

The Expert's Guide to

# Passwordless Authentication

Preventing unauthorized access in post-pandemic  
times and beyond.

A primer and practical guide.

# Table Of Contents

## **P.3 Foreword**

## **P.4 What is Passwordless**

What is Passwordless Authentication, how is it currently done and why now is the perfect time to take on the challenge.

## **P.4 Best Practices**

Some of the cybersecurity industry's current best practices to get passwordless right from the start.

## **P.10 Don'ts - Avoid Pitfalls**

Every change in security comes at a risk. Let's walk you through how to avoid those risks and make it work for you, instead.

## **P.10 Summary**

## Foreword

# A global crisis that forces us to step up.

The pandemic has clearly shown that we need to significantly step-up our efforts and transition to improved approaches to prevent unauthorized access.

Many organizations have been painfully made aware of this fact. During the first months of the pandemic, corporate credentials exposed on the dark web have increased by more than 429% .

Even the most adamant advocates of the network perimeter have by now realized that it is just a relic of a long bygone era. A better approach to authentication is desperately needed and if we really want models such as Zero Trust Authentication to make a real difference, we need to stop patching the password like it's 1995.

Luckily, we are not living in 1995. In 2020, organizations are catching up quickly and there are lots of feasible options out there to replace passwords in ways that are secure, cost-effective and user-friendly. Gartner predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases — up from 5% in 2018.

This expert's guide aims to improve your understanding of passwordless authentication including shedding light on the industry's current best practices as well as critical pitfalls to avoid when considering passwordless for your organization.

# Passwordless Authentication

As opposed to password-based authentication, passwordless authentication does not rely on passwords or any other memorized secret to verifying a user's identity.

Instead of passwords, Identities can be verified based on a “possession factor”, which is an object that uniquely identifies the user (e.g. a one-time password, a registered mobile device, or a hardware token) or an “inherent factor” like a person's biometric (e.g. fingerprint, face, retina, etc.).

## How do you know that no one else knows your password?

Unlike possession or inherent factors, authentication that is based on something the user knows (a memorable secret such as a password, passphrase, or PIN code) is problematic because the user or the enterprise is unable to determine if their memorable secret is stolen or compromised.

How do you know that no one else knows your password? Additionally, memorable secrets are susceptible to easy theft, re-use by users, and requires constant management and handling by both users and IT managers.

## How is passwordless achieved?

There are different ways to achieve passwordless authentication. Making the right choice depends on organization's risk posture and business requirements.



### Email

Sign-In using a magic link or one-time code in the user's email inbox.



### Mobile Authenticator

Sign-In e.g. by approving the authentication on your smartphone.



### WebAuthN (FIDO2)

Sign-In by using the biometric capabilities of your device or a security key.

Signing-In in by sending a magic link to the users' is common, but by far the least secure option. The Mobile Authenticator, a mobile application installed on the user's smart-

phone, can make use of the smartphone’s hardware secure module and thus provide far better security. Since the smartphone is so widely populated this option can be a no brainer as it usually requires no additional hardware. WebAuthN, a standard commonly known as FIDO2, makes use of each device’s secure hardware module or the use of security keys to authenticate. While many companies have embraced the standard, it usually requires a separate hardware device if it’s not built in. A separate hardware can be forgotten, lost or stolen. When the authenticator is in-built, then it cannot be used on another device.

**Overall**, the Mobile Authenticator, especially when used as a MFA Authenticator e.g. when combined with biometrics and possession offers the greatest security, convenience while being a low hurdle to integrate.

### Email

- + fast & easy to implement
- relies on email provider
- not very secure

### Mobile Authenticator

- + very secure
- + high adoption rate
- + no additional hardware
- requires smartphone

