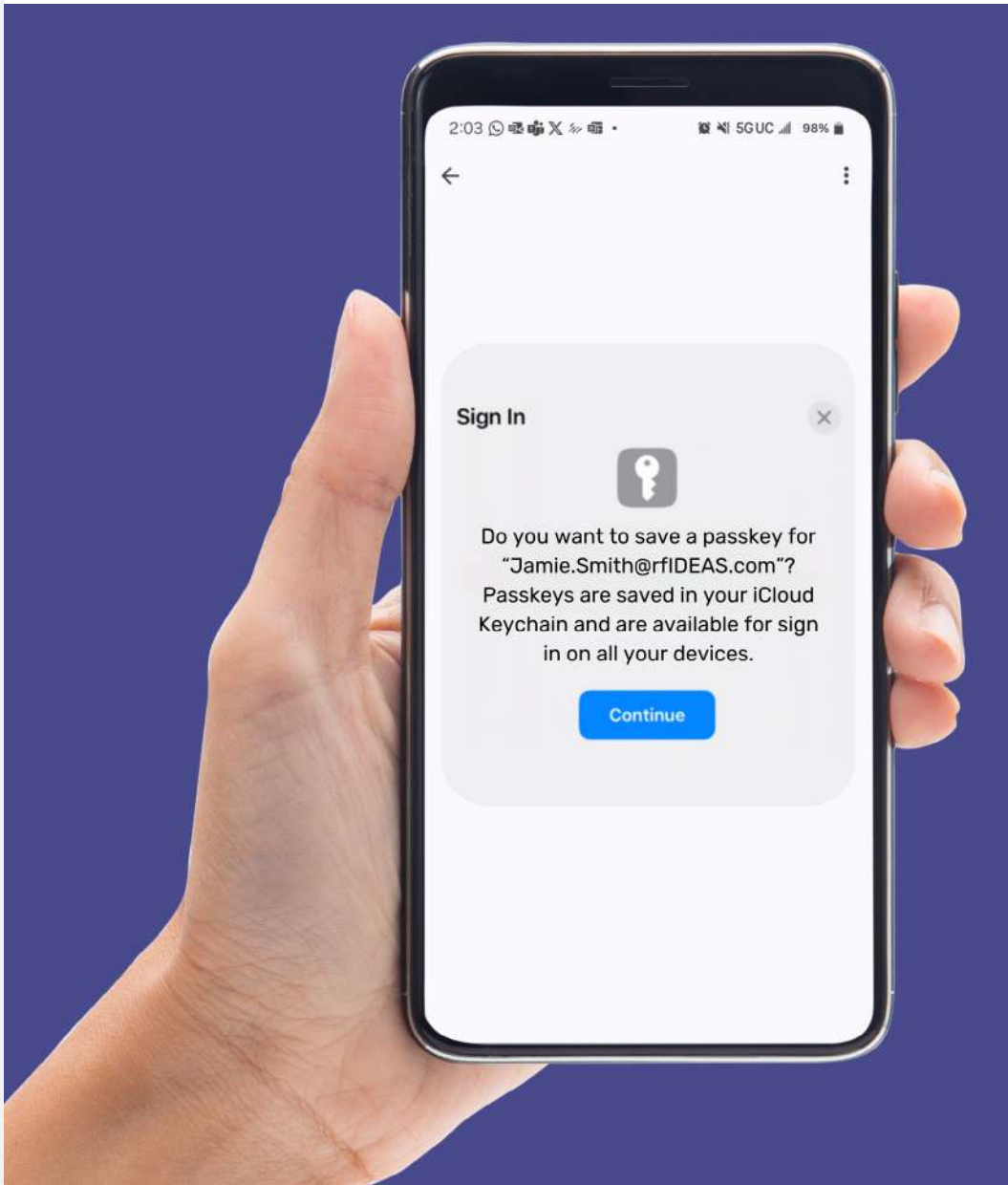
rf IDEAS

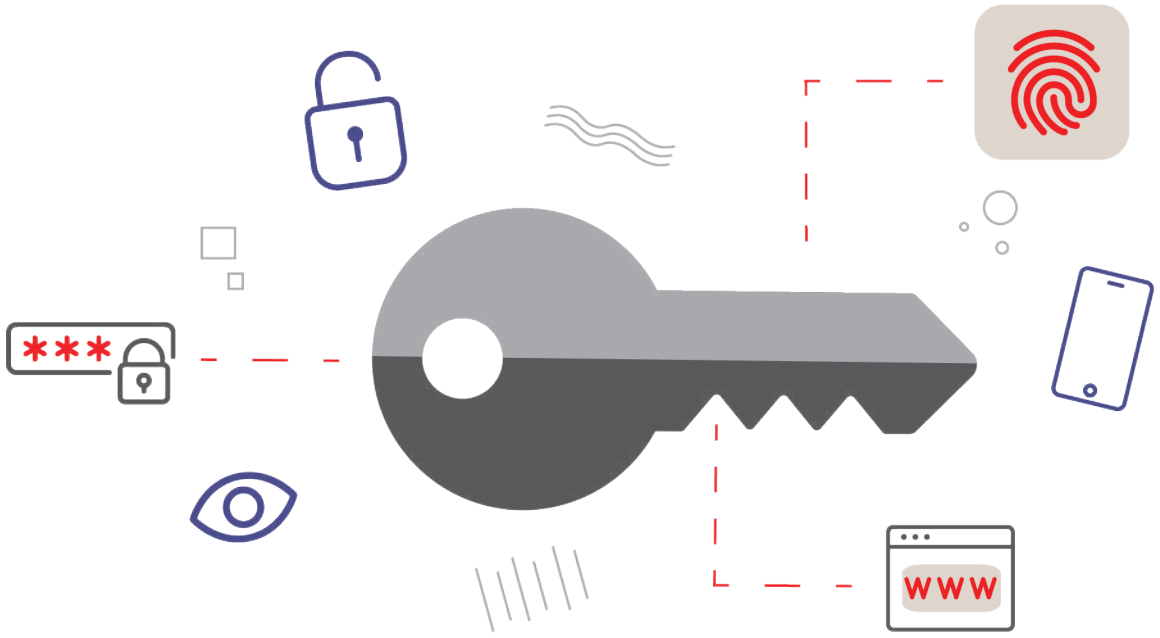
WHITE PAPER

A Comprehensive Overview of FIDO & Passkeys

Passwordless authentication to improve the cybersecurity landscape.



Overview of FIDO and Passkeys



Introduction

In today's rapidly evolving digital landscape, the necessity for robust and secure authentication methods has never been more imperative. Traditional password-based systems are increasingly vulnerable to cyber threats, leading to a growing demand for more secure alternatives. Cybercriminals are becoming increasingly sophisticated, employing techniques such as phishing, credential stuffing, and brute force attacks to exploit weaknesses in password-based authentication systems. These vulnerabilities not only compromise sensitive data but also erode user trust and confidence in digital services.

This white paper aims to provide a comprehensive overview of FIDO (Fast Identity Online) and passkeys, highlighting their significance in enhancing cybersecurity and improving user experience. FIDO and passkeys leverage public key cryptography to offer a more secure and user-friendly authentication experience. By eliminating the need for passwords, FIDO and passkeys mitigate the risks associated with password theft and reuse, providing a robust defense against phishing and other cyber threats. This document will delve into the technical aspects of FIDO and passkeys, including the cryptographic principles behind them, and explore their various use cases and industry applications.

By offering detailed insights into the technical aspects, benefits, and challenges associated with FIDO and passkeys, this document aspires to equip decision-makers with the knowledge required to confidently implement these advanced authentication methods. The white paper will also address the challenges and considerations