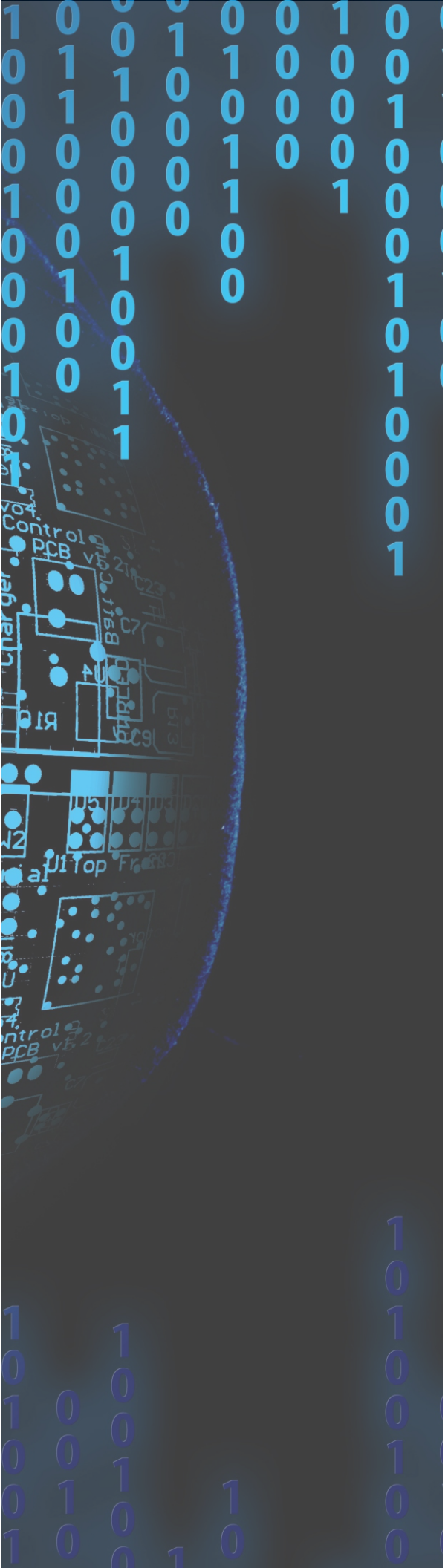
Identité™

Identité™ Presents | 2020 Whitepaper

NoPass™ to make authentication simple, secure and passwordless



Contents

03 Introduction

04 Burden of Password

06 Passwordless Technology

08 Full-Duplex Solution

09 Decentralized Authentication

10 Introducing NoPass™

11 The Simplest User Interface

13 NoPass™ SDK

17 NoPass™ and RADIUS

19 Our Place in the Market

20 Conclusion

Introduction

Password policy and hygiene have long challenged even the best I.T. industries. It is not just end users who are to blame for using weak and reused passwords, phishing frauds and storing passwords where they can easily be accessed are culprits. I.T. also bears responsibility for not properly, monitoring and securing their Identity Provider (IdP), usually Active Directory (A.D.) as well as the lack of enforcement and visibility into security measures to properly protect passwords. Many of today's security threats target user passwords/PINs.
Username + Password (U/P) requires only one secret – **THE PASSWORD.**

81% of data breaches are from weak, default or stolen passwords.

Verizon 2018

42% of end users admit to keeping passwords in Word, a spreadsheet or file on mobile device.

LostPass Report 2018

70% of successful breaches begin at the endpoint.

