IDEE

THE GUIDE: Passwordless Authentication.

Contents

Benefits, Challenges & Best Practice . . . 3

Introduction. . . . 4

What is Passwordless MFA? . . . 4

How Does Passwordless Authentication Work? . . . 5

Web Authentication Standard. . . . 6

The Benefits of Going Passwordless. . . . 7

Challenges to Passwordless. . . . 9

Best Practices. . . . 10

The Use Cases & Key Facts . . . 12

1. Passwordless with Remote Devices. . . . 13

    1.1 Passwordless with Virtual Private Network . . . 13

    1.2 Passwordless with Zero Trust Network Access . . . 14

    1.3 Passwordless with Remote Desktop Protocol . . . 15

2. Passwordless with Physical Devices. . . . 16

3. Passwordless with Cloud Services. . . . 17

4. Passwordless with SaaS Applications. . . . 18

5. Passwordless with Web Application. . . . 19

6. Passwordless with Mobile Application. . . . 20

Passwordless Use Cases Summary. . . . 21

Remote Devices . . . 21

Physical Devices . . . 22

Cloud Services . . . 23

Saas Applications . . . 24

Web Applications . . . 25

Mobile Applications . . . 26

AuthN by IDEE, The Difference . . . 27

Compliant & Compatible. . . . 30

Users Love AuthN by IDEE. . . . 31

Conclusion. . . . 31

Section 1.

Passwordless

Benefits, Challenges & Best Practice

Introduction.

Passwordless authentication has gained much traction in recent years and with good reason. Passwordless comes with many benefits, but for many organizations, there are also challenges and some risks. This guide seeks to provide practical and actionable advice, since through your research what you probably really want to know is passwordless right for you?

Our aim is to provide a comprehensive checklist across a number of common use-cases so that you may be able to better understand the application of passwordless and ultimately what is possible and what is not. This document is presented in two halves. First we provide a background and explain what passwordless is, its benefits and it challenges, and in the second half we delve deep into passwordless applications and specific use-cases.

Who is this guide for?

You are a CISO, reseller, VAR, MSP, CTO, CIO, Enterprise Architect, administrator or analyst.

What is Passwordless MFA?

Before we dive in, we should start with a clear definition of what passwordless is and what it is not. There are varying definitions.

Multifactor Authentication (MFA) either includes passwords, provides a passwordless user experience or is entirely passwordless.

1. **Password-based** solutions include a centrally stored credential that can be phished, stolen, or compromised and are therefore incredibly weak.

2. **Passwordless user experience** is a solution that removes the need of entering a password manually during the authentication process, but a centrally stored password still exists and used in every other area of the life cycle, such as initial set-up, new user on-boarding or remote access and recovery, to name just a few. In this instance there is still a password, held on a central database somewhere that is just waiting to be compromised.

3. **End- to-end passwordless** is a solution where no password is ever created or stored and is the most secure approach to authentication.

In this document when we refer to 'passwordless' we are talking about 'end-to-end passwordless' such as the AuthN by IDEE solution.

How Does Passwordless Authentication Work?

End-to-end passwordless (sometimes called true passwordless, or entirely passwordless) removes the need for shared secrets which can be phished. The authentication process is still based on possession and inherence, or possession and knowledge, but utilizes public key cryptography (public and private key pair) as follows:

1. **Possession** (something you have) and control of a private key locked in secure hardware on the device (cryptographic device) **AND**

2. Using **knowledge** (something you know - PIN) **OR**

3. Using **inherence** (something you are - biometric) to unlock the cryptographic device.

In the case of WebAuthn (W3C web authentication standard developed by the FIDO Alliance) the authentication flow looks like this:

1. User starts the log-in process & the request is sent to the server.

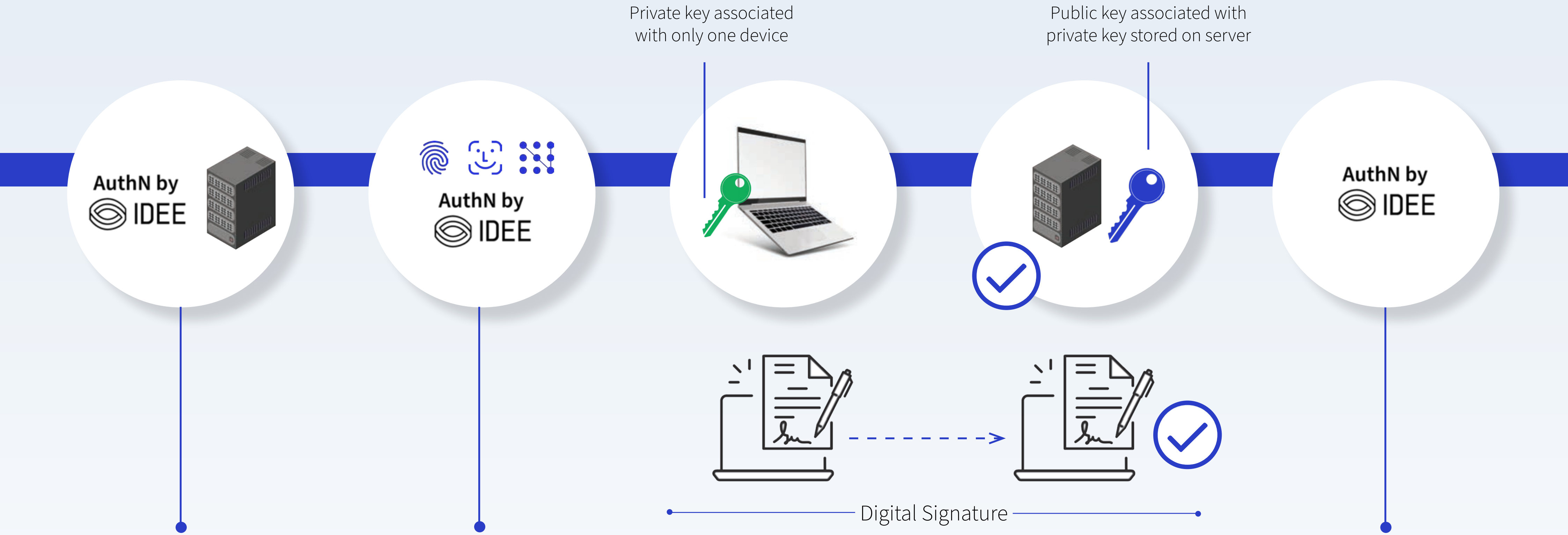
2. User is prompted to authenticate with biometrics or simply unlock their device.

3. After the device is unlocked, the private key signs the challenge and generates a response.

4. The server checks (verifies) the response with the public key of the user.

5. If the response is verified successfully, authentication is complete.

Web Authentication Standard.



Private key associated with only one device
Public key associated with private key stored on server
AuthN by IDEE
AuthN by IDEE
AuthN by IDEE
Digital Signature

1.

User starts the log-in process & the request is sent to the server.

2.

User is prompted to authenticate with biometrics or simply unlock their device.

3.

After the device is unlocked, the private key signs the challenge and generates a response.

4.

The server checks (verifies) the response with the public key of the user.

5.

If the response is verified successfully, authentication is complete.

The Benefits of Going Passwordless.

There are two main reasons why organizations should be looking (wherever possible) to implement passwordless, and these are **improved security and enhanced user experience.**

80%

Passwords are the root cause of over 80% of data breaches

$70

Average help desk labor costs for a single password reset

90

Users have more than 90 on line accounts

**Source: https://fidoalliance.org/what-is-fido/*

Improved Security

Passwords are fast becoming completely obsolete. They are the problem and have been for too long. Passwords are vulnerable to a plethora of high-impact security threats like phishing, brute-force attacks, and credential stuffing. Removing passwords from the authentication process eliminates the risk of password and credential-based attacks since there are no passwords to steal or compromise.

Prevent Credential Sharing

With passwordless authentication, users can't share passwords with others, preventing the risk of unauthorized access and sensitive business information disclosure.

Multifactor Authentication (MFA) Made Easier

Passwordless methods can seamlessly leverage other authentication factors like biometrics to create a strong MFA solution without relying on passwords.

Elimination of Password-related Issues

Users hate passwords and users forget passwords. Password reset requests lead to significant support overheads. Going passwordless can save significant costs with almost immediate payback. The average cost of one password reset is $70* including help desk staff and downtime. Even for small companies this can quickly become inviable, but for the enterprise this expense is one that is fast becoming intolerable.

Increased Productivity

Resetting passwords, not only costs businesses significantly in financial terms, but getting locked out of an account is a bottle neck in the workflow. Saying goodbye to passwords also means saying goodbye to productivity distractions and disturbances.

Better User Experience

Passwordless authentication methods are typically more user-friendly and convenient. Users can log in quickly using biometrics such as fingerprint, or facial recognition which greatly enhances the overall user experience. If biometrics is not possible, PIN is a viable option because it only works locally on that device; unlike passwords that can be used remotely.

✓ Reduced Friction

In an effort to “fix” the problems that arise from passwords, users are being asked to create ever longer and more complex passwords. Often the butt of jokes, asking users to create many unique combinations, with special characters and symbols is tiring and causes unnecessary friction during the login process. Passwordless authentication simplifies and accelerates the authentication flow, leading to higher user engagement and conversion rates.

✓ Compliance and Regulations

Some industries and regions have strict regulations on password security. Passwordless authentication can help meet these compliance requirements effectively.

So, what’s not to love?

Well, there are some challenges too - depending on your use case and what you are trying to achieve...

Challenges to Passwordless.

While passwordless authentication offers a huge range of benefits and may seem like an out-and-out no-brainer, it can also come with its own set of conditions.

Security, Not All Passwordless Solutions Are the Same

Some passwordless methods, like using email, Push, SMS, links, QR Codes or OTP are phishable. There shouldn't be a trade-off between going passwordless and your security. And there doesn't have to be. Understanding the difference between 1st generation MFA and phish-resistant or phish-proof MFA (which is also passwordless), is vital.

Email
Sign-in using a magic link or one time code (OTP) sent to the user's email.