for implementing FIDO and passkeys, providing practical guidance for organizations looking to adopt these technologies. Whether you represent an enterprise seeking to mitigate phishing attacks, a financial institution aiming to secure transactions, or a healthcare provider focused on safeguarding patient data, this white paper will serve as an invaluable resource for understanding the transformative potential of FIDO and passkeys.

What are FIDO and Passkeys?

FIDO (Fast Identity Online) is an open industry association launched in 2012 with the mission to develop and promote authentication standards that help reduce the world's over-reliance on passwords. The FIDO Alliance's goal is to change the nature of authentication by developing specifications that define an open, scalable, and interoperable set of mechanisms that reduce the reliance on passwords.[1]

Passkeys are a type of FIDO authentication credential designed to replace traditional passwords. They leverage public key cryptography to provide a more secure and user-friendly authentication experience. When a user registers a passkey, a pair of cryptographic keys is generated: a public key that is stored on the server and a private key that remains on the user's device. Authentication is performed by proving possession of the private key, which can be unlocked using biometrics, a PIN, or a pattern, enabling access to websites or applications.[2] According to the FIDO Alliance, passkeys are cryptographic credentials linked to a user's account on a website or application. By design, passkeys offer enhanced security and resistance to phishing attacks by cybercriminals attempting to steal passwords.

By eliminating password-related vulnerabilities, FIDO and passkeys offer significant benefits such as enhanced security, improved user experience, and reduced costs associated with password management.