### WebAuthN (FIDO2)

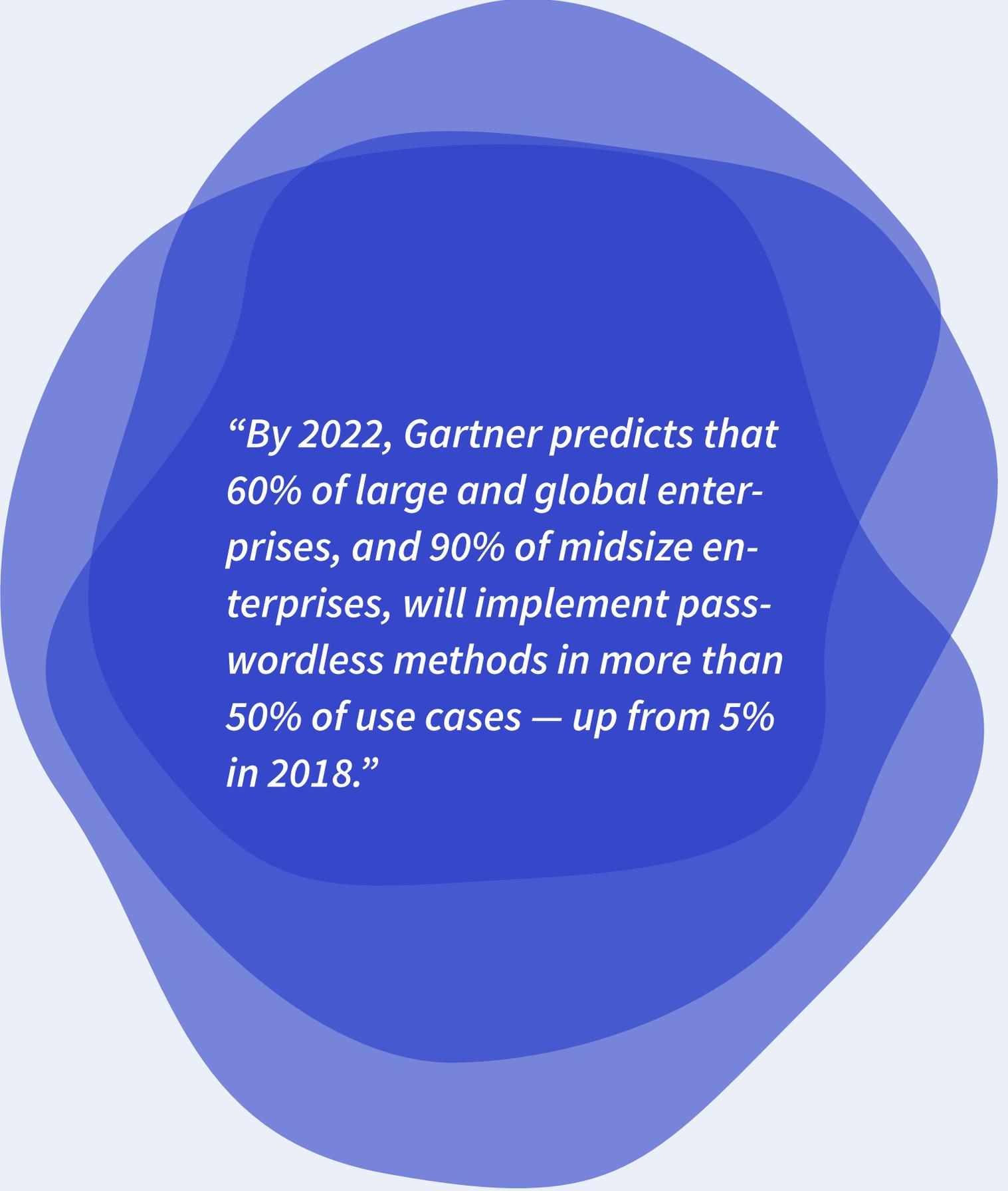
- + very secure
- + global standard
- + backed by big tech.
- not yet fully supported
- doesn’t work across devices

## Passwordless Experience vs. Truly Passwordless

Not all passwordless authentication solutions are created equal. The “How” you achieve passwordless authentication is critical. Often you find solutions that rely on merely hiding the password in the experience of the user while in the background replaying the password to authenticate. This is often referred to as “Passwordless Experience” and it still doesn’t solve the fundamental problem: How do you know that no one else knows your password?

While a passwordless experience provides certain benefits such as helping users not to forget their passwords, it is in no way comparable to the security benefits provided by a truly passwordless solution that doesn’t use passwords or memorized secrets at all.

With truly passwordless authentication, the authentication is based on a number of strong factors such as possession and inherence. Thus, making it inherently stronger than a memorized secret and additionally it eliminates all password-based threats such as phishing, credential stuffing, and others.



