onewelcome
a Thales company

how to go passwordless

whitepaper

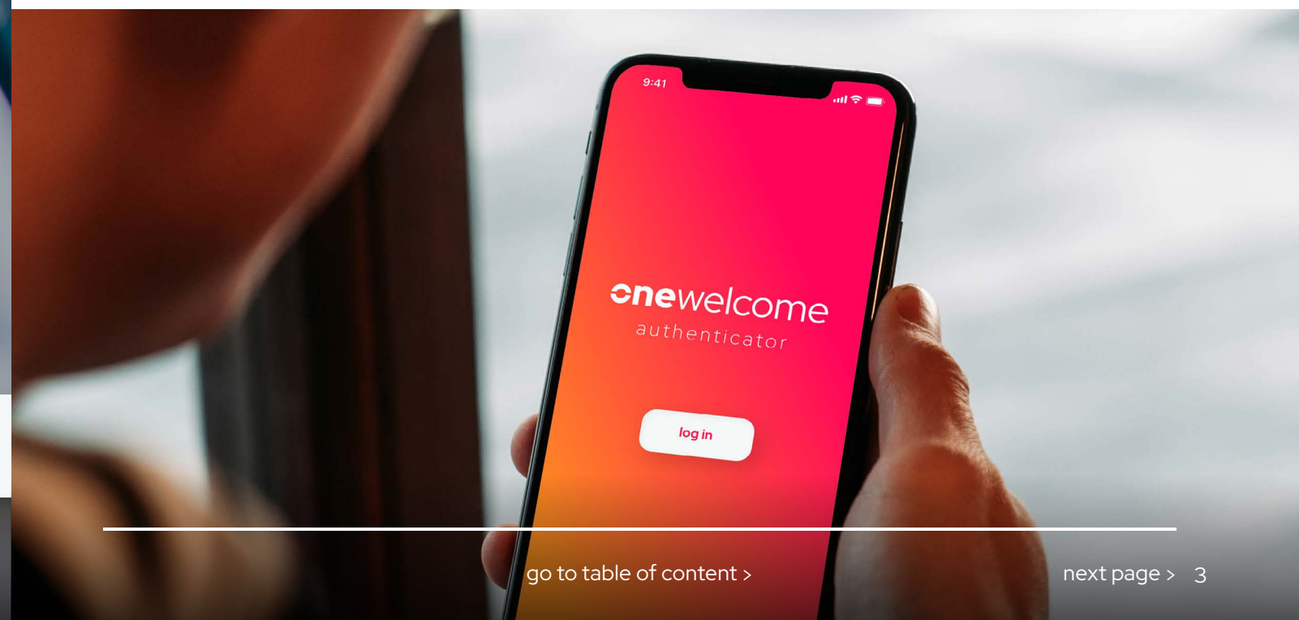
table of content

Note: This document is clickable.
Navigate through the document by clicking on the chapters, buttons and links.

introduction

Passwordless authentication has been a buzzword in the Identity & Access Management industry for a while now. This time it is not a technology push, but there is a clear business driver when it comes to your customer users; as an organisation you need to reduce any friction in the customer journey to be competitive. Many solution providers are taking steps towards creating a passwordless user experience but going completely passwordless can remain a challenge.

In this whitepaper we will cover the business drivers for going passwordless and the state of current Authentication solutions. In addition, we will share our view on the possibility of a completely passwordless world.



business drivers for passwordless authentication

1. Security: Passwords are the problem

Passwords have been used since the earliest days of computing, to control access to devices. Digitisation has changed the way companies operate their businesses and interact with their partners and customers, resulting in an explosive growth in online accounts, applications and portals to use. Nowadays passwords enable the right people to access the right information at the right time, in a secure and frictionless way.

Managing passwords and accessing accounts has gradually become easier for consumers, using everyday technologies like password managers, Apple Touch, Face ID and Apple Pay. For employees and business partners, technologies like mobile authenticator applications and fingerprint technology help provide a more secure, almost passwordless experience.