Technical Aspects of Passkeys

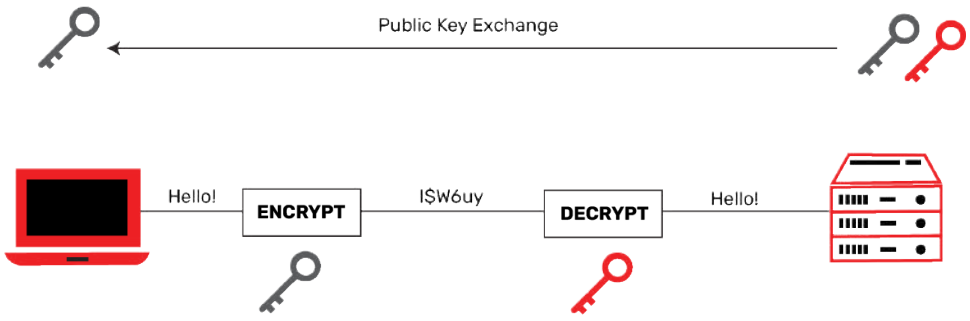
Cryptography Behind Passkeys

Cryptographic key pairs are fundamental to modern encryption and secure communication. They are used in various applications, including secure email, digital signatures, and secure web browsing. A cryptographic key pair consists of two keys: a public key and a private key. These keys are mathematically linked, but they serve different purposes and are used in different ways.

Public Key and Private Key

The public key is used to verify signatures and decrypt data that was encrypted with the corresponding private key. The private key is used to sign data and decrypt the data encrypted with the public key. The public key can be freely shared, enabling anyone to encrypt a message intended for the owner of the key. However, only the owner of the corresponding private key possesses the ability to decrypt the message, thereby ensuring that the communication remains secure. This system is referred to as asymmetric cryptography due to its use of two distinct keys for encryption and decryption.

Public Key Cryptography

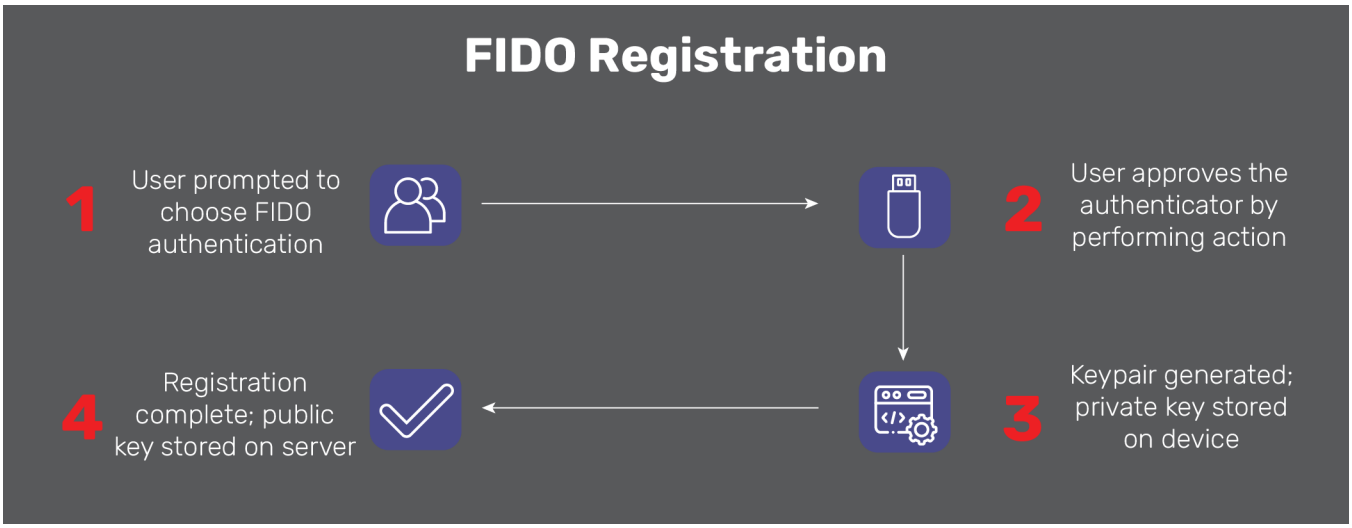


Key Generation

Key pairs are generated using cryptographic algorithms founded on mathematical problems known as one-way functions. These functions are straightforward to compute in one direction but challenging to reverse, thus ensuring the security of the keys. The generation process involves creating a large, random number to generate a pair of keys using an asymmetric key algorithm, ensuring the keys are mathematically linked.

Cryptographic keys provide robust security, but any compromise of the private key endangers the entire cryptographic secure key infrastructure. Consequently, safeguarding the private key with a secure storage method is vital. A hardware security module (HSM) is specifically designed for this purpose, ensuring the secure storage of private keys. As an example, the private key on a mobile device is kept on the Secure Enclave on Apple devices, Trusted Platform Module (TPM) on Windows and Android, and Samsung Knox for Galaxy devices.

The following graph illustrates the process of FIDO registration, detailing the steps involved in key generation.



Step 1:
During account registration, the user is prompted to choose a FIDO authentication mechanism supported by the application (also called the relying party).

