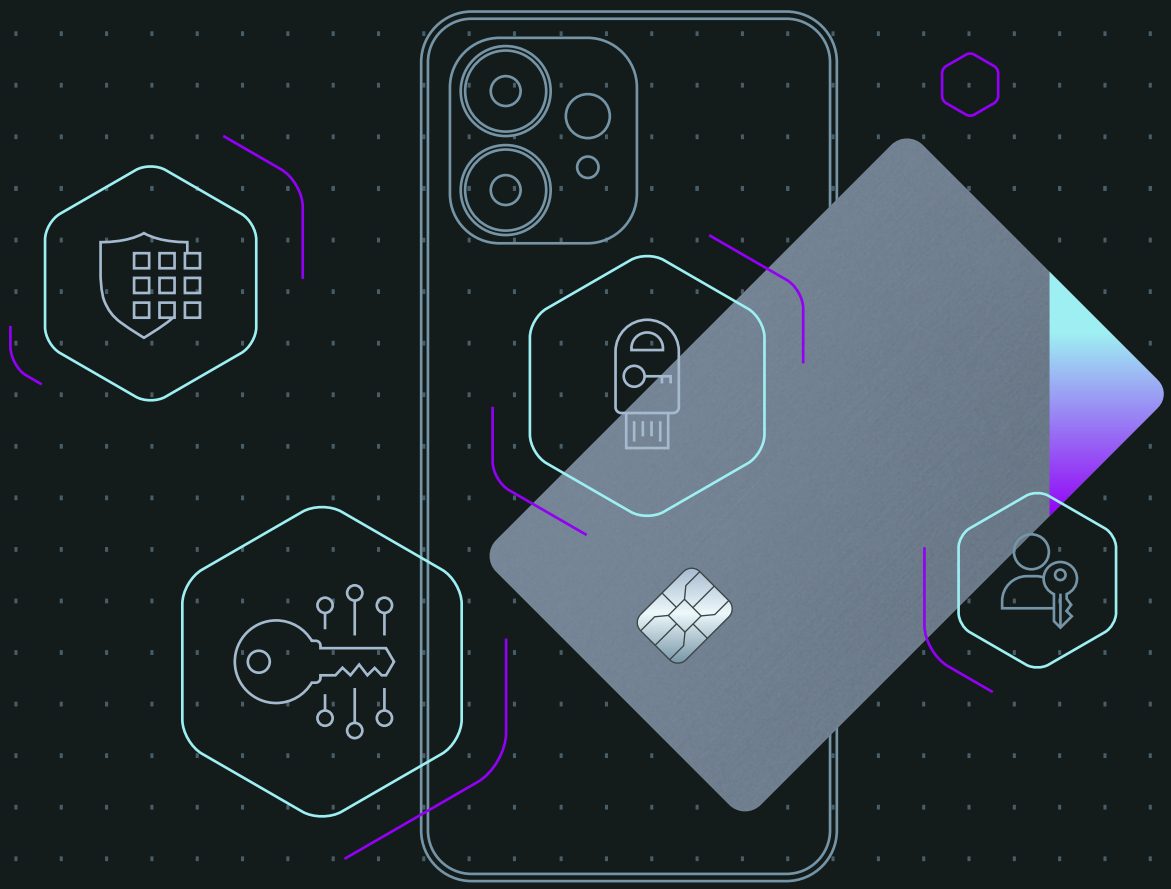
ARCULUS



WHITE PAPER

Passkeys: The Future of Authentication

The Future of Authentication

Weak passwords are the root cause of over 80% of data breaches.*

Over reliance on this outdated approach requires companies and customers to adopt enhanced security methods – such as passkeys – to protect their data and financial transactions by authenticating users.

* FIDO Alliance

Key Findings

Security Problems from Reused Passwords

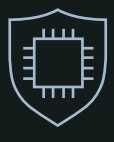
The FIDO Alliance estimates over 50% of all passwords are reused. This has caused the need for businesses to embrace a passwordless future, with data from Verizon's 2025 Data Breach Report (DBIR) revealing that only 3% of passwords meet NIST complexity requirements for password best practices.

Passkeys Are Easier and Faster

Passkeys have been found to be substantially easier and faster for users to authenticate and login to access accounts, with 69% having already enabled passkeys on one or more accounts.