Human behaviour is one of the biggest risks in the approach of using passwords as the key, although even with good practice passwords can still be hacked by brute force.
But the more passwords a user needs to manage, the higher the vulnerability of the accounts being exposed to hackers and cyber criminals, because people tend to continue using weak passwords, or reuse passwords across different accounts.

- The average person has about 38.4 online accounts for work and private purposes (Source: SC Magazine UK), secured with a username password combination.
- According to the UK's National Cyber Security Centre (NCSC), 23 million account holders worldwide still use "123456" as their password.
- 90% of internet users are worried about getting their passwords hacked.
- 80% of hacking-related breaches are tied to passwords (Source: Verizon 2020 Data Breach Investigations Report).

Passwords are the problem

38.4	23.000.000	90%	80%
The average person has about 38.4 online accounts for work and private purposes (Source: SC Magazine UK), secured with a username password combination.	According to the UK's National Cyber Security Centre (NCSC), 23 million account holders worldwide still use "123456" as their password.	90% of internet users are worried about getting their passwords hacked	80% of hackingrelated breaches are tied to passwords (Source: Verizon 2020 Data Breach Investigations Report)

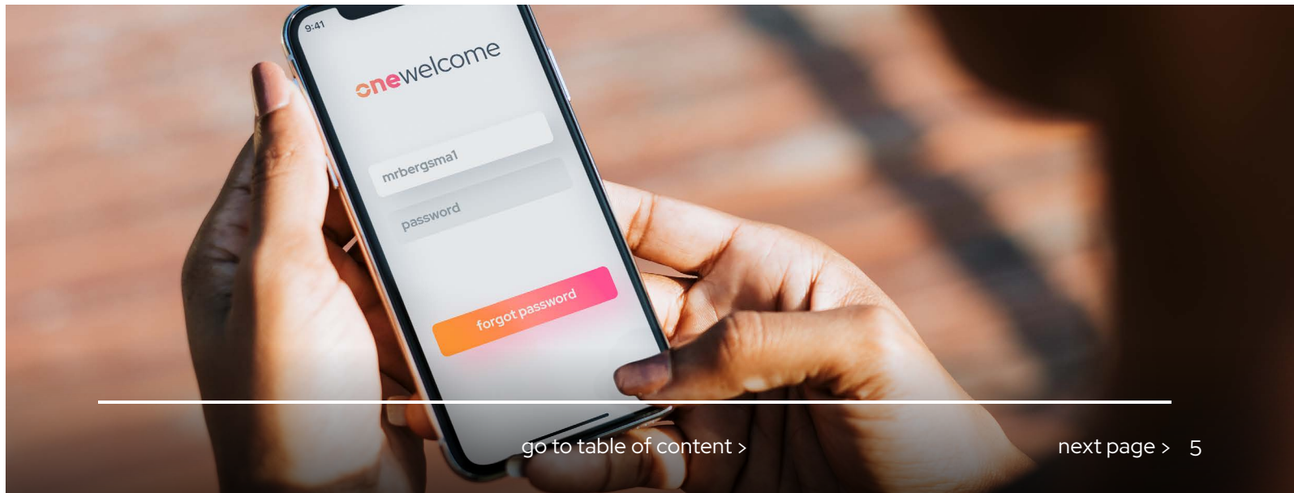
Password as means of authentication are not only a hassle for users but can also have a severe impact on organisations. Password resets can be a burden on IT organisations and support, not to mention the cost and reputational damage in case of a data breach. When Identity Management was still mainly focusing on employees getting access to their work applications, this could partially be covered by Single Sign-On solutions. But with IAM shifting towards CIAM, the impact on the user journey and on your business has become more vital. These numbers speak for themselves:

- 83% of mobile users say that a seamless experience across all devices is very important (Source: Root).
- 61% of users are unlikely to return to a site on mobile if they had trouble accessing it and 40% visit a competitor's site instead (Source: Google).
- About a third of online purchases are abandoned at checkout because consumers cannot remember their passwords (Source: MasterCard and the University of Oxford).
- In case of a breach, the costs are high. An IBM study calculated the amount of €150 for each record hacked. This includes lost business, legal fees, and compensation to affected clients.