Step 2:
The user approves the FIDO authenticator by performing an action that depends on the authenticator. Common actions include touching a fingerprint reader, touching a security key, entering a PIN, or other approved authentication methods.

Step 3:
A public-private key pair is created that is unique to the user's device, the user's account, and the relying party (application).

Step 4:
The public key is sent to the application and associated with the user's account. The private key never leaves the user's device.[3]

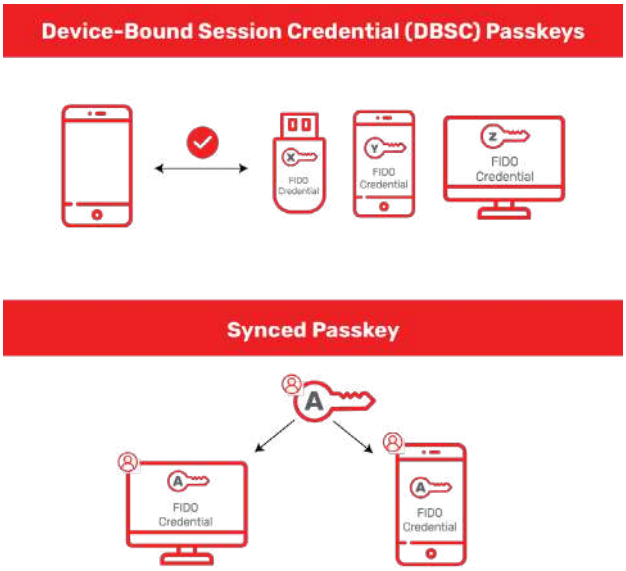
Once registration is complete, the FIDO login process involves several steps to ensure secure authentication:

1. When the user attempts to log in, the service (e.g. app or website) issues a cryptographic challenge.
2. At this point, the device generates a cryptographic proof using the private key during the registration process.
3. The cryptographic key is then sent to the client (or relying party).
4. Then the client forwards the proof to the FIDO server for verification and if the server successfully validates the proof, the user is granted access.

This process ensures that the private key never leaves the user's device, making it resistant to phishing and other attacks. During the registration process, the passkey generated will be either a synced or device bound passkey which will be explained next.

Synced vs. Device-Bound Passkeys

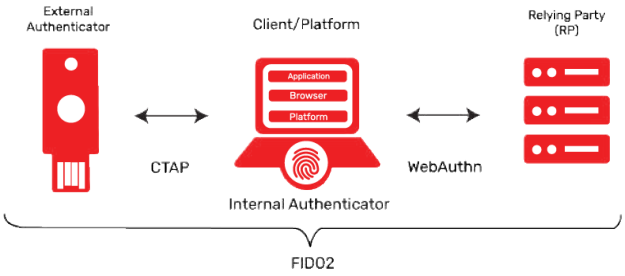
By understanding the differences between synced and device-bound passkeys, organizations can choose the appropriate authentication method based on their security requirements and user needs.



A synced passkey can be used across multiple devices through various password managers such as Google Password Manager and Apple Passkeys. This capability allows users to authenticate on new devices without needing to register unique credentials each time. Synced passkeys offer convenience across multiple devices and can be restored from a cloud account if a user loses one of their devices. While this offers a great user experience, synced passkeys are less secure compared to device-bound passkeys.

Device-bound session Credentials (DBSC) passkeys generate a pair of public and private keys stored securely on the device, providing stronger protection against impersonators attempting to hack a browser session. Since the private key remains on the device, servers will periodically verify its presence using the public key created at the beginning of the session. This allows, for example, a website to validate whether a cookie is being used from a different browser or IP address. Google Chrome and Microsoft Authenticator App employ device-bound passkeys to enhance security. A disadvantage of device-bound passkeys is that, if you lose or replace your device, a new passkey must be created.

FIDO2 Standards



The FIDO Alliance has introduced several specifications over the years, including FIDO2, which encompasses the Web Authentication (WebAuthn) standard and the Client to Authenticator Protocol (CTAP). These standards enable passwordless authentication across various platforms and devices, enhancing security and user experience.[2]

WebAuthn, a Web Authentication API standard published by the World Wide Web Consortium (W3C), is a core component of the FIDO2 specifications. It enables the use of passkeys and the creation of secure cryptographic key pairs. WebAuthn is currently supported by major web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari.[2]

The **Client to Authenticator Protocol (CTAP)** is a key component of the FIDO2, which aims to enable strong passwordless authentication. CTAP defines how external authenticators, such as FIDO Security Keys and mobile devices, communicate with browsers and operating systems to provide a secure authentication experience. This protocol works alongside the Web Authentication API (WebAuthn) to facilitate secure, phishing-resistant authentication methods. CTAP2, the latest version of the protocol, supports various transport protocols, including USB, NFC, and Bluetooth, allowing for flexible and secure communication between authenticators and clients. This protocol ensures that the authentication process is both secure and user-friendly, making it a crucial element in modern authentication systems.