*“By 2022, Gartner predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases — up from 5% in 2018.”*

Why you should care

# 5 Reasons to Go Passwordless

- 1 Prevent Account Takeover.** No matter your mitigation strategy, passwords remain a huge risk for account takeover. That new SSO doesn't help.
- 2 Prevent Phishing.** As long as there are credentials to phish, users remain your weakest link and the easiest way for an attacker to gain access.
- 3 No More Weak Credentials.** Let's face it: Users will find ways to make their passwords weak, which leads to making them easy to crack
- 4 Reduce Overhead.** Just think of the things you could do instead of managing passwords for your employees.
- 5 Convenience.** Password, OTP, SecureCode, and yet another verification email. The mechanisms in place today decrease productivity.



# Best Practices

Some of the cybersecurity industry's current best practices to get passwordless right from the start.

When considering going passwordless, some things are crucial to getting it right. Here are some of the best practices to get the best value throughout the authentication lifecycle (provisioning, usage and account management).

## **1. Register Devices properly**

To establish trust in the authentication process, the device has to be authentic and trusted. Therefore, the device and app have to be registered to establish trust from the root. This includes ensuring that at the point of registration the device is not rooted and that proper protection mechanisms such as a device lock and app attestation are present.

## **2. Bind the Identity to the Device**

To trust passwordless authentication - the provenance, authenticity, integrity and identity of the authentication origin (device) has to be assured and coupled with the user identity. The authenticator device, app and the user identity are inseparable. As a result, an explicit transitive trust between the device, the app and the user identity has to be established via identity binding. This ensures that only the real user can access a service by authenticating with the trusted device on the trusted app and that an attacker cannot spoof and/or copy a user's identity from an untrusted device and app.

## **3. Use explicit transitive trust**

Ensure that an authentication is not trusted merely because it came from a user device. There must be a verifiable assurance that a transaction was done on a "trusted app" tied to a "trusted device" coupled to that "specific user" and authorized under the "user's total control".

## **4. Get Account Recovery right**

Recovery is one of the most important aspects of getting passwordless authentication right to not undermine its benefits. To achieve a secure recovery, the real user must be the one that can access the recovered data. This is achieved by secure identity proofing and client-side account recovery. The recovery shall never be performed on the server-side. This prevents any server-based insider attacks and credentials harvesting.

## **5. Use secure authenticated channel**

The authentication data should be sent via the secure authenticated channel. Ensure that the integrity and identity of the parties (IdP, device and app) involved in the authentication process are established using a secure mutual authentication process. This ensures the confidentiality of the authentication data and that unauthorised parties cannot alter/manipulate the authentication.

## **6. Ensure verifier compromise resistance**

With great power comes great responsibility. It is advised to ensure that if the IdP is compromised, it won't have any impact on the user's credentials. Any authentication method that requires to store user authentication secrets (e.g. shared secret key such as when using OTPs) is not verifier compromise resistant.

## **7. Properly authorize Additional Devices**

Ensure that an unauthorised user cannot make changes e.g. add a new device to a user account. Authorizing a new device from an existing trusted user device ensures that the user has both devices when adding a new device. Hence, only the user can add another device.





# Don'ts, Pitfalls & Risks

As with every change in authentication, it's crucial to avoid the basic pitfalls and understand your risk.

## **1. Never just replay passwords**

While simply hiding the password from the user might help reduce some risks associated with passwords, most of the risks of the weak credential remain. If the user's SSO password is compromised access to all resources is given and the attacker has unhindered access. Same goes for user's individual accounts.

## **2. Don't use credentials that aren't tied to a specific device**

When you keep the same credentials on each device without ensuring that the credentials can only be used with that specific device, then the credentials can be cloned to other devices and misused.

## **3. Don't use implicit trust when adding new devices**

By only using access to email mailbox to add devices or recover an account doesn't guarantee the true identity of the user. An email address may be compromised and used to recover a user account and thus be an easy way for attackers to bypass the secure identity binding as described above. The recovery method should be as strong as the authentication method. A convenient way of doing so is by having users approve adding a new device using their current authenticator device.

## **4. Don't use weak authentication factors**

This might seem obvious, but in practice we still very often needlessly rely on weak authentication factors. Authentication factors such as SMS, magic-link, manual entry, knowledge factor, etc. should be avoided where possible as they can be easily hijacked, stolen and replayed. Strong factors such as possession and control of a cryptographic key stored inside a secure element of a smartphone is the preferred way to go.

