- SMART LOCKS
- SMART HOMES

BENEFITS

HYPR has made it easy for enterprises to deploy secure decentralized authentication across millions of users, with immediate benefits:

PREVENT BREACHES

By storing personal information such as biometrics, PINs, and passwords safely on users' personal devices, HYPR significantly reduces the risk of a centralized data breach while enhancing the security of online services.

ELIMINATE FRAUD

Enforcing flexible levels of assurance for high-risk transactions allows service providers to implement the right level of security for their online services. Coupled with decentralized authentication that prevents credential reuse, HYPR prevents account takeover and unauthorized activity to save you millions of dollars in fraud-related costs.

ENHANCE USER EXPERIENCE

By providing fast and friction-less authentication to mobile and web applications, HYPR provides your users a secure omni-access experience that keeps personal information safe.

DECREASE IT COSTS

HYPR has saved enterprises millions in service costs by reducing passwords resets, help desk requests, and call center inquiries. The HYPR solution is pre-integrated with dozens of biometrics, authenticators, and plugins for your IAM/IDP and fraud systems, reducing time to deployment and development costs.

INCREASE CONTROL

HYPR provides an advanced biometrics orchestration engine designed to deliver any administrator literal real-time control over authentication policies. Biometric sensors can be enabled or disabled across large populations of users in real-time with fallback authenticators to ensure the user experience remains flawless.

- **Manage, provision and deploy millions of users in real-time**
- **Fully API-driven integration with any IAM/IDP**
- **Real-time control, analytics and reporting**

HYPR SECURES MILLIONS OF USERS ACROSS THE FORTUNE 500 INCLUDING:

One of the world's top four global asset managers

One of the world's largest credit card networks

One of the world's two largest device manufacturers

CAPABILITIES

Decentralized Client

Authentication Server

The HYPR solution consists of a Decentralized Client and Authentication Server. These easy-to-deploy components empower an array of powerful decentralized authentication capabilities

MULTI-FACTOR BIOMETRICS

HYPR enables fingerprint, face, voice, eye, and palm recognition and provides dozens of biometric modalities out-of-the-box, fully integrated, and ready to deploy across billions of devices and sensors.

PASSWORD-LESS AUTHENTICATION

Biometrics and proximity based login allows users to be authenticated quickly and easily without use of passwords.

OUT-OF-BAND PUSH AUTHENTICATION

Enable users to authenticate to web applications using out-of-band push authentication via mobile.

STEP-UP AUTHENTICATION

Applications can perform step-up authentication based on business rules to support transactional logic based on multiple levels of assurance.

FIDO AUTHENTICATION

HYPR Provides FIDO-Certified authentication for FIDO UAF and U2F authentication out-of-the-box.

HTTPS OR BLE AUTHENTICATION

The HYPR Secure Employee Access solution enables users to perform the authentication functions from mobile devices over WiFi or over Bluetooth Low Energy (BLE) communications.

CONCLUSION

THE FUTURE IS DECENTRALIZED

We cannot continue to store credentials in central repositories where they are currently being stolen at an alarming rate. The age of the mega breach should be history and only a decentralized architecture can make that the case. HYPR's decentralized model secures identity credentials in a trusted environment on a user's trusted device to reduce the attack surface and change the whole business model for cyber criminals who logically target centralized identity stores. A criminal attack on a decentralized authentication system is neither trivial nor scalable.

Today, enterprises store many keys in one place and each user is responsible for many keys. Inverting this model will allow enterprises to store many keys in many secure places and for users to own one trusted key to many applications.

When the world's credentials are decentralized in this way, authentication becomes so much easier and of course, safer. CEOs and enterprises can rest assured they are protected from fraud and massive credential breaches. You can trust your users, your employees, and your connected devices. HYPR's vision is that of a secure decentralized future, in which enterprises can **trust anyone** and their users can **access anything**.

For more information about HYPR's decentralized authentication solution please visit **www.HYPR.com**

TRUST ANYONE

ABOUT HYPR CORP

HYPR is the leader in decentralized authentication with millions of users secured across the Fortune 500.

As enterprises transition from passwords to biometrics, they face the challenge of centralized authentication. Businesses often store user credentials in a centralized repository, creating a single point of failure targeted by hackers. Centralized authentication carries high risk, rising IT costs and has remained the #1 cause of major data breaches - until now.

The HYPR solution ensures that personal credentials always stay safely decentralized and encrypted on users' devices. By eliminating the need for a centralized credential store, HYPR removes the target and reduces the size of the attack surface to minimize your risk of a data breach.

HYPR unlocks a world of possibilities - empowering business leaders to eliminate fraud, accelerate transaction speeds, and reduce IT costs, all while increasing control and flexibility across mobile, web, and IoT applications.

With HYPR, enterprises are changing the way millions of users experience fast, secure access to our connected world.

TRUST ANYONE.

ABOUT GOODE INTELLIGENCE

Goode Intelligence is an independent analyst and consultancy company that provides quality advice to global decision makers in business and technology.

Goode Intelligence works in information security, mobile security, authentication and identity verification, biometrics, enterprise mobility and mobile commerce sectors.

Founded in 2007 by Alan Goode and headquartered in London Goode Intelligence helps both technology providers, investors and IT purchasers make strategic business decisions based on quality research, insight and consulting.

Goode Intelligence works with a cross-section of clients, from global brands that are ranked on the FTSE/Fortune 100 to start-up technology companies.

www.goodeintelligence.com

THANK YOU

HYPR CORP
45 W. 34TH ST. SUITE 710
NEW YORK, NY
10001

TRUST ANYONE

www.HYPR.com