Importance of FIDO2 Passkeys Across Industries

By implementing FIDO authentication, various industries can achieve higher security standards, improve user experience, and ensure compliance with regulatory requirements. This makes FIDO a crucial component in the modern authentication landscape.

Enterprises

FIDO significantly mitigates the risk of phishing and credential attacks by removing the reliance on traditional passwords. Enterprises encounter several challenges when implementing passkeys, including:

- **User Resistance:** Employees may be reluctant to transition from traditional passwords to passkeys due to unfamiliarity and perceived complexity.
- **Integration Challenges:** Integrating passkeys with existing systems and applications can be complex and time-consuming.
- **Cost:** The initial expense of deploying passkeys, including hardware and software, can pose a barrier for some organizations.

FIDO addresses these challenges by:

User Experience
FIDO passkeys provide a seamless user experience by allowing employees to authenticate using biometrics or PINs, which are more user-friendly than traditional passwords.

Scalability
FIDO standards are inherently scalable, simplifying the deployment of passkeys and ensuring seamless integration throughout the organization.

Efficiency
FIDO helps lower costs by reducing the need for password resets and management.

According to the FIDO Alliance, 75% of enterprises reported a reduction in sign-in time after implementing FIDO authentication and a 95% reduction in password reset requests among enterprises using FIDO authentication.[4] A study by Statista found that nearly half of IT professionals worldwide had adopted FIDO2 standards for workforce authentications by 2023.[5]

Financial Services

In the financial sector, FIDO provides secure transaction processing and account access, mitigating the risk of fraud and identity theft. The financial services industry encounters several challenges when implementing passkeys, including:

- **Fraud Prevention:** Financial institutions must ensure that passkeys offer robust protection against fraud and unauthorized access.
- **Customer Satisfaction:** Building customer trust and encouraging the adoption of passkeys can be challenging.
- **Regulatory Compliance:** Financial institutions must comply with regulations such as PSD2, which mandate strong customer authentication.

FIDO addresses these challenges by:

Security
FIDO passkeys provide strong, phishing-resistant authentication across all logical access end points, reducing the risk of fraud and unauthorized access.

User Experience
FIDO passkeys deliver a seamless and user-friendly authentication experience. With continued education on their purpose and capabilities during implementation, passkeys facilitate customer trust and adoption.

Compliance
FIDO Passkeys allow financial institutions to enact MFA for transactions or other use cases, which complies with mandates like PSD2.

By utilizing cryptographic keys instead of passwords, financial institutions can comply with stringent regulatory requirements such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), and PSD2 (Payment Services Directive 2). This approach ensures the protection of customer data and the security of transactions, thereby fostering trust and confidence among clients.

Healthcare

Healthcare providers benefit significantly from FIDO by safeguarding patient data and streamlining access for medical professionals. However, they can face unique challenges when implementing passkeys, including:

- **Regulatory Compliance:** Ensuring adherence to regulations like HIPAA can be complex when adopting new authentication methods.
- **Data Security:** Protecting sensitive patient data is paramount, and any new authentication method must meet stringent security requirements.
- **User Training:** Healthcare professionals may require training to effectively use passkeys, which can be time-consuming and costly.

FIDO addresses these challenges by:

Compliance
FIDO passkeys meet HIPAA requirements in healthcare organizations by storing private keys on user's device, reducing the risk of unauthorized access to Protected Health Information (PHI).

Security
FIDO passkeys employ public key cryptography to protect patient data, which is considered one of the most secure authentication methods available today.

Ease of Use
FIDO passkeys are designed to be user-friendly, reducing the need for extensive training and facilitating adoption by healthcare professionals.

With the ongoing digitization of medical records, it is imperative to ensure that only authorized personnel can access sensitive information. FIDO provides a secure and efficient method for authenticating users, thereby ensuring compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act) and enhancing the overall security of healthcare systems. Additionally, with the growing adoption of telehealth and remote care, FIDO offers a secure means for patients and healthcare providers to authenticate themselves during virtual consultations, thereby maintaining the security of patient data even when accessed remotely.

Government

For government agencies, FIDO enhances security for sensitive data and ensures compliance with regulatory standards. Government agencies face unique challenges when implementing passkeys, such as:

- **Security:** Protecting sensitive government data and systems from cyber threats is a top priority.
- **Interoperability:** Ensuring that passkeys work seamlessly across various government systems and applications can be challenging.
- **User Training:** Government employees may require training to effectively use passkeys, which can be time-consuming and costly.

FIDO addresses these challenges by:

Security
FIDO passkeys provide robust, phishing-resistant authentication, helping to safeguard sensitive government data and systems.

Interoperability
FIDO standards are designed to be interoperable, facilitating the deployment of passkeys across various systems and applications within government agencies.