## **5. Don't make use of shared secrets**

Storing shared secrets such as in OTPs creates a possible of harvesting the secret either from the IdP server or from the user device. Use asymmetric keys with possession or inherence factors where possible.

## **6. Don't opt for buying additional hardware**

When considering a switch to passwordless authentication or improving your authentication security stance it might be tempting to buy additional hardware. The reality is though, that the costs and risks associated with new hardware usually outweigh their benefits. Not just the costs to acquire and implement, but also the running cost of maintaining the hardware. In addition to cost, introducing new hardware means new vulnerabilities and threats will be introduced with them. E.g. as opposed to smartphone where the owner quickly realizes theft, stolen hardware tokens may go unnoticed for days, resulting in more time for attackers to do harm.

## **7. Don't make a decision without properly evaluating your risk posture**

No decision should ever be made without properly understanding your risk posture, the current threats you are exposed to and how it would change. We have developed a free online threat model specifically to help you do that.

The “How” you do it matters

# Understanding Risk

Every mode of authentication comes with a certain risks. Below we listed some of the commonly used authentication mechanisms itself and how they compare in terms of the risks they create.

## Password

Single-Factor authentication using a password.

20

## Magic Link

Single Factor Authentication using a magic link to your email.

20

## Password Vaulting + 2FA (OTP, SMS)

Multi-Factor Passwordless Experience + using OTP as second factor.

15

## Passwordless MFA Authenticator

MFA, Truly Passwordless Mobile Authenticator.

12

## AuthN - Passwordless Absolut™ Zero-Trust Authentication

MFA, Truly Passwordless Mobile Authenticator with recommended safeguards.

4

### Where does this data come from?

In collaboration with the **National Cyber Security Center (NCSC)** in the UK we've created a comprehensive threat model to help organizations assess their IAM risk and make better decisions. The threat model is created based on the **Center for Internet Security (CIS) Risk Assessment Method** that conforms to and extends established risk assessment standards, such as **ISO/IEC 27005**, **NIST SP 800-30**, and **RISK IT**. Learn more and get the full model at [getidee.com/threat-model](https://getidee.com/threat-model).

# Summary

## **Passwordless is not just the future. It's a great option for today.**

Dealing with Identity is always a risk. But it's a risk that we have to deal with.

If you're considering to improve your authentication in 2020 and beyond, going passwordless is clearly the best path forward. And switching can actually be a breeze, considering the options out there.

Looking at current options, choosing a method that actually replaces passwords instead of just hiding them is key. This is sometimes referred to as "Truly Passwordless".

While the choice depends on your risk appetite, experts suggest using a Multi-Factor passwordless authenticator with proper safeguards in place. This helps you strike the right balance between security, usability and cost.

A couple of things matter to get it right, such as: properly registering and binding identity to the device, establishing transitive trust, using secure authenticated channels and making sure all use cases including recovery are done right.

And in the end it's always advised to use a threat model to understand risks and your posture, e.g. by using our online [risk calculator](#).

## Get Truly Passwordless, Zero Trust Authentication across your entire organization with AuthN™ by IDEE, today.

IDEE GmbH is a Cybersecurity vendor established in Munich delivering the most secure authentication and authorization SaaS offering available today. IDEE's AuthN™ is the truly passwordless zero-trust authentication and authorization service Made in Germany.

By truly eliminating passwords & credential databases AuthN™ removes not only all password related threats, but also reduces that immense pressure on budgets. AuthN™ has also been proven to enable transformation with a short time to result. The service is extendable based on industry standard protocols and can be applied to common and bespoke use cases in a wide range of applications and services, from ERP, CRM and UCC systems to HR applications.

Built on a zero-trust and zero-knowledge distributed-hyperledger architecture AuthN™ not only significantly increases security but also simplifies auditing and compliance. The built-in features such as advanced Multi-Party-Authorization & 3FA satisfy industry related regulatory requirements at no additional cost.

And this is why AuthN™ has gained the trust of CIOs and Identity and Access Management experts alike.

Supported by UK's NCSC & GCHQ IDEE GmbH is an active member of Bitkom and Teletrust in Germany with security and privacy by design as guiding principles. The company is based in Munich, with further locations in London and Belgrade.

[Learn More](#)

[Contact Sales](#)