Mobile
Sign-in by authenticating via a call, SMS, OTP, push, or QR-code from the users phone.

WebAuthn (FIDO2)
The user unlocks their device (the user device is the same as the cryptographic device) with either PIN or biometric to sign the challenge using the private key.

Least secure → *Most secure*

Device Dependence

Many passwordless methods rely on specific devices or technologies, such as biometric sensors, smartphones, or hardware tokens. This dependency can limit accessibility for users who don't have compatible devices or prefer not to use certain technologies.

In this case, organizations should look for solutions that provide same device authentication using the WebAuthn standard. In this instance, any device made after 2015 should be compatible.

Cost and Infrastructure

Implementing passwordless authentication may involve initial setup costs, especially if additional devices, additional software and/or hardware, or third-party services are required.

Organizations need to evaluate the complete costs before deciding on which passwordless method to adopt, including technology that can provide agent-less solutions (where no additional hardware or software is required).

Integration Challenge

Integrating passwordless authentication into existing systems and applications can feel daunting, especially if these systems were built around traditional password-based authentication.

This challenge can be overcome if existing systems support modern authentication standards such as SAML, OIDC, WS-FED. If not existing VPN, ZTNA, and reverse proxy solutions are good options. We will explore this in more detail below, but it may be possible to still achieve passwordless even with legacy systems.

Passwordless (And Security) Across the Whole Life-cycle

Without a password as a backup, account recovery can seem challenging. If a user loses access to their primary authentication device, alternative self-service or administrator assisted recovery mechanisms must be in place.

Leveraging Zero-Trust concepts such as transitive trust and identity proofing, allows for self-service while ensuring that the complete user identity life cycle is immune to phishing, provable and cannot be subverted by a privilege insider.

Best Practices.

Register Devices

To establish trust, the authentication device has to be established following strong identity proofing. This then becomes the root of trust for other authenticators.

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, and the user identity should be inseparable. As a result, an explicit transitive trust between the device, and the user identity have to be established via identity binding. This ensures that only the real user can access a service by authenticating with the trusted device and that an attacker cannot spoof and/or copy a user's identity.

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 carried out on a "trusted service" tied to a "trusted device" coupled to that "specific user" and authorized under the "user's total control". This should form the basis of enterprise zero trust security journey.

Get Account Recovery Right

Recovery is one of the most important aspects of getting passwordless authentication right and not undermining its benefits. To achieve a secure recovery, the real user must be the one that can access the recovered data. This can be 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 credential harvesting.

Use Secure Authenticated Channel

The authentication data should be sent via a secure authenticated channel. Ensure that the integrity and identity of the parties (Identity Provider and Relying Party) involved in the authentication process are established using a secure mutual authentication process. This ensures the confidentiality of the authentication data and that unauthorized parties cannot alter, manipulate or subvert the authentication process.

✓ Ensure Verifier Compromise Resistance

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

✓ Properly Authorize Additional Devices

Ensure that an unauthorized 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 is in total control when adding a new device. Hence, only the authorized user can add another device.

> **"OTPs and codes should be deprecated. They are no longer fit for purpose, just as passwords."**
>
> **Dennis Okpara, Chief Security Architect & DPO, IDEE GmbH**

IDEE

Section 2.

Passwordless

The Use Cases & Key Facts

Use Cases & Key Facts.

1. Passwordless with Remote Devices.

A strong passwordless solution is the most secure way of accessing remote systems. The traditional username and password have been the most exploited means by which cybercriminals have infiltrated organization's networks. The single biggest challenge is how to deploy passwordless authentication for remote systems. Here are some of the ways you can utilize passwordless authentication to protect remote systems.

1.1 Passwordless with Virtual Private Network

Virtual Private Network (VPN) ensures that an organization's internal business resource cannot be accessed via public network, but it doesn't eliminate the need for strong authentication. Even with VPN, your organization is still exposed to all sorts of credential-based attacks.

Here's how to go passwordless with VPN.

1. Choose a VPN solution that supports modern authentication such as SAML and OIDC.
2. Choose an (IdP) that offers support for modern authentication protocols.
3. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
4. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
5. Connect your VPN solution to the IdP via modern authentication protocols such as SAML and OIDC.
6. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication.
7. Your employees can then authenticate to your VPN via a federated IdP using passwordless authentication to access remote systems.

This approach offers enhanced security, convenience, and the best user experience.

Key Fact:
Supporting modern authentication methods is not enough. The authentication solution needs to be able to prevent all credential phishing and password-based attacks otherwise it's not worth the investment.

1.2 Passwordless with Zero Trust Network Access

The primary concept behind ZTNA is the principle of "never trust, always verify." It means that instead of assuming trust within the network, ZTNA ensures that every user and device attempting to access a resource is thoroughly authenticated and authorized, regardless of their location or device.

Here's how to go passwordless with ZTNA and eliminate all credential-based attacks:

1. Choose a ZTNA solution that can integrate with an IdP system to ensure that user identities are verified before granting access.
2. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
3. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
4. Integrate your ZTNA solution with the IdP system via modern authentication protocols such as SAML and OIDC.
5. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication.
6. Your employees can then authenticate to your ZTNA solution via an IdP using passwordless authentication to access remote systems in the cooperate network.