Ease of Use
FIDO passkeys are designed to be user-friendly, reducing the need for extensive training and making it easier for government employees to adopt.

The adoption of phishing-resistant authentication methods is crucial for protecting government information systems from cyber threats. Government agencies in countries such as Australia, Canada, France, and the United Kingdom have acknowledged and included references to FIDO standards in their policy documents and regulations related to online authentication. The FIDO Alliance has been collaborating with the U.S. government to enhance and expedite the integration of FIDO technology within federal agencies. This initiative aligns with the broader federal zero trust strategy, which aims to strengthen cybersecurity through the implementation of phishing-resistant multi-factor authentication (MFA). The Office of Management and Budget (OMB) has recognized FIDO as an alternative to the government's Personal Identity Verification (PIV) standards for MFA, underscoring its significance for the federal workforce.[6]

Current Adoption and Challenges

The adoption of FIDO and passkeys is on the rise as organizations acknowledge the need for more secure and user-friendly authentication methods. The FIDO Alliance reports that passkeys, which utilize public key cryptography, are designed to replace traditional passwords, offering enhanced security and resistance to phishing attacks. Over 200 major companies currently support passkeys on their websites and applications, signifying a shift towards secure authentication practices. Prominent companies such as Walmart, Amazon, Target, Playstation, Discord, and Canva have implemented passkeys, demonstrating their versatility and broad appeal across various industries.[7]

According to an article from BleepingComputer, Amazon has achieved a significant milestone with over 175 million customers now utilizing passkeys for account login. This rate of adoption demonstrates the increasing preference for passwordless authentication methods, which provide enhanced security and convenience. Amazon has implemented passkeys as the default sign-in option on mobile devices for customers who have configured them. Additionally, passkey support has been extended to its Audible service. This initiative is part of Amazon's broader strategy to enhance the accessibility of passkeys and promote a more secure, passwordless internet. Passkeys enable users to authenticate using biometric methods such as fingerprints, facial recognition, or PINs, which are less vulnerable to phishing attacks compared to traditional passwords. Dave Treadwell, Amazon's Senior Vice President of e-commerce, highlighted that this initiative is designed to offer customers both ease of use and enhanced security in their Amazon experience. The company intends to extend the deployment of passkeys to additional Amazon applications and services throughout the coming year.[8]

These statistics highlight the growing adoption and effectiveness of passkeys in enhancing security and user experience across various platforms and industries.

Some key statistics on passkey adoption:

Each password reset comes with a cost to any organization and that could reach **an average of $70** according to Forrester.[9]

Passkeys have been found to have **4x higher** login success rates and enable **2x faster** logins than traditional methods.[10]

GitHub has dramatically increased 2FA adoption with passkeys, achieving a **95% 2FA opt-in rate** (Paskeys, 2024).[10]

Dashlane has seen a **70% increase** in conversion rate for signing-in with passkeys compared to passwords.[10]

CVS Health has experienced a **98% drop** in mobile account takeover fraud with over 10 million users enjoying passwordless logins.[10]

More than 85% of all customer authentications on Intuit's mobile apps are now done using passkeys.[10]

Challenges Facing FIDO Adoption

Despite their benefits in enhancing security and user experience, there are several challenges associated with the adoption of passkeys. One of the primary challenges is educating users about the advantages of passkeys. Many users, particularly those who are not technologically inclined, may lack an understanding of what passkeys are or how they function. They may be hesitant to use them due to misconceptions, such as the belief that their biometric data will be shared with websites. Another significant hurdle is overcoming user resistance. Users have become accustomed to traditional passwords and may be reluctant to switch to a new authentication method. This resistance can stem from a lack of understanding or simply a preference for familiar processes. Many users have established habits regarding password usage, including the use of password managers. Transitioning to passkeys necessitates altering these habits and embracing new practices, which can be a gradual and challenging process.

It is essential to ensure that passkeys function seamlessly across different platforms and devices. Challenges associated with making passkeys interoperable can impede their widespread adoption. It is imperative for users to have confidence in the compatibility of passkeys across various services without encountering any issues. To ensure a smooth adoption to passkeys, the FIDO Alliance created a comprehensive web resource launched to accelerate the adoption of passkeys called Passkey Central. This platform is designed to provide consumer service providers with the necessary education and steps to implement passkeys for simpler and more secure sign-ins. Passkey Central provides essential features including educational resources, implementation guidelines, and various tools designed to expedite the adoption of passkeys. These efforts aim to enhance internet security and user-friendliness. For businesses, particularly small and medium-sized enterprises (SMBs), the preparedness of their infrastructure to support passkeys can present an obstacle. They must ensure that their systems are compatible with passkey technology and that it can be seamlessly integrated into their existing security protocols. Proper training and awareness are crucial for both employees and customers. Organizations need to invest in training programs to educate users on the effective and secure utilization of passkeys.