2. A frictionless User Experience

Resetting passwords while trying to log in happens all the time, causing friction in the customer journey. Twentyone percent of users forget passwords after 2 weeks, and 25 percent forget one password at least once a day, according to a research by the Baymard institute, a Denmark-based . In a study analysing password behaviour in e-commerce, they also observed an 18.75% checkout abandonment rate among account users, all caused by a forgotten password, followed by "password reset email" issues.

Different surveys show that most people would prefer different login options, without passwords. According to Google, 75% of Americans are frustrated with passwords and would prefer other login options without passwords. The Ponemon Institute, specialised in independent information and privacy management research, reports that 55 percent of individuals and IT specialists would like to protect their accounts by a method that does not involve the use of passwords. In addition to strong security, users indicate to value ease of use.



multi-factor vs. passwordless authentication

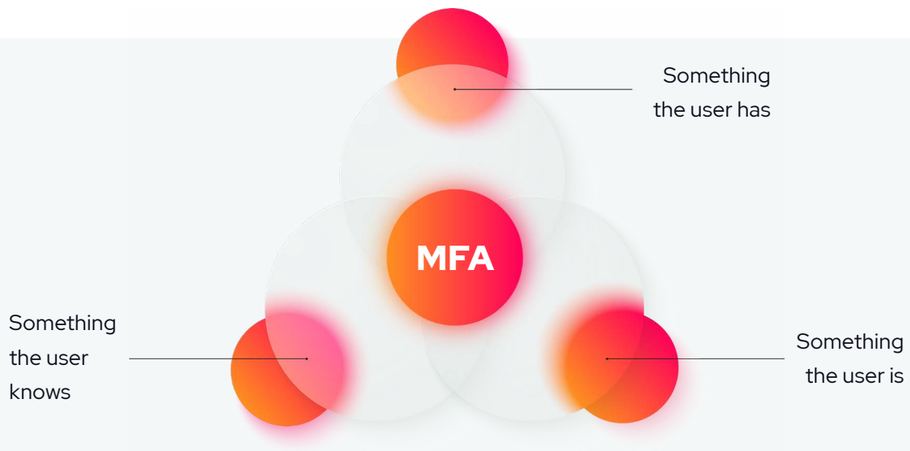
The adoption of Multi-Factor Authentication is growing, and in regulated industries such as financial services and insurance often mandatory. It makes online authentication more secure by adding extra steps to the authentication process. The three main factors used in Multi-Factor Authentication are:

1. Something the user knows (for example passwords);
2. Something the user has (a specific device);
3. Something the user is (biometrics).

Multi-Factor authentication options and the use of Identity providers (IDP's) can create the perception of Passwordless Authentication. In the Consumer Identity space there are two partial solutions – the integration of trusted IDP's (like social- or bank-id) or the password managers provided by Google and Apple.

If you have added a second factor (e.g. a push notification on mobile) to your account, you can sometimes stay logged in and only use your second factor as standard login option, creating a passwordless experience. However, in many cases accounts are initially still set up using a username and password combination and the password is still used as a fallback when you need to reset your account. And although an additional factor lowers the security risks, the vulnerability of username/password is still present, although less worrisome.

In a real Passwordless Authentication scenario, the username/password combination should be removed from the process and replaced by something else entirely. Technology is advancing, the world of biometrics has commoditised, so in fact the future holds many options to truly go passwordless.



usability and security: a balancing act

Passwordless authentication can be a balancing act between usability and security.
Many point solutions currently available in the market offer a passwordless user experience, but actually require the accounts to be activated with a username/password and the second factor functions as the 'passwordless' part. Of course, this is a major step forward, solving the usability issue. Customers do not have to go through the hassle of remembering and typing in their passwords anymore.

But it is also possible to go completely passwordless. The options are evolving, continuously improving security and user experience. However, going completely passwordless requires a different way of thinking. Sometimes organisations will need to re-evaluate their preferred customer journey scenarios, because usability prevails over security or the other way around.