LostPass Report 2018

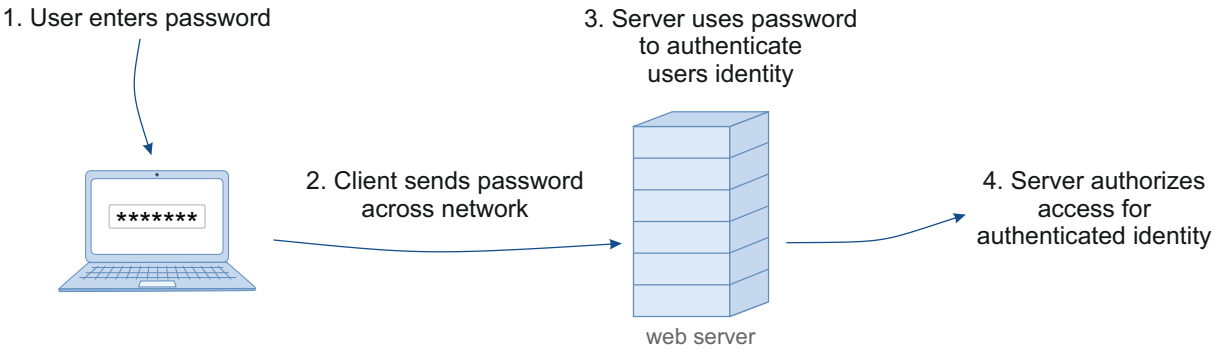
IT around the world see the beginning of a new era, where passwords are considered as a relic of the past. Even the strongest passwords are easily phishable. The motives to eliminate authentication systems using passwords are endlessly compelling and all too familiar to every enterprise IT organization.

BUT HOW DO YOU GET THERE?

With so many enterprises adopting biometrics and new methods of user authentication, analysts and vendors have discussed password elimination at great lengths across the industry. However, many have stopped short of acknowledging an inconvenient truth – that most companies that have adopted biometrics have not actually eliminated their passwords.
This white paper defines the criteria for a true Full-Duplex password-less architecture.

Burden of Passwords

Passwords are the most used form of website authentication. Password authentication requires users to create a key that only they (and the website) know as a way to access their online accounts.



Password based security has become less secure in recent times due to more sophisticated phishing attacks and challenges faced by users to create and manage numerous passwords. Also, the centralized storage of millions of user credentials (including passwords) in a cloud or a website server can provide a single point of target for hackers, which can greatly increase the cost of a single security breach.

Online attacks like Man-in-the-Middle (MitM) and Man-in-the Browser (MitB) can pose a substantial threat to online authentication by secretly modifying the communication between user and server. Online services are beginning to initiate stricter password rules and complicated methods for strong authentication, but these can pose **CHALLENGES** for the majority of users.

WHAT ARE THE PROBLEMS WITH PASSWORDS?

- Cause friction
- Difficult to create, remember and restore
- Guessable
- Rarely changed
- Often reused
- Sent over open networks
- Vulnerable from insufficient encryption to poor security controls on password vaults

PASSWORD-LESS TECHNOLOGY HAS A LOW ADOPTION RATE

There is no thought around making it super easy for all users, not during the registration of a user nor the actual authentication. Gathering all kinds of information from the user during the long and confusing registration procedure are the users nightmares for using these password-less solutions.
Carrying a hardware dongle all the time or receiving an SMS or email and then entering them in to complete the authentication process adds up to the hardship the user must take to gain that extra security and let go of passwords.

PASSWORD ARE EXPENSIVE – because users frequently forget them. For every password reset that incurs, soft costs are associated with the productivity lost while a user can't sign in. The company also incurs hard costs for every hour a Helpdesk administrator spends helping a user reset their password.

FEAR THAT HELP DESK COSTS WILL ACTUALLY GO UP

Current password-less solutions are costly. Examples of those are the two-step verification with SMS text messaging or voice. Another is the use of hardware OTP dongles that are expensive and can be lost. But overall, we should consider the fact that restoration of current multi-factor authentication methods and credentials will require additional training and an increase help desk call workload.

$1 mln

is spent per year on staffing and infrastructure to handle password resets alone.

Forrester Research

21 calls

per user per year on average receive support services.

META Group

70%

of all helpdesk calls are related to passwords, such as resetting employees' forgotten passwords.

Gartner

What if there is a solution to make it **MORE SECURE YET EASIER** than traditional password or OTP?

Password-less Technology

Multi-factor authentication (MFA) – for instance, a pin and password, or biometrics – has presented a more secure method for organizations. With increasingly complex access environments and more access points than ever before, IT teams have every reason to add multi-factor authentication options such as smart cards, hard and soft tokens, SMS, and more – wherever users connect to resources.
By going beyond passwords to add authentication steps, you can make user access to your resources **MORE SECURE.**

Today, IT security are moving toward passwordless authentication using advanced technologies like biometrics, PIN, and public/private key cryptography. Moreover, **NEW STANDARDS** like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) are enabling passwordless authentication across platforms. These standards are designed to replace passwords with biometrics and devices that people in your organization already use, such as security keys, smartphones, fingerprint scanners, or webcams.