Key Fact:
ZTNA is particularly relevant in today's evolving threat landscape, where remote work and cloud-based services are more prevalent. Passwordless authentication offers an extra layer of security ensuring that user identities, which is the major tenant of ZTNA, cannot be compromised, stolen and/or sold by initial access brokers to cybercriminal gangs.

1.3 Passwordless with Remote Desktop Protocol

Remote Desktop Protocol (RDP) allows users to access a remote machine remotely. RDP relies on username and password for authentication. This makes it vulnerable to brute force and all sorts of password related attacks. Therefore, it is crucial to protect RDP with strong authentication to prevent unauthorized access to assets.

Here’s how to go passwordless with RDP to eliminate all credential-based attacks:

To use Azure AD authentication with Remote Desktop Protocol (RDP) for accessing Windows Virtual Machines (VMs) in Azure, you can follow these steps:

1. Choose an identity provider (IdP) that offers support for modern authentication protocols such as SAML and WS-FED
2. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
3. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
4. Federate your Azure AD tenant with the IdP system via modern authentication protocols such as SAML and WS-FED.
5. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication.
6. Enable Azure AD login for RDP on your virtual machines (VM) on your tenant.
7. Ensure that the users you want to grant access to the VM are assigned the necessary roles and permissions (Virtual Machine Contributor or Virtual Machine User).
8. Assigned users would be redirected to the IdP and authenticated using passwordless authentication to access the VM using RDP.

This approach offers enhanced security, prevents brute force attack and all password-based attacks on RDP.

Key Fact:

This eliminates the need for RDP credentials, which can be phished, stolen and/or sold in the dark web. Azure AD authentication for RDP only works for Windows VMs in Azure that meet the required OS version and have Azure AD authentication enabled.

2. Passwordless with Physical Devices.

Physical access to devices (computers) is usually done using a password and username, which makes unauthorized access inevitable.

Here's how to use passwordless authentication to protect employee devices.

1. Choose an identity provider (IdP) that offers support for modern authentication protocols (WS-FED).
2. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
3. Ensure that your employee devices are compatible with Windows Hello (WH) or Windows Hello for Business.
4. Federate your Azure AD tenant with the IdP system using WS-FED.
5. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication.
6. To access a company computer for the first time, employees would be redirected to the IdP and authenticated using passwordless authentication. After which the employee is required to setup WH.
7. Subsequently, the employees only need to use WH to access their computers.

Key Fact:
Employees never ever have to remember a password. This not only makes the security phish-proof but also makes the login experience seamless. This works with Azure AD only domains, hybrid domains (Azure AD plus on-prem AD), and on-prem AD only domains.

3. Passwordless with Cloud Services.

Digital identity is the holy grail of cloud security. Almost all cloud service breaches are caused by stolen and/or weak credentials. This demonstrates that the traditional username/password and conventional MFA are not fit-for-purpose.

Here's how to use passwordless authentication to protect your cloud services (AWS, Google, Oracle, Azure, and others)

1. Choose an identity provider (IdP) that offers support for modern authentication protocols such as SAML and OIDC.
2. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
3. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
4. Connect your cloud service to the IdP via modern authentication protocols such as SAML and OIDC.
5. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication and granting them the required permissions on the cloud service.
6. Your employees can then authenticate to the cloud service via an IdP using passwordless authentication.

This approach offers a seamless user experience and enhanced security where access credentials cannot be stolen, modified and/or subverted by cybercriminals.

Key Fact:

Supporting modern authentication methods is not enough. The authentication solution needs to be able to prevent all credential phishing and password-based attacks, otherwise, it's not worth the investment.

4. Passwordless with SaaS Applications.

Here's how to use passwordless authentication to protect your SaaS applications (such as Office 365, Salesforce, Atlassian, Workday, Bamboo HR, Zendesk and TeamViewer).

1. Establish a single source of truth for employees' identities (e.g., Azure AD, Google Workspace, Bamboo HR). Common source of employees' identities is AD and Azure AD.
2. Verify that your employee's directory (IAM) can integrate with your SaaS applications for federated/delegated authentication.
3. Federate your SaaS applications with your IAM system. This makes the IAM system responsible for authenticating your employees to the SaaS applications.
4. Choose an identity provider (IdP) that offers support for modern federated authentication protocols such as SAML and OIDC.
5. Ensure that the passwordless authentication method(s) offered by the IdP is phish-proof.
6. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
7. Federate your IAM with the IdP via modern authentication protocols such as SAML and OIDC. This makes the IdP responsible for authenticating your employees to the IAM system which in turn grants access to the SaaS applications.
8. Use SCIM to seamlessly provision your employees on the IdP system to enable them for passwordless authentication.
9. Your employees can then authenticate to the SaaS applications via the IdP using passwordless authentication.

This approach offers a seamless single sign on (SSO) user experience and enhanced security without duplication of credentials.

Key Fact:

Federated identity (SSO) is not enough. The authentication solution needs to be verifier impersonation and compromise resistant, prevent all credential phishing and password-based attacks, otherwise, it becomes a single point of failure should the IdP be compromised.