The Majority of Data Breaches Involve A Human Element

The 2024 Verizon DBIR survey showed that 68% of all data breaches involve some type of "human element," including stolen or compromised credentials.

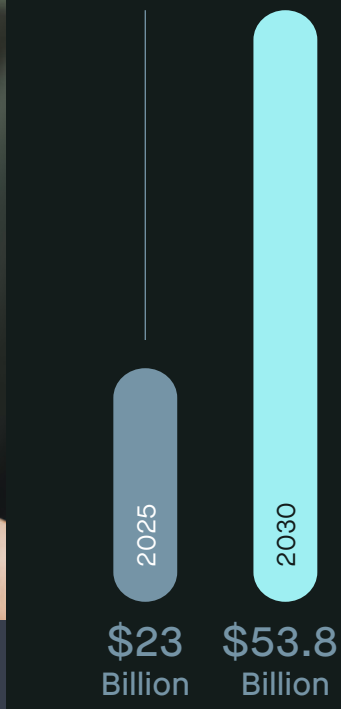


Hardware-Based Solutions Offer More Security

As passkeys become more widely adopted, hardware-based solutions offer even more robust security to protect users' identity, privacy, data and financial transactions.

INTRODUCTION

For Better Security, Look Beyond Passwords



Over the years, passwords formed a crucial part of the security equation but as hackers have become more advanced, passwords have proven to be an often-exploited weakness.

With the rise in cybercrime, weak passwords are becoming an increasingly significant liability for companies. Much of this illegal activity is driven by compromised or stolen credentials. The Verizon 2025 Data Breach Report showed that only 3% of passwords meet NIST complexity requirements for password best practices.

Additionally, the pain and inconvenience for customers who are hacked is enormous. Juniper Research revealed that the fraud cost to financial institutions is expected to rise from $23 billion in 2025 to $58.3 billion in 2030.

With monetary losses mounting and complaints continuing to rise, companies and their customers must utilize more comprehensive security measures to provide additional protection for data and authentication. One solution to these issues has been an increasing reliance on two-factor and multi-factor authentication (MFA) methods to help shore up defenses.

While an improvement to passwords, MFA has drawbacks as cybercriminals have deployed social engineering, AI tools and other techniques to bypass these protections. Additionally, many of the MFA methods in use today create a difficult user experience and are still not secure enough to stay ahead of hackers.

Put simply, passwords cannot be fixed. They are inherently weak and unable to sufficiently protect customer accounts and data. They are the cause of many frustrations; the challenge of creating a 'strong' password that fits with the requirements and the time-consuming reset process adds friction to user experience. Businesses need to move away from these legacy authentication methods to increase security, and at the same time, enhance the customer experience.

Enter Passkeys

Passkeys offer a better approach to identity and authentication, championed by the FIDO Alliance along with its partners. Formed in 2012 as an open industry association, the FIDO Alliance's mission is to reduce the world's reliance on passwords and improve online authentication security. Their partners include Apple, Google, and Microsoft — all of whom have deployed passkeys at scale across their platforms. Unlike MFA, which adds a layer on top of passwords, passkeys replace them entirely.

Passkeys aren't a security upgrade anymore — they're the new baseline.

Eliminate the need for passwords

Passkeys help to authenticate through the use of public and private keys that connect users to their devices, allowing them to safely access their data and accounts.