An example to illustrate this: Looking at the three main factors in user Authentication, what if "something the user has" becomes the leading feature in an authentication process? What will happen in the case of damage or loss of the device that is used for authentication, especially if the key is not shared on a server, but stored on the device?

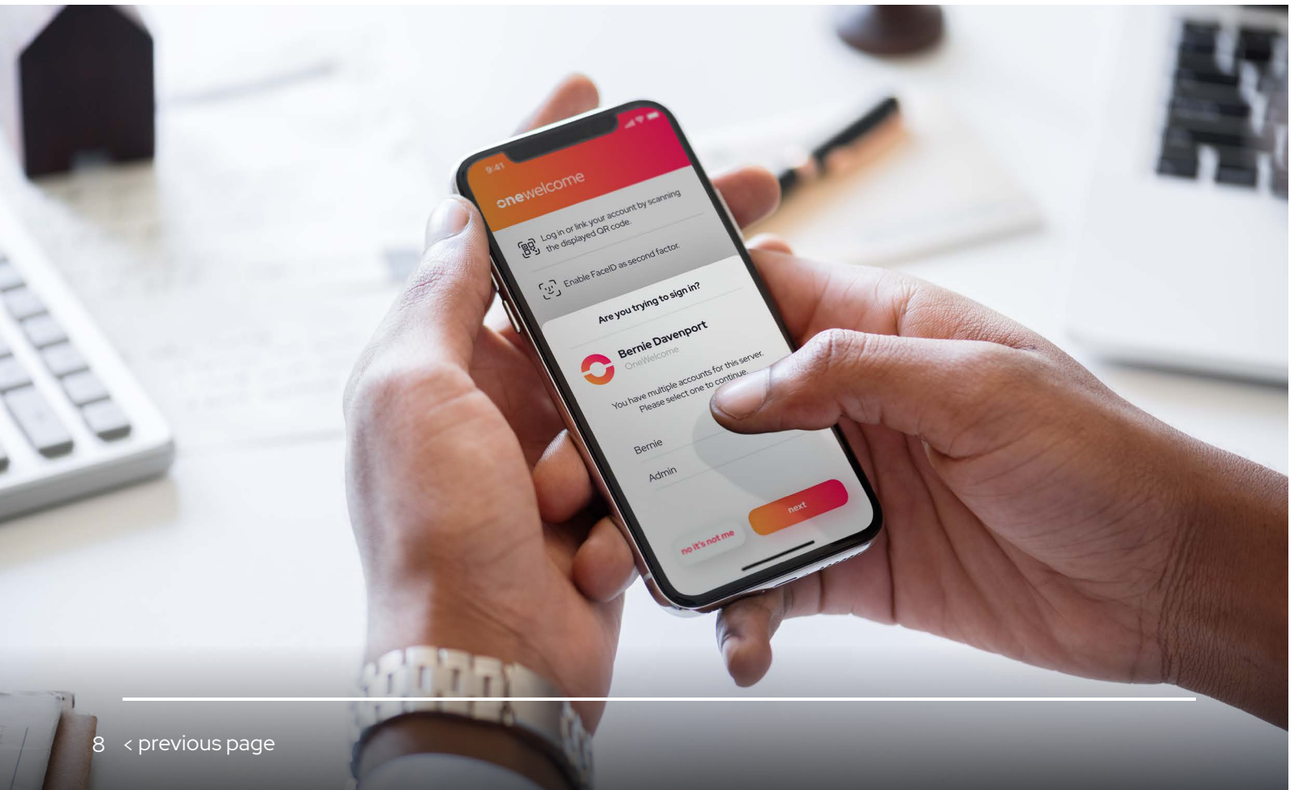
There are a few solutions, both with advantages on either the usability or the security side. You could opt to let users enrol multiple devices and as such, allow them to fall back to another enrolled device. If you want to stay more secure and not share keys across multiple devices, a resetting process could take place through Customer Care. A more secure option, because you do not share keys, but less customer friendly.