5. Passwordless with Web Application.

Over 74% of all breaches include the human element through error, privilege misuse, use of stolen credentials or social engineering.[1]. This is because web applications are exposed on the public Internet, anyone with the right credentials can access them.

Here's how to use passwordless authentication to protect web applications:

1. Determine the types of authentications supported by your web applications.
   a. If your web applications support modern authentication, then choose an identity provider (IdP) that offers support for modern authentication protocols such as SAML and OIDC.
   b. If your web applications don't support modern authentication use application proxy to ensure passwordless authentication is required before is granted to the applications
   c. If your web applications don't support modern authentication and you can't deploy application proxy, choose an IdP that offers custom API for strong passwordless authentication.
2. Ensure that the passwordless authentication method(s) offered by the chosen IdP is phish-proof.
3. Ensure that your employee devices are compatible with the passwordless authentication method(s) offered by the IdP.
4. Connect your web applications to the IdP using modern authentication protocols, application proxy or Custom API.
5. Provision your employees on the IdP system to enable them for passwordless authentication and granting them the required permissions to the web applications.
6. Your employees can then authenticate to the web applications via an IdP using passwordless authentication.

This approach prevents web application attacks caused by weak and phished credentials.

Key Fact:

Modern authentication protocols such as SAML and OIDC is the recommended approach for federated/delegated authentication. It makes it easy to deploy passwordless authentication without making changes to your applications.

[1] *Source: https://www.verizon.com/business/resources/reports/dbir/*

6. Passwordless with Mobile Application.

It's very important to protect unauthorized access to enterprise resources on mobile devices especially with the ever-increasing risks of BYOD.

Here's how to use passwordless authentication to protect mobile applications:

1. Determine the types of authentications supported by your mobile applications.
    a. If your mobile applications support modern authentication (e.g. via Webview), then choose an identity provider (IdP) that offers support for modern authentication protocols such as SAML and OIDC.
    b. If your mobile applications don't support modern authentication, choose an IdP that offers custom API and/or Mobile SDKs for strong passwordless authentication that you embed into your mobile applications.
2. Ensure that the passwordless authentication method(s) offered by the chosen IdP is phish-proof.
3. Ensure that your employee mobile devices are compatible with the passwordless authentication method(s) offered by the IdP.
4. Connect your mobile applications to the IdP either via modern authentication protocols or Custom API/SDK.
5. Provision your employees on the IdP system to enable them for passwordless authentication and granting them the required permissions to the mobile applications.
6. Your employees can then authenticate to the mobile applications via an IdP using passwordless authentication.

This approach prevents attacks caused by weak and phished credentials.

Key Fact:
Modern authentication protocols such as SAML and OIDC is the recommended approach for federated/delegated authentication. It makes it easy to deploy passwordless authentication without making changes to your applications. Alternatively, you can embed passwordless authentication directly into your mobile applications via SDK.

Passwordless Use Cases Summary.

Below we have summarized the use cases in a table for quick reference (in order) showing you how to achieve passwordless, which solutions are available to achieve the desired outcome & level of security, along with the benefits that can be achieved.

REMOTE DEVICES

Use Cases	How to Achieve Passwordless	Benefits	1st Generation MFA *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	Phishing Resistant MFA *(FIDO2 & WebAuthn)*	Phish-proof MFA *(AuthN by IDEE)*
Remote Devices e.g., Terminal servers, Virtual Machines and Remote Desktops	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Integrate your remote access solution with your IdP via modern authentication protocols (such as SAML, OIDC and WS-FED). • Authenticate your employees to your remote devices via the IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		Eliminates the cost of password management.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense/

Passwordless Use Cases Summary, cont...

PHYSICAL DEVICES

Use Cases	How to Achieve Passwordless	Benefits	1st Generation MFA *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	Phishing Resistant MFA *(FIDO2 & WebAuthn)*	Phish-proof MFA *(AuthN by IDEE)*
Physical Devices e.g., Windows 10 devices	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Ensure that your employees' devices are compatible with Windows Hello (WH) or Windows Hello for Business. • Federate your AD/Azure AD tenant with your IdP via WS-FED. • Authenticate your employees to their devices via the IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		Eliminates the cost of password management.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense/

Passwordless Use Cases Summary, cont...

CLOUD SERVICES

Use Case	How to Achieve Passwordless	Benefits	**1st Generation MFA** *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	**Phishing Resistant MFA** *(FIDO2 & WebAuthn)*	**Phish-proof MFA** *(AuthN by IDEE)*
Cloud Services e.g., AWS, Google, Oracle, and Microsoft Cloud Service Platforms	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Integrate your cloud service platform with your IdP via modern authentication protocols (such as SAML, OIDC and WS-FED). • Authenticate users to your cloud service platform via the IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense/

Passwordless Use Cases Summary, cont...