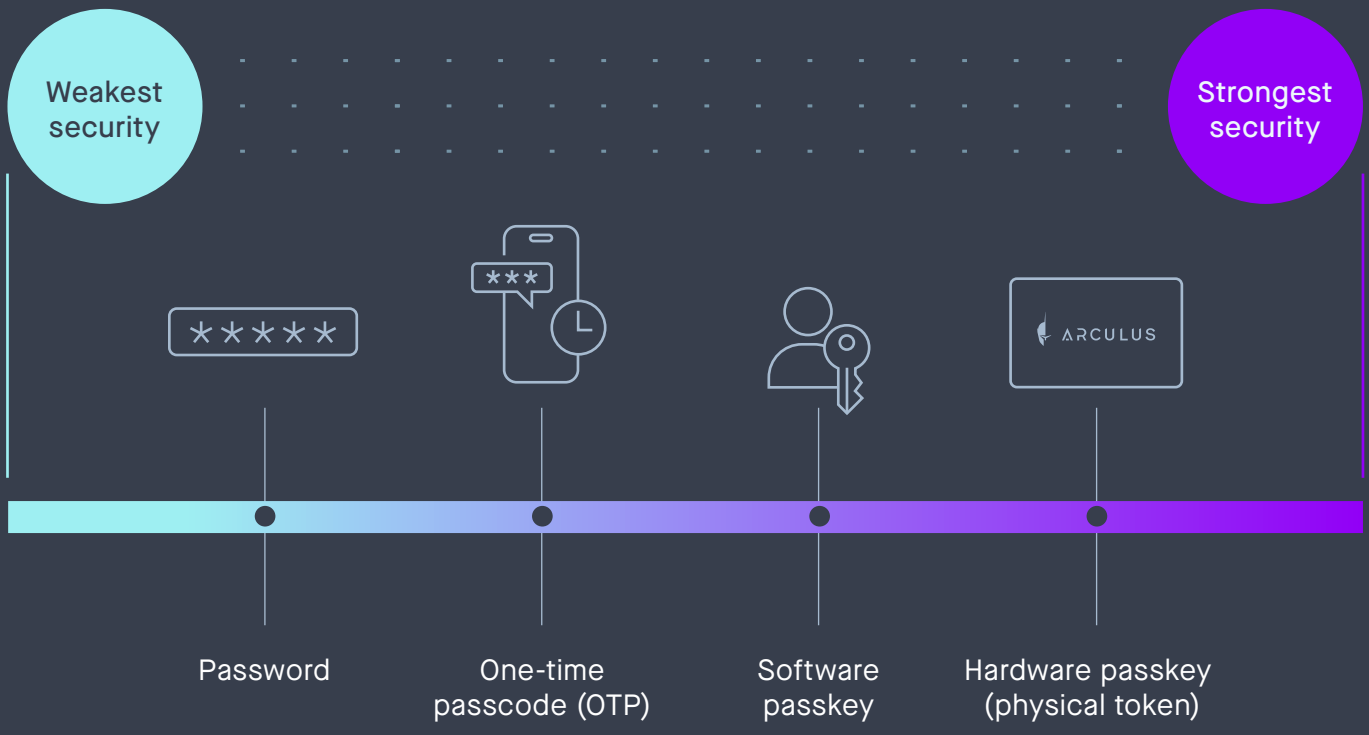
Combine with other security methods, such as biometrics

Multifactor authentication provides users additional protection and peace of mind.

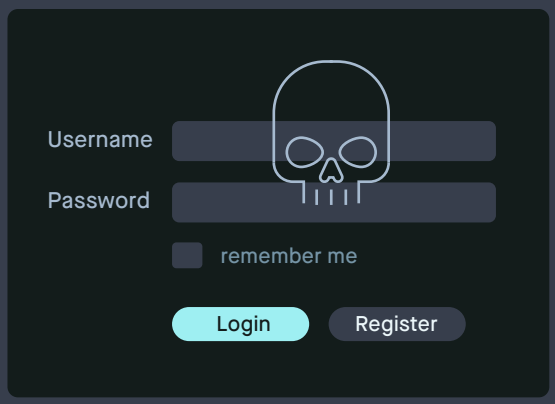
Frictionless, safe and secure access

Passkeys offer companies and their customers a frictionless experience that allows for safe and secure access to their data. This is especially relevant to financial services and banking where proving identity is crucial.

Passkeys Offer A More Secure and Convenient Way Forward



For years, passwords have failed to keep up with evolving attacks and techniques deployed by cybercriminals.



In 2025, the largest-ever data leak exposed more than 16 billion login credentials from major platforms like Google, Facebook, Apple, and even government services. Concerningly, this is only becoming more common, with a study by Juniper Research predicting a 153% surge in fraud by 2030.

Passkeys are engineered to make stolen credentials worthless. During the login process, the service verifies a cryptographic signature using a stored public key. If the signature is valid, authentication is complete.

The private key never leaves the user's device. Only that key can complete authentication with the corresponding public key — meaning even if an attacker intercepts the exchange, there is nothing to steal.

