BEYOND IDENTITY

Passwordless customer authentication – Reduce friction and increase security

WHITEPAPER | APRIL 2022

technology leaders club

The explosion of consumers transacting online and accelerated digital transformation has left companies trying to keep up with modern experiences, infrastructure and products to serve their digital users. But what has been the impact on consumers of moving digital?

Online security has failed to keep up with the speed of digital transformation, leaving challenges that need to be dealt with in order to provide a frictionless yet secure experience for users.

We hosted a roundtable that brought together of security architects, IT, network & security operations directors, process & innovation professionals to discuss:

- Whether password requirements stop consumers from creating accounts, therefore transactions
- Whether consumers forget or make too simple passwords, so they don't forget
- Consumer loyalty – are consumers more loyal to companies where they have accounts?
- How account issues affect consumer transactions
- Whether consumers favour products where they have an account over similar products

Rela8 Group's Technology Leaders Club roundtables are held under the Chatham House Rule. Names, organisations and some anecdotes have been withheld to protect privacy.

About Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in – eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication. Their invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements and improve the user experience and conversion rates.

Their revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device and continuously analyses hundreds of risk signals for risk-based authentication.

Passwordless maturity

Not all passwordless space is created equal. Some organisations could use a separate method of MFA like a one-time code delivered via SMS or email. These 'out of band' methods provide one way to solve the friction problem for consumers. Organisations need to understand what problem they are trying to solve with passwordless authentication, and this will differ depending on the industry and any regulation requirements.

The challenges of passwordless authentication

With most retail companies using ecommerce, they are trying to solve the problem of friction. They need to make it as easy as possible for their customers to make transactions, or they may lose the business. This is especially true where margins are tight, because even a small decrease in the conversion rate could have a big impact on the bottom line.

But this is not the scenario with fintech or health insurance services for example. Account takeover or fraud credential stuffing has a direct impact on the business because the customer base loses trust in their ability to store personal data. Plus there may be fines and regulation breaches. So the problem they are trying to solve is data and customer security. Passwords are a shared secret and confidence in a shared secret is not as high as a hardware token, asymmetric cryptography or Fido based protocols.

Some companies are trying to move towards a risk-based authentication which may identify higher risk authentications, such as geographical or time-based logins. They may ask for a biometric verification if unusual behaviour is identified. Sophisticated organisations try to keep the authentication frictionless by default, but they can add other levels if needed to help their customers and preserve the integrity of the transaction.

The pitfalls of going passwordless

While there are so many benefits to passwordless, the one drawback is that single point of failure and how it can be overcome. Although some applications are technically passwordless, there is still a password hidden somewhere within. MFA that uses SMS push notification and one time pass codes are still phishable, so the concern is not just around the password itself but about how systems can be protected.

A second problem with going passwordless, is in the understanding of customers. Usernames and passwords have been around for a long time, and consumers tend to trust the security they offer. They feel more in control. Organisations therefore need to carefully consider the problem they are trying to solve in going passwordless, and whether it is the right solution.

In Finland, one solution has been to create a strong citizen identity, so if consumers want to look into their tax or social security portal, they use their bank credentials for authentication. This means that the organisation you are logging into does not need to know you, and you don't need to create a username and password. Although this system also has drawbacks and whilst used on government and health site, it is not used on ecommerce sites.

> “The concern is not just around the password itself but about how systems can be protected”

Passwordless solutions

The burden for going passwordless needs to be shifted from users to technology. A machine can use private keys verified through certificates to access to other machines with certificates through a chain of trust protocol. Thousands of transactions daily take place through this so if the complexity of certificate management can be solved a similar schema could be deployed for removing the password from use.

The trusted platform module (TPM), and the biometrics local to modern devices along with the fundamental immovability of a private key that is generated and can never leave the hardware enclave, provides usability for the consumer as well as security benefits. It moves organisations away from relying on passwords, because recovery can be a device extension, a re-enrolment, or even another identity proofing flow, if really high trust is needed at recovery and registration.

Giving users flexibility of choice may make them feel more empowered in their digital security and identity. Going passwordless may be something that is not deployed 100% across all users because changing behaviour is not easy, and some customers may prefer a social login or a one-use code, while others may not. They may need help to migrate to a different model of authentication. Giving customers a choice and understanding what problem the business is trying to solve make a good starting point.

Weighing up the options

There is no one solution to going passwordless. The authentication landscape varies greatly between industry and individual businesses, with many financial/insurance companies having to meet statutory regulations. Organisations should map out their options and consider the backend data to make sure they understand the problem they are trying to solve, whether this is a reduction in friction for their customers, or greater security around the storage of personal data.

Passwordless authentication is not without its problems. A single point of failure and push notifications that are not resistant to phishing can provide access to hackers. Consumers can be distrustful of security that does not need a username and password, but customer empowerment through choice and a good security posture can give companies a competitive advantage.

Therefore, in going passwordless, organisations should concentrate on moving the burden away from their customers and using available technology within modern devices. TPMs coupled with biometrics and the private key within the enclave can offer both security and usability benefits, along with a reduction in friction for consumers.

> “The burden for going passwordless needs to be shifted from users to technology”

Rela8 Group serves the technology leaders community by giving executives a platform to identify challenges, connect with key innovators and understand where their business is going next. Based on these three pillars, we create engaging and stimulating B2B programs as well as custom gatherings for senior leaders and solution providers.

technology **leaders club**

rela8
group