Password replacement options can help organizations provide convenience and ease-of-use without high-security risks. Ideally, with password-less authentication, you can have a future ecosystem of authentication that meets the organizational needs of high security and privacy, usability, and interoperability among different authentication devices.
Moving forward, end-users should never have to deal with passwords in their day-to-day lives. In addition, with an intuitive sign-in/ sign-up user experience, help desk **COSTS CAN BE REDUCED.**

PASSWORD-LESS DELUSIONS

WHY isn't password-less authentication deployed more frequently? It is important to consider this. If the technology and capability of password-less authentication is here already, **WHY** are so few sites are using password-less authentication? Before we answer that, lets look at the progress made so far – **PASSWORD-LESS STANDARDS.**

From a standards point of view, FIDO reflects the industry's answer to the global password problem and addresses all of the issues of traditional authentication.

SECURITY

FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.

PRIVACY

Because FIDO cryptographic keys are unique for each internet site, they cannot be used to track users across sites. Plus, biometric data, when used, never leaves the user's device.

CONVENIENCE

Users unlock cryptographic login credentials with simple built-in methods such as fingerprint readers or cameras on their devices. Consumers can select the device that best fits their needs.

SCALABILITY

Websites can enable FIDO2 through a simple JavaScript API call that is supported across leading browsers and platforms on billions of devices consumers use every day.

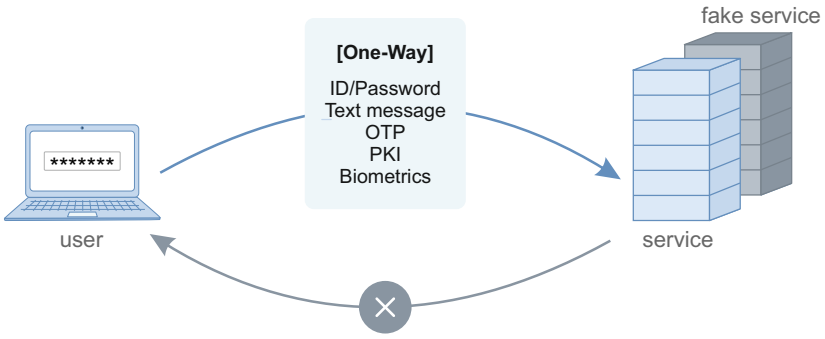
WebAuthn

Web Authentication (WebAuthn) enables online services to use FIDO Authentication through a standard web API that can be built into browsers and related web platform infrastructure. It is a collaborative effort based on specifications initially submitted by FIDO Alliance to the W3C and then iterated and finalized by the broader FIDO and W3C communities. WebAuthn was designated an official web standard in March 2019. WebAuthn allows users to log into internet accounts using their preferred device. Web services and apps can – and should – turn on this functionality to give their users an easier login experience via biometrics, mobile devices and/or FIDO security keys.

These standards are helping to get everyone on the right track to a pure password-less solution, but implementing them in such a way that it is simple enough for everyone to use is really one of the main reasons why we don't see more password-less solutions in use. There are also we also some inherent security weaknesses that still need to be addressed.

Full-Duplex Solution

There is a real urgency to move away from authentication systems that put passwords at the center. Most companies, however, stop short of actually eliminating the password. When password-less user experience is mistaken for password-less security, everyone pays the price.



All existing user authentication technologies work under the assumption that the service provider is always authentic. They send the credential information from the client to the server side. It means that it is one-way authentication from the client to the server. If the user provides his/her credentials, such as a user password, One Time Password or biometric information, without checking the service provider's authenticity, the credentials can be intercepted and used to impersonate the actual user.

IDENTITÉ™ PREVENTS EACH OF THESE TYPES OF ATTACKS.

The Full-Duplex solution of **Identité™** uses a safe and easy authentication system for the users. The three needed elements of successful authentication, are:

Something You Know

****

Username or the ID you use for logging in

Something You Have

Smartphone, one-time passcode or Smart Card

Something You Are

Biometrics, like your fingerprint, retina scans or voice recognition

We deliver the best solution to balance these three. With the help of advanced encryption methods and our user-friendly application, we offer **ABSOLUTE SECURITY** with a seamlessly easy experience for our users and their services.