In general, FIDO2-supported passkeys come in two main forms:

Software Passkeys

The private key is generated by software and stored on the user's device or synced to the cloud. Tied to a phone, computer, or password manager, these passkeys can be backed up and transferred across devices. But what makes them convenient also presents a attack vector for hackers – software passkeys are a vast improvement over passwords, but not as strong as hardware passkeys.

Hardware Passkeys

The private key is generated inside dedicated hardware and never leaves it — not syncable, not extractable, never exposed online. Specifically engineered for security, the key cannot be phished, cloned, or remotely compromised. What's in the hardware, stays in the hardware.

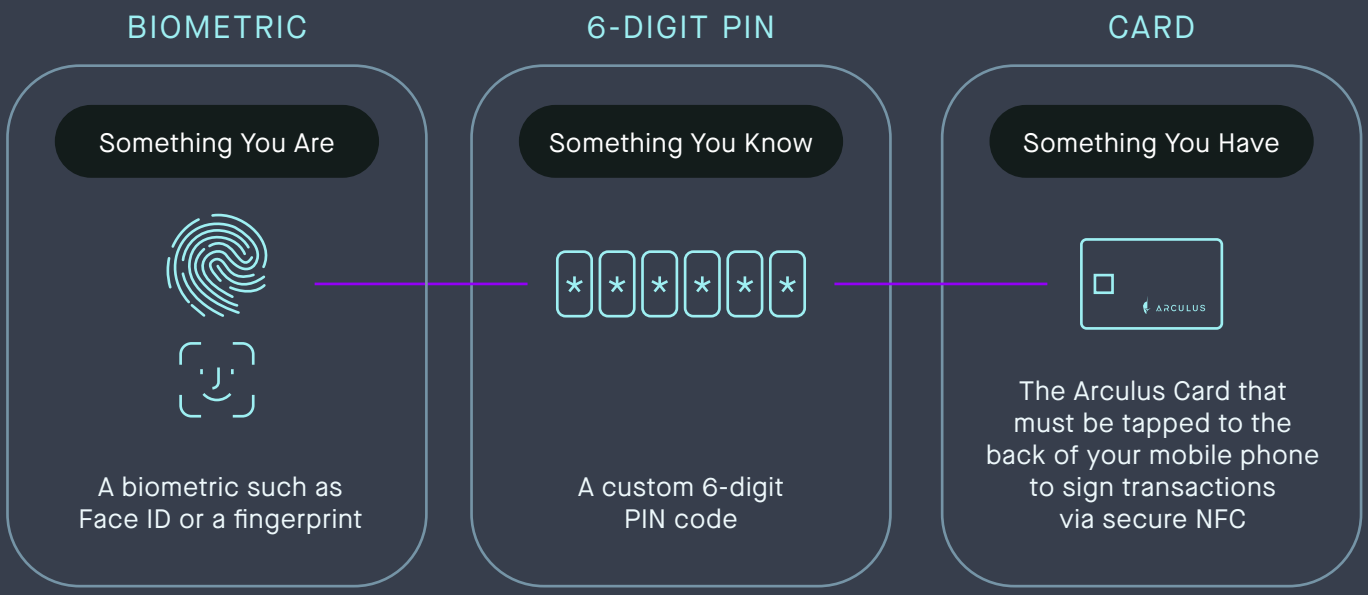
While the FIDO2 standards have existed for about a decade, the standard received a boost as Apple and Google began offering the security technology, branded as passkeys, to their users through iPhones and Android-based devices, according to an article published in the Wall Street Journal.

Another aspect that makes passkeys an increasingly attractive option for security is the fact that the technology can be combined with multifactor authentication methods, such as biometrics, to ensure greater levels of protection for personally identifiable information (PII) and financial data.

The sole use of biometrics for authentication has limitations, leaving it vulnerable to cybercriminals. Stolen biometric data is also a concern, however, incorporating this authentication method with passkeys adds yet another layer of protection.