Through comprehensive education, user-friendly implementation, and ensuring interoperability, these challenges can be effectively addressed. As a result, the adoption of passkeys can be accelerated, leading to a more secure and convenient authentication landscape.

Future of FIDO and Passkeys

The future of FIDO and passkeys appears promising with numerous advancements aimed at enhancing both security and user experience. According to a recent report, public awareness of passkeys has significantly increased from 39% in 2022 to 57% in 2024. The FIDO Alliance is actively developing new specifications and standards to improve the security and usability of passkeys. A notable development is the introduction of the Credential Exchange Protocol (CXP) and Credential Exchange Format (CXF), which will standardize the secure transfer of credentials across different providers. This initiative addresses the current limitation where passkeys are often restricted to specific ecosystems or password managers, allowing users to transfer their passkeys seamlessly between various platforms and services.

The FIDO Alliance is collaborating with major technology companies such as Apple, Google, and Microsoft to facilitate the secure movement of passkeys across different ecosystems, thereby ensuring a seamless authentication experience for users. Furthermore, the FIDO Alliance is investing in next-generation multi-factor authentication (MFA) technologies to enhance security and simplify the user experience.
These developments underscore the continuous efforts to improve the security and ease of use of FIDO and passkeys, establishing them as essential components in the future of online authentication.

FIDO has transformed the cybersecurity landscape by providing a robust alternative to password-dependent logins. The FIDO standard eliminates the need for passwords by utilizing cryptographic keys that reside on secure devices such as smartphones, fingerprint readers, or security tokens.

This approach offers several advantages:

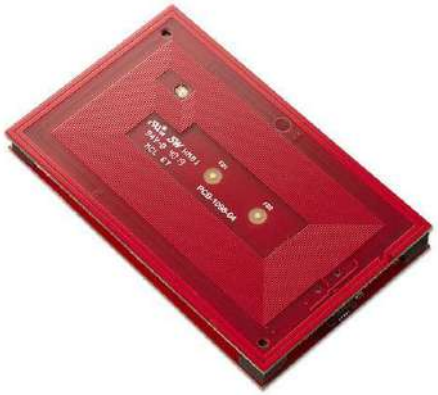
- **Phishing-resistant:** Unlike passwords, cryptographic keys are not vulnerable to phishing attacks, as they cannot be intercepted or replicated.
- **Data breach-proof:** Even if a server is compromised, attackers cannot steal the private key stored on the user's device, making it virtually impossible to impersonate the user.
- **Convenience:** Users no longer need to remember or manage complex passwords, simplifying the login process.

The integration of FIDO with protocols like TLS (Transport Layer Security) through the Web Authentication (WebAuthn) API has further enhanced the overall security framework for online interactions. This integration plays a pivotal role in achieving passwordless authentication and has proven effective against various types of cyberattacks.

By addressing these challenges and continuing to promote the benefits of passkeys, adoption rates are expected to increase, leading to a more secure and user-friendly authentication landscape.

The rf IDEAS Advantage

rf IDEAS has positioned itself as a frontrunner in FIDO solutions by providing an extensive array of products and services aimed at improving security and user experience. The following key points of rf IDEAS in this domain:



WAVE ID® Plus OEM Micro

ConvergeID™ Software Solution

rf IDEAS' ConvergeID™ software solution seamlessly converts existing credentials into FIDO2 keys, enabling passwordless authentication for Single Sign-On (SSO) and Identity and Access Management (IAM) systems that do not support the FIDO2/WebAuthn protocol. This solution enhances security and user convenience by eliminating the need for passwords and reducing password fatigue.

WAVE ID® Nano

Expansive Product Portfolio

rf IDEAS offers a diverse range of FIDO-compliant products, including the WAVE ID® Nano, WAVE ID® Plus Mini and WAVE ID® Embedded OEM which provide secure and efficient authentication for shared workstations and single sign-on. These products are designed to meet the needs of various industries, including healthcare, financial services, and government.

WAVE ID® Plus Mini

Interoperability and Scalability

rf IDEAS products are designed to be interoperable and scalable, making it easier for organizations to deploy FIDO authentication across various platforms and devices. This flexibility ensures that FIDO authentication can be integrated into existing systems without significant disruptions.

By delivering a seamless and user-friendly authentication experience, rf IDEAS assists organizations in reducing costs related to password management while enhancing overall security. rf IDEAS is dedicated to advancing FIDO authentication standards by offering robust solutions so organizations can strengthen their cybersecurity posture.