Decentralized Authentication

CENTRALIZED passwords lead to mass breaches & credential reuse.
The continued use of centralized passwords alongside “password-less experiences” gives companies a false sense of security while they remain vulnerable to credential stuffing attacks. When companies store user credentials in a centralized repository, they create a huge target for hackers and invite credential reuse.

THE CENTRALIZED CREDENTIAL STORE IS:

- hackers' favorite target
- single point of failure
- high risk of breach
- susceptible to credential re-use
- expensive to secure and maintain

DECENTRALIZED authentication enables true password-less security.
Organizations are replacing the use of centralized passwords with decentralized authentication. Rather than storing millions of passwords in a single repository, user credentials are decentralized and stored safely on their personal devices. This approach removes the hackers' primary target and renders credential stuffing attacks infeasible.

DECENTRALIZED CREDENTIALS

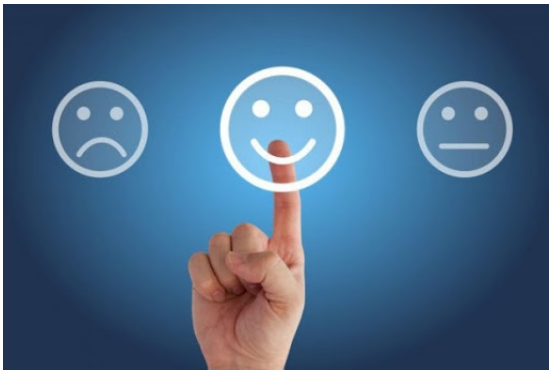
- stored safely on personal devices
- true password-less architecture
- stop mass breaches, fraud & phishing
- resistant to credential re-use
- low cost to secure and maintain

Introducing NoPass™

We believe authentication should be simple and secure. Many in the industry don't believe you can have simplicity and security. To achieve maximum security, many believe users must do more. However, before passing the burden on to the end user, lets look at the definition of multi-factor authentication. MFA involves combining multiple steps to verify three things – something you know, something you have and something you are.

Identité™

If users find that the methods for password-less authentication take longer or are more complicated, they either won't use it or will find ways to get around it. At **Identité™**, we are laser focused on the user experience. Our approach to usability and design have just as much weight in engineering the solution as making sure it is secure. Our methods for registration and strong authentication without passwords require fewer actions and can be executed by the user in less time than the traditional username and password. It's as simple as scan/tap/confirm from any smartphone. Alternate methods are available for those without those devices.



The Simplest User Interface

Research studies show that “User Experience” is widely considered to be one of the most important decision factors in choosing an authentication technology. We believe our methods and user experience is the best and easiest to use in the industry.

Below is an illustration of how such an operation would take place. Along with very strong security, the user does not even need to enter a password. The **NoPass™** server and application in the phone takes care of all of the bi-directional handshaking, requiring only that the user compare two images (a picture and a 3-digit number), then swipe or touch the approve button, and they are connected.

This method provides a million encrypted combinations, and is virtually un-hackable since the metadata is valid for only a few seconds and is totally useless after that. Even if the user mistakenly approves the transaction, we are able to detect the intrusion and block the entry into the server.

MULTI-FACTOR AUTHENTICATION

Multi-factor Authentication is a best practice that adds another layer of security to your user login. **NoPass™** enables quick and easy addition of MFA to your security strategy without compromising user experience or creating extra work for your dev team.

MUL

Detect whether the device is compromised or “jailbroken” (iOS devices) or “rooted” (Android devices). Developers can configure the app to run this check on launch (or at any other time) and then have the app perform certain actions if the device is found to be compromised.

LOGGING AND REPORTING

Log various events, actions, and other device activity to allow admins to generate log reports through the **NoPass™** Admin Console.

GEOFENCING

Program certain behaviors into an app based on a device's proximity to configured areas. Configure different actions into your app based on device location, such as displaying warning messages, restricting user access and wiping apps.

CERTIFICATE PROVISIONING

Provision the certificates directly to your app giving you control over what data your device users can access through certificate authentication.

NoPass™ and RADIUS

For most business to enterprise users, remote access has become a necessary requirement to maintain 100% availability for business applications and IT Operations. Most of the remote access is still done with a userID and password. Some have purchased very expensive MFA tools that are difficult to use and even harder to recover in case of lost credentials.