SaaS APPLICATIONS

Use Case	How to Achieve Passwordless	Benefits	1st Generation MFA *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	Phishing Resistant MFA *(FIDO2 & WebAuthn)*	Phish-proof MFA *(AuthN by IDEE)*
SaaS Applications e.g., Office 365, Salesforce, Atlassian, Workday, Bamboo HR, Gitlab and Zendesk	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Integrate your SaaS applications with your IdP via modern authentication protocols (such as SAML and OIDC). • Authenticate your employees to your enterprise SaaS applications via the IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense/

Passwordless Use Cases Summary, cont...

WEB APPLICATIONS

Use Case	How to Achieve Passwordless	Benefits	1st Generation MFA *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	Phishing Resistant MFA *(FIDO2 & WebAuthn)*	Phish-proof MFA *(AuthN by IDEE)*
Web Applications	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Integrate your Web applications with your IdP via: • Modern authentication protocols (such as SAML and OIDC) • Application proxy or • Custom API • Authenticate users to your Web applications via your IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Prevents up to 74%[2] of all web application attacks.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense
[2] Source: https://www.verizon.com/business/resources/reports/dbir/

Passwordless Use Cases Summary, cont…

MOBILE APPLICATIONS

Use Case	How to Achieve Passwordless	Benefits	**1st Generation MFA** *(phishable PUSH, QR Code, OTP/SMS/Email Link)*	**Phishing Resistant MFA** *(FIDO2 & WebAuthn)*	**Phish-proof MFA** *(AuthN by IDEE)*
Mobile Applications	• Choose an Identity Provider (IdP) that offers strong passwordless authentication. • Integrate your Mobile applications with your IdP via: • Modern authentication protocols (such as SAML and OIDC) • Custom API or SDK • Authenticate users to your Web applications via the IdP.	Prevents brute force attacks.	✓	✓	✓
		Prevents credential phishing.		✓	✓
		Prevents AiTM attacks.		✓	✓
		Prevents up to 90%[1] of all ransomware attacks.			✓
		Reduces the risk of BYOD.			✓
		Eliminates credential phishing & password-based attacks.			✓
		Eliminates account takeover.			✓
		Eliminates unauthorized access.			✓
		End-to-end passwordless (i.e., registration, authentication, adding device(s), recovery).			✓
		Truly passwordless (not a password manager).		✓	✓

[1] Source: https://riskandinsurance.com/sponsored-the-human-firewall-and-modern-defense/

Section 3.

Passwordless

AuthN by IDEE, The Difference

The IDEE Difference.

Prevent Account Takeover

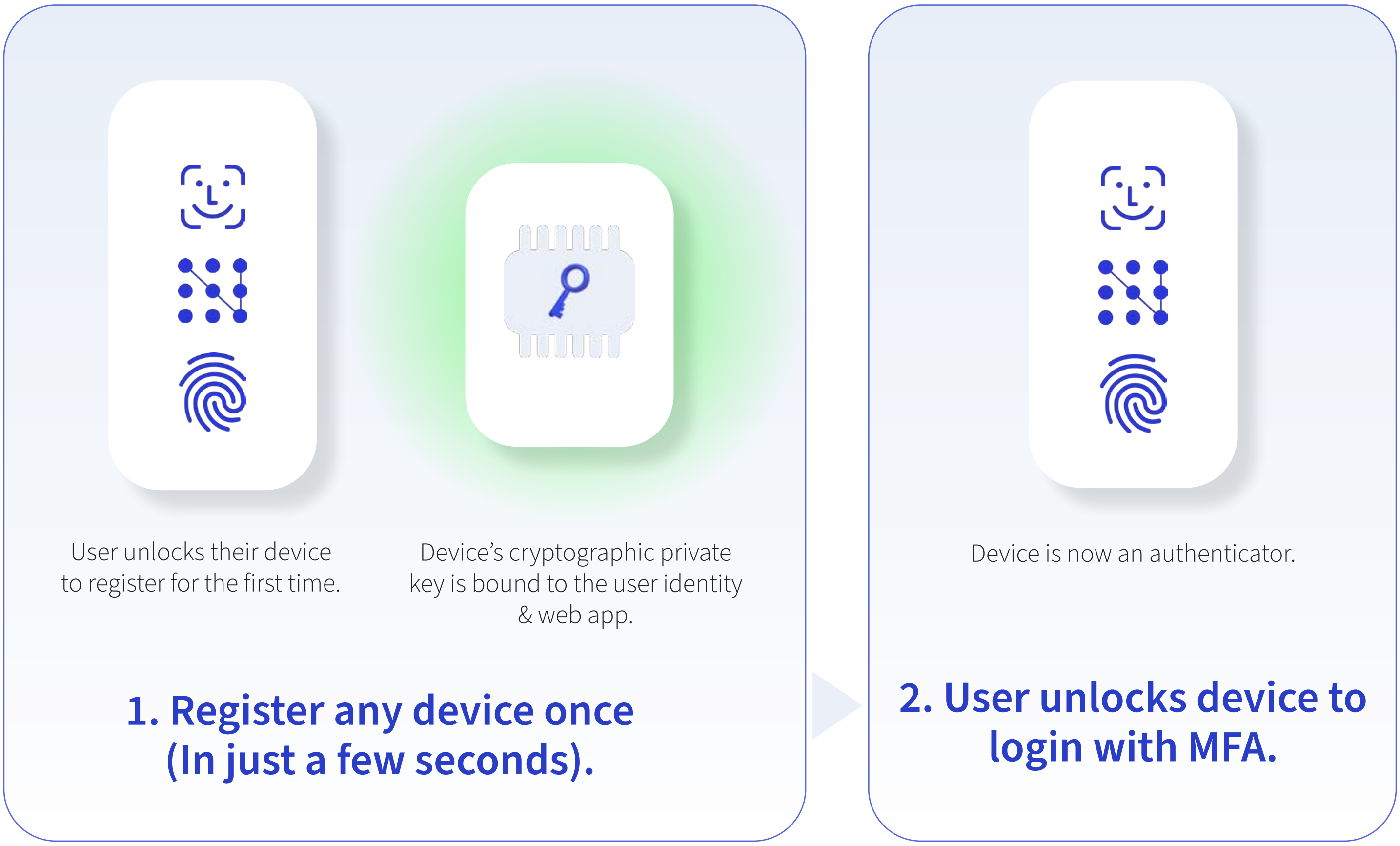
Ultimately the goal of any multifactor authentication solution, should be security-first - that is, to protect against account takeover.