Embracing FIDO for a Secure Future

In today's rapidly evolving digital landscape, the need for robust and secure authentication methods is increasingly critical. Traditional password-based systems are becoming more susceptible to cyber threats, driving a demand for secure alternatives. FIDO (Fast Identity Online) and passkeys present a transformative solution by utilizing public key cryptography to deliver a more secure and user-friendly authentication experience. By eliminating passwords, FIDO and passkeys reduce the risks associated with password theft and reuse, providing strong protection against phishing and other cyber threats.

The adoption of FIDO and passkeys is growing as organizations recognize the necessity of more secure and user-friendly authentication methods. Whether representing an enterprise looking to mitigate phishing attacks, a financial institution aiming to secure transactions, or a healthcare provider focused on safeguarding patient data, this white paper serves as an invaluable resource for understanding the transformative potential of FIDO and passkeys.

The future of FIDO and passkeys is promising, with numerous advancements aimed at enhancing both security and user experience. The FIDO Alliance is actively developing new specifications and standards to improve the security and usability of passkeys. By addressing challenges and continuing to promote the benefits of passkeys, it is expected that adoption rates will increase, leading to a more secure and user-friendly authentication landscape.

In conclusion, the long-term benefits of FIDO for security and user experience are significant. By providing a secure, user-friendly, and cost-effective authentication solution, FIDO is set to play a pivotal role in the future of online security. Organizations adopting FIDO authentication can anticipate improved security, enhanced user satisfaction, and reduced costs, making it a valuable investment in the digital age.

How You Can Do Your Part

As we navigate the complexities of the digital age, the need for robust and secure authentication methods has never been more critical. Stakeholders must now take decisive action to implement these advanced authentication methods within their organizations.

For Enterprises:

- Adopt FIDO Authentication: Transition from traditional passwords to FIDO passkeys to mitigate phishing attacks and improve overall security. The seamless user experience provided by FIDO can enhance employee productivity and satisfaction.
- Invest in Training: Educate employees on the benefits and usage of FIDO passkeys to ensure a smooth transition and maximize adoption rates.
- Integrate with Existing Systems: Collaborate with IT teams to integrate FIDO authentication into existing systems and applications, ensuring compatibility and scalability.

For Financial Institutions:

- Enhance Security Measures: Implement FIDO passkeys to secure transactions and account access, reducing the risk of fraud and identity theft.
- Build Customer Trust: Communicate the benefits of FIDO passkeys to customers, highlighting the enhanced security and user-friendly experience.
- Ensure Regulatory Compliance: Utilize FIDO authentication to meet regulatory requirements such as PSD2, GDPR, and CCPA, ensuring the protection of customer data and transaction security.

For Healthcare Providers:

- Safeguard Patient Data: Adopt FIDO passkeys to protect sensitive patient information and streamline access for healthcare professionals.
- Facilitate Remote Care: Use FIDO authentication to secure telehealth and remote care services, ensuring the privacy and security of patient data during virtual consultations.
- Meet Regulatory Standards: Ensure compliance with regulations like HIPAA by implementing robust FIDO authentication methods.

For Government Agencies:

- Protect Sensitive Data: Implement FIDO passkeys to enhance the security of government information systems and safeguard against cyber threats.
- Promote Interoperability: Ensure that FIDO authentication works seamlessly across various government systems and applications, facilitating secure access for employees and contractors.
- Invest in Training: Provide training programs for government employees to effectively use FIDO passkeys, reducing the need for extensive support and improving adoption rates.




By taking these steps, stakeholders can leverage the transformative potential of FIDO and passkeys to create a more secure and user-friendly authentication landscape. The time to act is now - embrace FIDO authentication and lead the way in enhacning cybersecurity and user experience

Let rf IDEAS be part of your FIDO adoption process

Explore ConvergeID Passwordless Platform

425 N Martingale Rd, Suite 1680 Schaumburg, IL 60173
Phone: +1 (866) 492-8231
Email: sales@rfIDEAS.com
rfDIEAS.com/passkeys

References
1. https://fidoalliance.org/overview/
2. https://fidoalliance.org/passkeys/
3. https://www.descope.com/learn/post/fido2
4. https://fidoalliance.org/statistics-sources/
5. https://www.statista.com/statistics/1460632/fido-standards-adoption-by-companies-worldwide/
6. https://www.mitre.org/news-insights/media-coverage/inside-cybersecurity-identity-authentication-standard-for-federal-agencies
7. https://9to5mac.com/2024/11/20/200-companies-support-passkeys/
8. https://www.bleepingcomputer.com/news/security/amazon-says-175-million-customers-now-use-passkeys-to-log-in/#:~:text=When%20the%20user%20next%20attempts,different%20platforms%20and%20password%20managers
9. Source: 2018. Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers Report. Forrester Research
10. https://state-of-passkeys.io/
11. https://fidoalliance.org/new-design-guidelines-optimizing-user-sign-in-experience-with-passkeys/
12. https://www.macrumors.com/2024/10/15/fido-alliance-portable-passkeys-across-platforms/