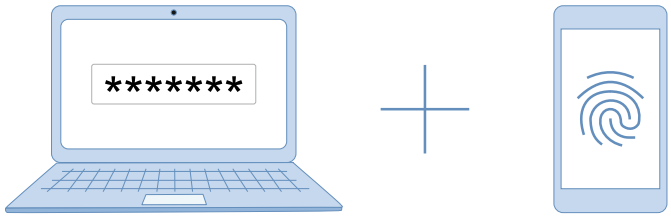
RADUIS

Radius Server allows for systems that support the Radius protocol to work in Tandem as a Radius client. The Radius Server holds and checks the username and password credentials and it can ask a Radius client to perform additional factors of authentication.
RADIUS additionally leverages a username and password that is unique to each user (usually the person's credentials stored within the IdP if integrated). By doing so, network security is increased due to the need for unique credentials.

The RADIUS protocol is a popular way to secure network access among IT admins. If admins were able to leverage two-factor authentication (2FA) when using RADIUS, that security capability would be greatly increased.

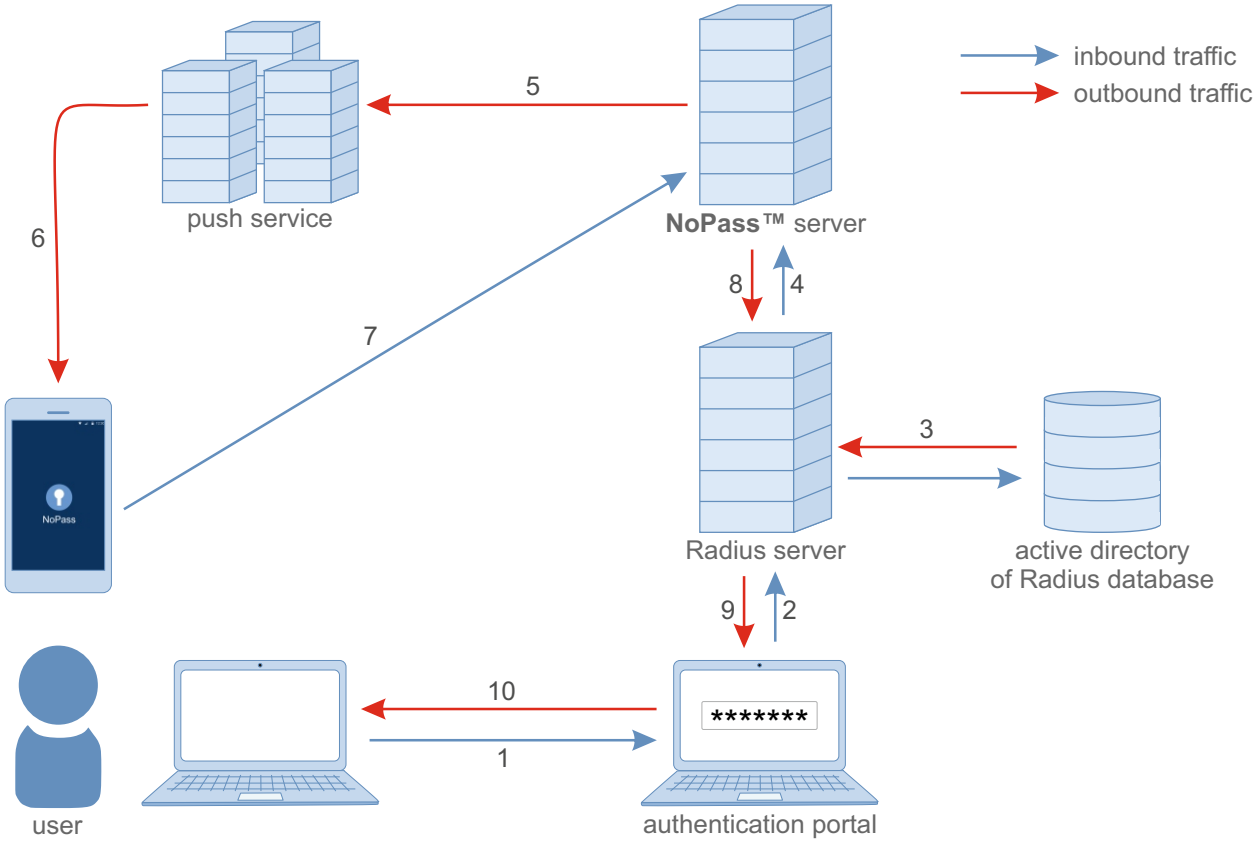
NOPASS™ 2FA

With the increase in phishing and other identity attacks in our day and age, authentication that requires a username and password (like RADIUS) can be potentially at risk. Sophisticated social engineering schemes and clever tactics can fool even the most savvy of users. In order to combat this, many organizations have started adding an additional step to these login processes, called two-factor or multi-factor authentication (2FA or MFA).
NoPass can act as a Radius client and perform two additional factors of authentication. This is something you have, which is the time sensitive secure token on the phone and something you are, which is the biometric on the phone.



TWO IN TANDEM

So, since RADIUS mirrors other logins that require a username and password, it makes sense to add 2FA to the process in order to further lock down network access. The **NoPass™** authentication server has the capability to act as a Radius Client, thus adding a 2nd factor of authentication to the user authentication process.



IT admins can also use **NoPass™** built-in 2FA service to enforce tighter security on their RADIUS (and VPN) authentication. A **NoPass™** user can leverage a single set of credentials, protected by 2FA, to access virtually all of their IT resources, regardless of their platform, protocol, provider, or location.