> It's the combination of authentication factors that provides the strongest protection — something you have, something you know, and something you are. For example, a card, a PIN, and biometrics, working together with passkeys, deliver a level of security that no single factor can match."
>
> Tom D'Eletto, Head of Product, Arculus

Multifactor authentication with Arculus



As passkeys gain momentum, the next step is bringing these standards to an even higher level of protection. Google and Apple have made meaningful progress with their implementations, though synced passkeys do come with tradeoffs — tying security to a Google or Apple ID means the passkey is only as safe as that account. And because these passkeys sync across your profile, losing access to that account means losing access to your keys.

There is an increasing desire to remove friction from the user experience, especially in financial services. By employing FIDO technology, businesses can offer their customers a secure way to authenticate themselves. Historically, offering highest level of security without compromising user experience has provided a challenge to businesses. Now, with Arculus, individuals can simply tap their card to their smartphones to authenticate themselves and their transactions.

> With Arculus, your payment card can be used in the authentication process. Customers do not need to purchase an additional hardware device, like a USB security key. At the technical level, the card acts as a cryptographic key that works across multiple standards. You can just use your bank card to log into your bank the same way you use it at an ATM — it's a matter of taking what FIDO has proven works and improving the experience so it can be implemented at mass scale."
>
> Tom D'Eletto, Head of Product, Arculus

> Through the implementation of these standards, consumers can log in using private keys — cryptographic credentials that only they control and that never leave their device. As we see more services and companies move in that direction, it becomes a good thing for security and for passkey adoption."
>
> Tom D'Eletto, Head of Product, Arculus

The powerful combination of secure Arculus technology and premium metal cards offer three distinct advantages:

- The combination of security, convenience, and a premium form factor is what sets Arculus apart. With Arculus Authenticate™, customers seamlessly log into their financial institution's app with a simple tap of their metal card to their smartphone, paired with a PIN or biometric.
- Customers do not need to buy additional devices (such as USB dongles) to benefit from the increased security of hardware keys. The premium metal card becomes their hardware security device with Arculus Authenticate.
- Businesses can drive customer engagement and brand loyalty through the metal payment card form factor and interactions with Arculus Authenticate technology. All these advances allow companies and their customers to transition to a passwordless world — and for businesses that move early, the opportunity to lead on both security and customer experience has never been greater.

Conclusion

Passwords Are Weak

Statistics show that weak passwords are the root cause of 80% of data breaches, and over 50% of all passwords are reused. This continues to fuel cybercrime and identity theft, with one report finding over 550 million stolen passwords posted to the dark web since 2017.

Passkeys Pave a Way Forward

With the backing of the FIDO Alliance and the adoption of the FIDO2 standards, passkey use and acceptance have gained momentum.

Hardware Passkeys of the Future

For those seeking even stronger security, hardware passkeys will become the norm. Arculus technology allows customers to tap their hardware passkeys via a payment card form factor to their smartphones. Arculus Authenticate integrates passkey technology into premium metal cards, allowing businesses to offer a frictionless experience to their customers while providing the highest level of security.

Reach out to us at b2b@arculus.co to schedule a demo and to learn more about how Arculus Authenticate can work for your business.

Arculus is a trusted leader in passwordless security, developed by CompoSecure–the world's leading producer of premium metal payment cards. Our fully customized security solutions are user-friendly and secure.

The Benefits of Arculus Business Solutions

Improved Security

By eliminating the need for complicated passwords and enabling one-tap signatures, the Arculus Business Solution, Arculus Authenticate, reduces the risk of unauthorized access and ensures the security of transactions.

Enhanced User Experience

Arculus Authenticate is easy-to-use and convenient, providing customers and employees with a streamlined log-in and transaction experience. This can improve user satisfaction and loyalty.

Customizable Solution

Businesses can customize Arculus Business Solutions to meet their unique needs, allowing for greater flexibility and adaptability.

Reputation & Trust-Building

By enhancing security and improving the customer experience, businesses can build customer trust and strengthen their brand reputation.

Tap-to-Transact Protection

The ability to sign transactions easily through a simple tap to a smartphone provides a fast and convenient way to authenticate transactions.

Secure Cryptographic Signing

Arculus Business Solutions offers the most up-to-date cryptographic signing via FIDO2, ensuring the highest level of security.

Cost Savings

By preventing credential-based fraud and reducing password recovery support requests, Arculus Business Solutions delivers significant cost savings. With fraud costs projected to reach $58.3 billion by 2030, the financial case for hardware-backed passkeys is clear.