OneWelcome Mobile Identity (OMI)

OneWelcome Mobile Identity is a powerful set of features and technology to help organisations on their path to passwordless login and authentication. The solution can be embedded in your own mobile apps through a combination of a secure SDK and API calls, or it can be used as a standalone feature using the OneWelcome Authenticator app, which is available for both iOS and Android.
ww
OMI supports the following use cases depending on configured options, with a high flexibility to choose which of the use cases should be supported and how.

QR code authentication (using the OneWelcome Authenticator app)

One of the use cases that can be addressed with OneWelcome's Authenticator app is passwordless authentication using a QR code. After landing on the login page, the user can choose to log in with a mobile device, using a QR code. A quick scan, and the user is authenticated. To use this option, the user needs to have the OneWelcome Mobile authenticator downloaded to his device and the device needs to be linked to a valid OneWelcome account.



Authentication with push notification (using the OneWelcome Authenticator app)

OMI supports push notifications as a second factor of authentication, but this can also be set up as a passwordless scenario. After landing on the login page, the user can choose to log in with his username (for example an email address), without having to fill in a password. Instead, there are different options to configure the authentication flow. The push notification can be set up as a default second factor or users can choose from a menu with different second factor authentication options (such as a magic link or One Time Password through SMS), amongst which the push notification can be chosen. A push notification is sent to the user's device, and with a simple push and swipe the user is authenticated.

OMI integrated in your own mobile application

OneWelcome also offers a mobile SDK that supports 14 software languages. This means that you are flexible to integrate the highest level of authentication to your own existing apps, providing customers with a completely frictionless yet very secure digital user journey.
Using the mobile SDK will enable the following use cases:

- Protect an application from unauthorised access by requiring a PIN or Biometric key to unlock the application at start-up.
- Users can start a session in your mobile app and, if desired, the session ID can be exchanged for OAuth / OIDC Access and ID tokens for usage towards your backend applications and API's.
- Let users scan a QR code and authenticate your applications on a desktop.
- Receive and confirm push notifications as part of the MFA flow for users authenticating on another device.

Whether you chose to integrate authentication in your own mobile apps, or use a separate mobile authenticator to offer your customers the best and most secure experience, OneWelcome Mobile Identity helps you create a passwordless authentication process.

For more information, visit our website or contact us at info@onewelcome.com.

about OneWelcome

OneWelcome is Europe's #1 cloud Identity platform. We give organisations in finance and other selected industries the agility and speed to provide their consumers and business partners secure & seamless access across portals, apps and things. Trusted identities and easy access are the corner stone in any winning digital strategy; with OneWelcome's cloud service that's all being taken care off. Born and headquartered in Europe, OneWelcome provides features such as Flexible Onboarding, Identity Validation, Consent Management, GDPR support, MFA and Delegation. All of this provided via multi-branded-UI and API's, making OneWelcome one of the most flexible CIAM solutions on the market. Analysts like Gartner and KuppingerCole have been recognising OneWelcome as a worldwide Product Leader with "Excellence" ratings since 2014. On top of that, OneWelcome is the largest certified supplier for the Dutch government ID 'eHerkenning', notified under eIDAS.

OneWelcome at a glance

richest product
Richest CIAM & B2B IAM capability in the market, Customer Journey Management, Consent Management, B2B Delegation and Mobile Identity.

customer-centric
OneWelcome offers a multitude of service options to support customers with their digital identity operations.

certified & compliant
OneWelcome complies with all European standards and is ISO27001 and SOC 2 type 1 & 2 certified.

true European player
In-depth understanding of European identity challenges, like GDPR, eID's, Bring-Your-Own-Identity and Identity Proofing.

trusted
Trusted by more than 100 customers across Europe and the Dutch Government for its identity infrastructure.

the analysts confirm
Recognised by Gartner and KuppingerCole as 'Product Leader' and 'CIAM & B2B IAM specialist'.

onewelcome
a Thales company

+31 33 445 05 50
info@onewelcome.com
onewelcome.com

Soesterweg 310E | 3812 BH | Amersfoort | The Netherlands

< previous page

go to table of content >