AuthN by IDEE prevents all credential phishing and password-based attacks including Adversary in The Middle (AiTM) attacks. It is passwordless and agentless, which is why it can be deployed in just 15 minutes or less.

AuthN by IDEE:

Every registered device is an authenticator

How it works.



User unlocks their device to register for the first time.

Device's cryptographic private key is bound to the user identity & web app.

1. Register any device once (In just a few seconds).

Device is now an authenticator.

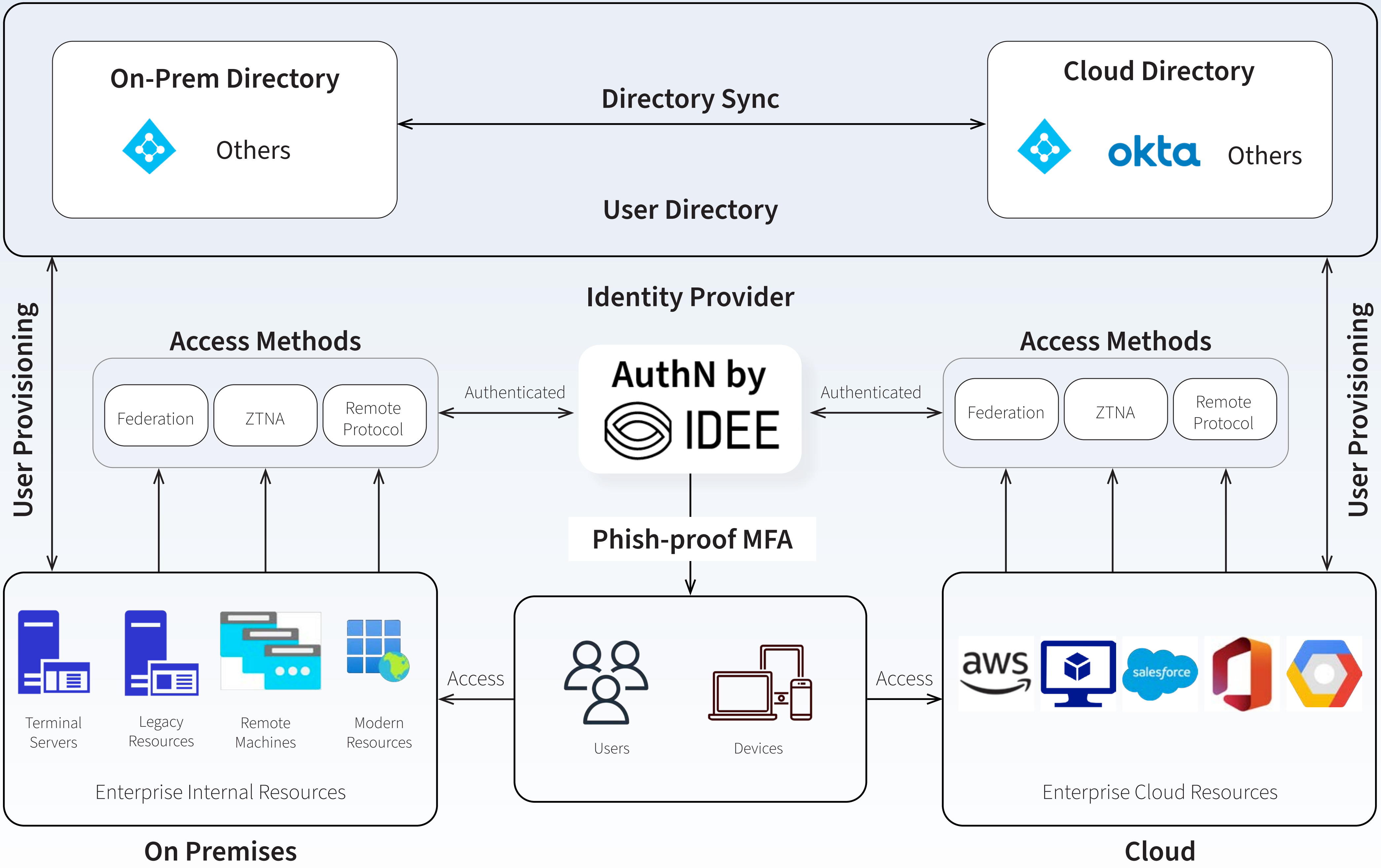
2. User unlocks device to login with MFA.

