1KOSMOS

FIDO2 Authentication with 1Kosmos

Confidently phase out passwords and give Workers, Customers and Citizens a convenient login experience.

FIDO (Fast Identity Online) authentication is a powerful technology that brings significant benefits to organizations by providing a convenient way to access company resources for the workforce, and a more secure and convenient way to access online services for customers and citizens.

Introduction

In today's digital age, ensuring the security of user authentication has become increasingly important for organizations. With the ever-growing threat landscape, organizations must adopt advanced authentication solutions to protect their sensitive information and assets. The FIDO Alliance has been working towards a passwordless future, where strong authentication is delivered with a user-friendly experience. This paper will provide an overview of how 1Kosmos delivers FIDO2 authentication for stronger user authentication.

What is FIDO2 Authentication

FIDO2 is the latest authentication standard introduced by the FIDO Alliance, which offers strong and simple authentication. FIDO2 authentication eliminates the need for passwords, making it more secure and user-friendly. The FIDO2 authentication process involves a user device, such as a smartphone or a security key, and a server that confirms the user's identity. The FIDO2 authentication process uses public-key cryptography, which means the protocol eliminates the need for passwords and offers a strong and secure authentication mechanism.

FIDO2 Authentication for the Workforce

Traditional password-based authentication systems are vulnerable to a variety of security threats, such as phishing, social engineering and brute-force attacks. These threats can lead to security breaches and the loss of sensitive data. With FIDO2 authentication, employees can be empowered to use their personal devices, such as smartphones or corporate-issued security keys, or supporting desktop systems to authenticate into corporate systems and applications. This eliminates the need for traditional passwords and reduces the risk of security breaches caused by password-related attacks.

- **Stronger Security:** FIDO2 utilizes public-key cryptography to provide robust security. It replaces weak password-based authentication with a more secure approach, reducing the risk of password-related attacks such as phishing, credential stuffing, and password theft.
- **Elimination of Passwords:** FIDO2 allows for passwordless authentication, eliminating the need for users to remember and manage multiple passwords. This reduces the likelihood of weak passwords, password reuse and the associated security vulnerabilities.
- **Multi-Factor Authentication (MFA):** FIDO2 supports multi-factor authentication, combining multiple authentication factors for stronger verification. This can include something the user possesses (e.g., a security key), something they know (e.g., a PIN), and something they are (e.g., biometric data). MFA significantly increases the security posture, making it harder for attackers to gain unauthorized access.
- **Simplified User Experience:** FIDO2 enhances user experience by streamlining the authentication process. Users can simply plug in a FIDO2-enabled security key, use biometrics like fingerprints or facial recognition, or authenticate through a mobile device. This ease of use reduces friction and improves productivity.

- **Interoperability and Standardization:** FIDO2 is an open standard that is widely supported across different platforms, devices, and web browsers. This interoperability allows organizations to adopt FIDO2 authentication with flexibility and ensures compatibility with various systems and applications.
- **Reduced Support Costs:** With FIDO2, the reliance on passwords is minimized, resulting in fewer password-related support requests such as resets and account lockouts. This can lead to reduced support costs and IT helpdesk burden, enabling IT teams to focus on more critical tasks.
- **Scalability and Future-Proofing:** FIDO2 offers scalability, accommodating organizations of different sizes and growth rates. It can be seamlessly integrated into existing systems and scaled as needed. Additionally, FIDO2 is designed to be future-proof, providing a secure foundation for authentication in the long term.

FIDO2 is designed to be future-proof, providing a secure foundation for authentication in the long term.

FIDO2 Authentication for Customers and Citizens

FIDO2 can provide a more secure and convenient way to access online services. With FIDO2, customers can use their personal devices, such as smartphones or supporting workstations, to authenticate into online services without the need for traditional passwords. This eliminates the risk of password-related security breaches like ATO attacks and can make it easier for customers to access and manage their accounts.