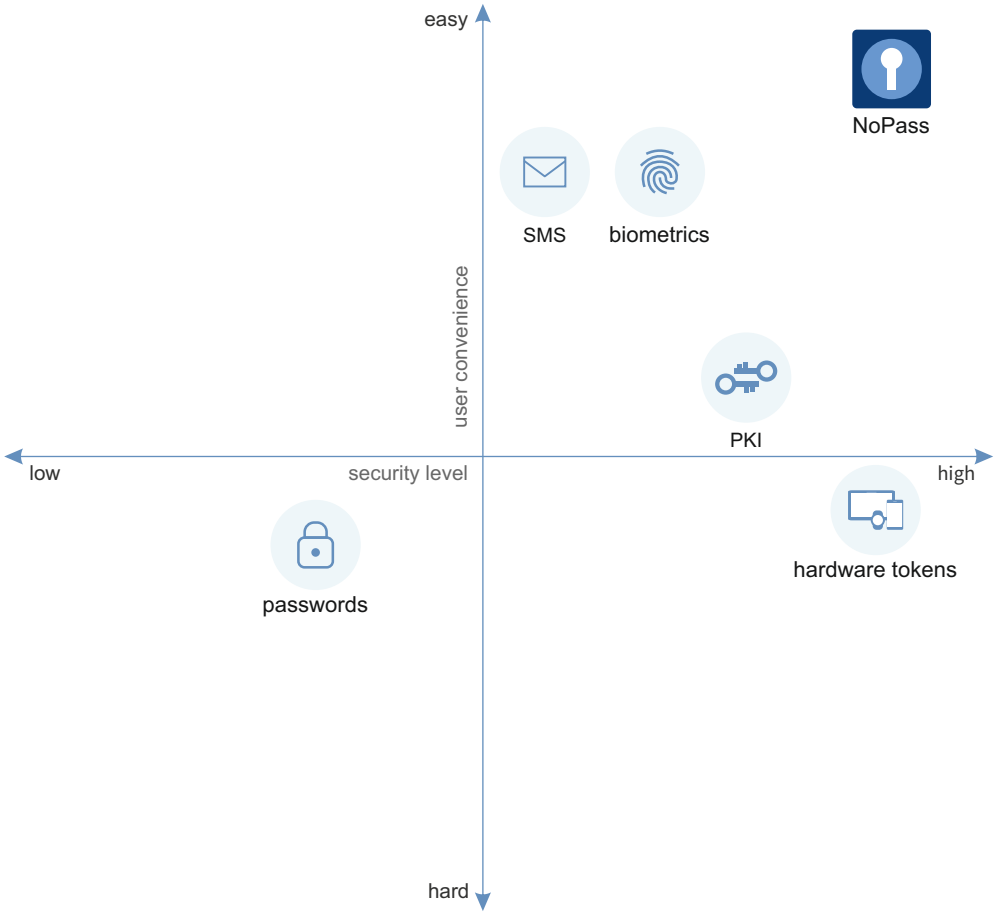
Our Place in the Market

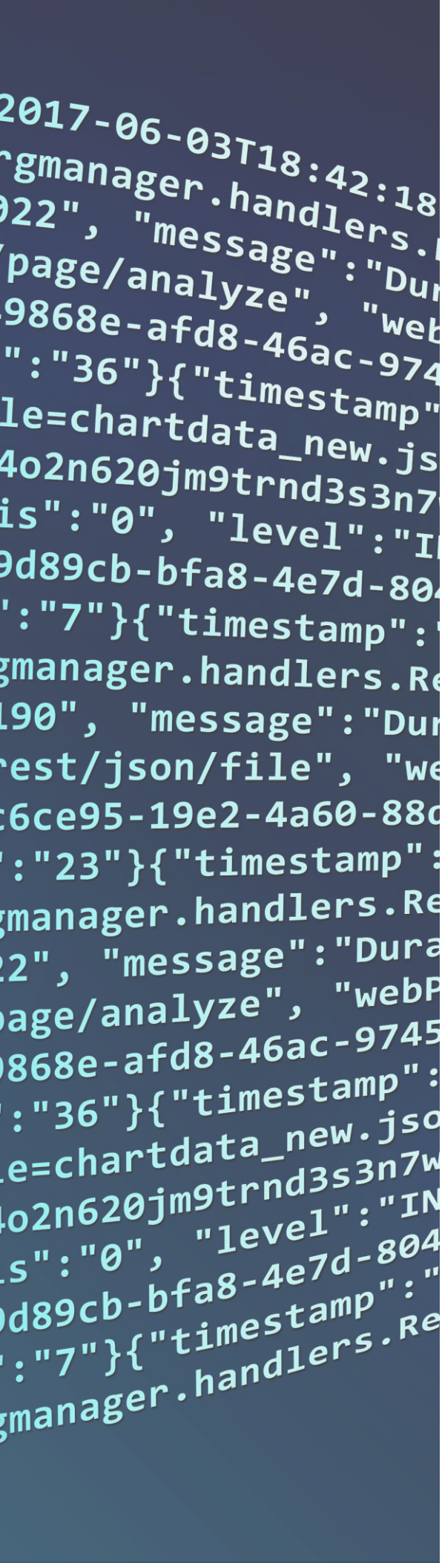
PENDING PATENTS IN DIFFERENT AREAS

- Concept of using a picture and digits for comparison
- Identify hacking methods in which we prevent or detect a threat
- Passwordless VPN authentication

WHY WE ARE BETTER?

- We incorporate the best elements of all current methods
- **Full Duplex Authentication™** (No user data sent until Server is authenticated)
- Multi-Factor, Multi-Channel User Verification
- Visual Comparison of Codes (No data to enter)
- Impossible to hijack the OTP codes because only metadata is sent
- Lower total cost of ownership





Conclusion

The adoption of modern multi-factor authentication technologies – like biometrics and public key cryptography in widely accessible devices – is one of the most impactful steps that can meaningfully reduce a company's identity risk. Given emerging requirements, organizations are slowly preparing themselves by making a plan to start moving to password-less technologies.

Nonetheless, password-less technologies are still not widely implemented. Going password-less is a long-term approach for secure authentication, and it's still evolving. It can take time to transition. Complicated and multi step processes have caused user dissatisfaction. Ease of use has been the biggest barrier until now, **NoPass™** helps users get over this hurdle by creating an easy and straightforward process that leads to a better user experience and more revenue.

NoPass™ Full Duplex Authentication™ process follows a decentralized authentication model. This lets us work together with any kid of traditional user authentication technology, such as PIN, OTP, PKI, and Biometrics. **NoPass™** has a flexible architecture to easily integrate with any User Authentication solution.

Decentralized authentication solutions such as **NoPass™**, allows for transformation of password-less experiences into true password-less registration and authentication. From financial services to the healthcare sector, large enterprises are adopting decentralized systems at a remarkable pace and are seeking to transition to a complete password-less architecture. **NoPass™** enhanced security finally protects both enterprise and the user, leading to higher levels of trust.

© Identité™ Inc. All Rights Reserved | www.identite.us

NoPass™ from Identité™