ZERO PASSWORDS. ZERO TRUST.

ZERO KNOWLEDGE. ZERO AGENTS. ZERO PII.

Just un-phishable MFA.

Passwordless architecture means you can finally eliminate all password-based threats.
And because AuthN is decentralized, we have no central credentials database - the single point of failure that hackers seek to exploit.



Compliant & Compatible.

✓ **NIST Compliant**

We are compliant with NIST's digital identity & authentication guidelines.

✓ **FIDO2 Compliant**

Expanding upon a FIDO2 compliant architecture, AuthN by IDEE is a strong zero-trust application of MFA.

✓ **PSD2 Compliant SCA**

Our MFA uses strong PSD2 compliant authentication.

✓ **Based on Proven Technology**

We leverage PKI, TPM/Secure Enclave, Blockchain and strong encryption.

✓ **Defense In-Depth**

One layer is not enough. We employ layered security for every action.

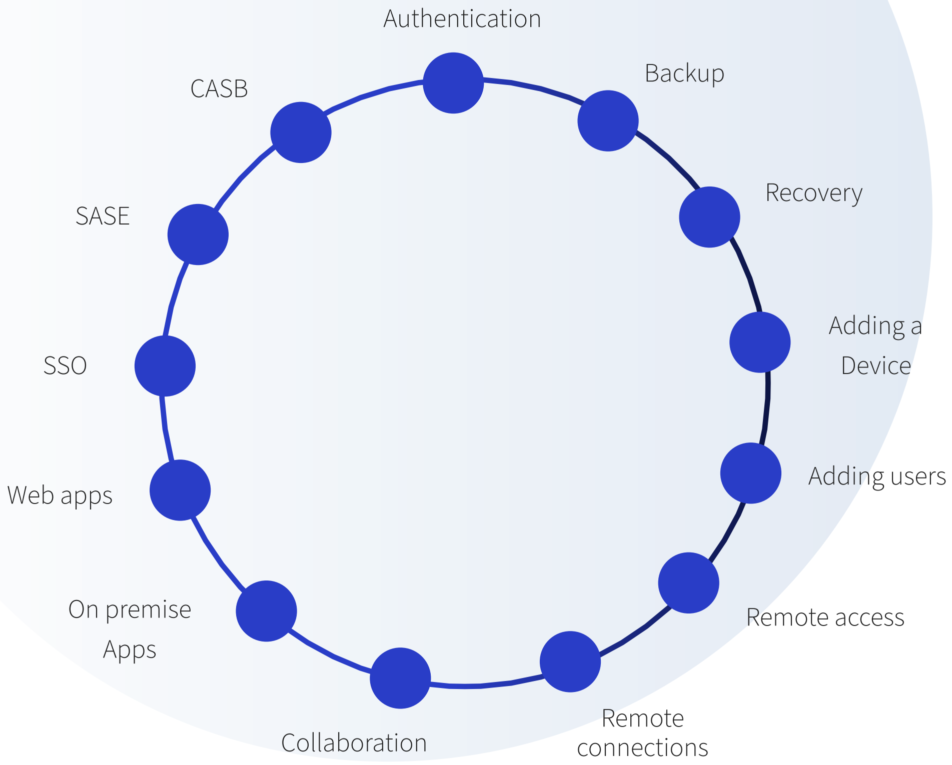
✓ **Decentralized Credentials**

Fully decentralized asymmetric keys stored inside the device security chip.

✓ **Strong Encryption**

AES-256-Bit & ECC-512.

End-to-end passwordless protection at every step of the life cycle, for every use case including remote access and legacy systems.



Users Love AuthN by IDEE.

AuthN by IDEE

✓ No Passwords

End-to-end passwordless.

✓ No Second Device

You don't need a second device, or any additional hardware such as USBs, fobs, keys, or anything else you might otherwise have to plug into your machine.

✓ No Push, QR, Text, OTPs

Never again will users have to perform multiple actions on more than one device to login to their systems. Remove friction and increase productivity.

✓ Simply Unlock Device

All that is required to authenticate, is for a user to unlock their device.

READ THE REVIEWS ON G2

Conclusion.

What you really want to know is, “Is Passwordless Right for Me?”

We think the answer is yes. Passwordless is right for almost every single organization and the barriers that do exist, can very easily be overcome with the right solution. Passwordless is not exclusively for the enterprise. Small and medium sized businesses and all types of use cases can utilize passwordless, just as MFA in general should be accessible to all.

We hope that we have provided a thorough and comprehensive overview of the benefits and we hope you agree with us: the world is better without passwords! It's definitely time to move on and embrace the capabilities of passwordless authentication!

To find out more about how we can help you on your passwordless journey, please get in touch.

Contact us for a demo.

sales@getidee.de

getidee.com