- **Enhanced Security:** FIDO2 provides a higher level of security compared to traditional password-based authentication methods. It eliminates the reliance on passwords, which are prone to various attacks such as phishing and credential theft. With FIDO2, customers and citizens can enjoy stronger protection for their sensitive information and online accounts.
- **Passwordless Convenience:** FIDO2 enables passwordless authentication, eliminating the need for customers and citizens to remember and manage multiple passwords. This significantly reduces the burden of password management and the risk of weak or reused passwords. Users can authenticate using biometrics like fingerprints or facial recognition, or by plugging in a FIDO2-enabled security key, providing a seamless and convenient user experience.
- **Privacy Protection:** FIDO2 authentication preserves user privacy by employing public-key cryptography. The authentication process does not involve sharing the user's biometric data or any personal information with the service providers. This ensures that the privacy of customers and citizens is upheld while still maintaining strong security.
- **Interoperability and Wide Adoption:** FIDO2 is an open standard that is widely supported by major platforms, devices, and web browsers. This broad adoption ensures that customers and citizens can use FIDO2 authentication across different online

services, websites, and applications, without being tied to a specific vendor or technology. It offers a consistent user experience and simplifies the authentication process.

- **Mitigation of Account Takeovers:** FIDO2's multi-factor authentication capability adds an extra layer of protection against unauthorized access to customer and citizen accounts. By combining different authentication factors such as biometrics and security keys, it becomes significantly more challenging for attackers to compromise accounts through methods like credential stuffing or brute-force attacks.
- **Trust and Assurance:** FIDO2 authentication provides customers and citizens with increased trust and assurance in online transactions and interactions. The strong security measures and reduced reliance on passwords instill confidence that their personal information and digital identities are safeguarded. This can encourage greater engagement with digital services and promote broader adoption of online platforms.
- **Regulatory Compliance:** FIDO2 authentication aligns with various regulatory requirements related to data protection and privacy, such as the General Data Protection Regulation (GDPR) in the European Union. By implementing FIDO2, organizations can demonstrate their commitment to security and compliance, which is essential for handling customer and citizen data responsibly.

There Is a New FIDO2 Authentication Method on the Way - Passkeys

Recent collaborations between industry giants such as Apple, Microsoft, and Google, alongside the FIDO Alliance and the World Wide Web Consortium, have solidified the support for passkeys as an authentication method.

This innovative approach to authentication relies on cryptographic keys and leverages cloud storage to securely store credentials for multiple devices. By combining a passkey on their smartphone with encrypted and safely stored cloud-based credentials, users can enjoy a streamlined and secure account authentication process.

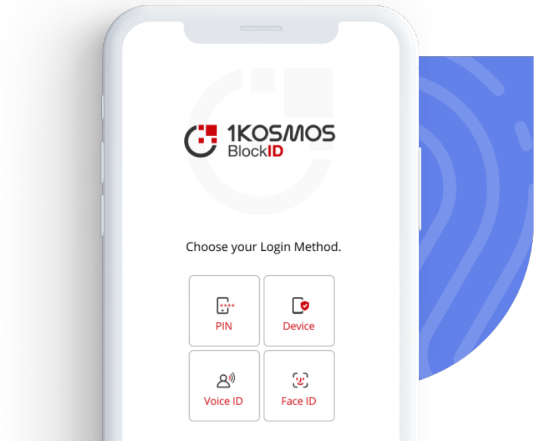
The advent of passkeys brings forth a new era, eliminating the need for traditional passwords and paving the way for enhanced security and efficiency. Integrated seamlessly with existing applications, passkeys have the potential to significantly reduce the risks associated with identity theft and phishing attempts.

There is a catch with passkeys, however. For organizations seeking an extra layer of security, device-bound passkeys present a compelling option. In the current iteration, user authentication would be stored within the Microsoft, Google and Apple ecosystems. This means users could authenticate from anywhere with unmanaged devices and auditing would be difficult if not impossible. Not to mention an ability to share passkeys, should frighten security teams enough to look for another option.

For customers and citizens, the promise of convenience, user experience, and security - passkeys are exactly what the industry has been driving toward.

Integration of 1Kosmos with FIDO2 Authentication Methods

1Kosmos has been a member of the FIDO Alliance and is committed to supporting a passwordless future. 1Kosmos offers a FIDO2 certified BlockID platform that provides strong identity verification and authentication capabilities. The 1Kosmos BlockID platform offers a combination of government-certified biometric and document verification, which adds an immutable identity layer on top of FIDO2 authentication. This makes credential sharing and identity impersonation impossible, enhancing the security of the authentication process.



User Journey of 1Kosmos with FIDO2 Authentication

The 1Kosmos implementation of the FIDO standard emphasizes interoperability. This approach guarantees that FIDO security keys from various vendors and hardware equipment from various suppliers will work together efficiently. Further, this interoperability will be achieved with cross-browser support for passwordless authentication.

1Kosmos facilitates seamless interoperability not only among connected web applications but also across workstations by linking the FIDO token to the user account. Our support for FIDO-based authentication also includes Windows and Mac workstations. Users can leverage the BlockID mobile app, which serves as a FIDO authenticator, to log into their workstations.

1Kosmos strictly adheres to the FIDO Key Authentication process involving the following steps:

Enrollment

During the enrollment process, the user registers their FIDO key on the 1Kosmos control plane (the platform). The FIDO key generates a unique public-private key pair. The public key is registered on the platform, while the private key remains securely stored on the FIDO key.

Authentication

When the user attempts to log in to the service, the FIDO key plays a vital role in the authentication process. **Here's a step-by-step breakdown:**

1. **User Verification:** The user enters their username on the service's login page. The FIDO key is connected to the user's device (e.g., via USB) and activated.

2. **FIDO Key Interaction:** The FIDO server on the control plane generates a cryptographic challenge, which is sent to the user's device. A unique challenge is generated for each authentication session which ensures freshness and prevents replay attacks.

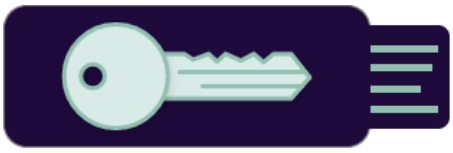
3. **User Consent:** The user interacts with the FIDO key to provide consent, typically through a physical action such as pressing a button on the key. This action cryptographically signs the challenge, ensuring the user's consent and validating the response.

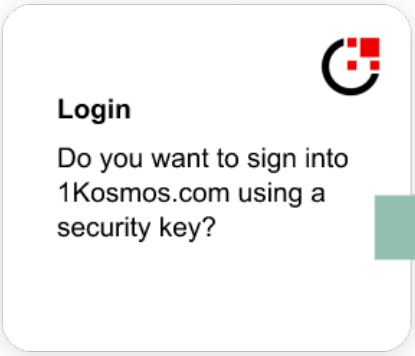
4. **Public and Private Key Registration:** The signed response is sent back to the FIDO server on the platform. The server retrieves the previously registered public key associated with the user's account.

5. **Verification:** The FIDO server verifies the authenticity of the response using the stored public key. If the verification is successful, the user is granted access to the service.

1Kosmos Supported FIDO Authentication Deployment Methods

- **FIDO Auth Device Independence:** 1Kosmos provides users the ability to register & authenticate from any device utilizing FIDO2 key-based authentication. As a result, organizations will benefit from the enhanced security protocol that enables passwordless login procedures. The approach utilizes an "enroll-once-use-anywhere" methodology, where the end-user can now seamlessly register their security key on the 1Kosmos AdminX control plane and utilize it for authentication across various services and platforms. Specifically, this includes both web applications that have been integrated with 1Kosmos BlockID, as well as Windows workstations that have the BlockID Credential Provider installed.
- **FIDO Key Onboarding with PIN:** FIDO (Fast Identity Online) Key Onboarding with PIN refers to a secure and user-friendly method of authentication that utilizes a physical hardware key, commonly known as a FIDO key or security key. 1Kosmos supports the FIDO key authentication, combined with a Personal Identification Number (PIN). The PIN acts as an additional layer of protection by requiring users to input a unique code when using their FIDO key for authentication purposes. This PIN is distinct from traditional passwords and provides an added level of security.
- **FIDO Key Authentication:** Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication using specialized USB or NFC (Near-Field Communication) devices. FIDO2 is a further development of the U2F protocol with an extended version of CTAP (Client to Authenticator Protocol), now called CTAP2. 1Kosmos also supports the cryptographic capabilities which U2F keys provide. Where organizations require FIDO2/U2F keys to secure access from multiple devices, 1Kosmos links the FIDO2 token to the user account for access requests.





- **WebAuthn:** Web Authentication (WebAuthn) and FIDO are related but not exactly the same thing. WebAuthn is a web standard developed by the World Wide Web Consortium (W3C) that enables strong authentication on the web. FIDO, on the other hand, is an open authentication framework that provides a set of specifications and protocols for secure user authentication. However, 1Kosmos supports both protocols and enables Web Authentication through FIDO methods.
- **FIDO Auth with LiveID:** 1Kosmos LiveID is a FIDO2 certified authentication method that performs a liveness verification when capturing the user's picture and gesture. It then leverages AI to validate the identity record upon access attempt. The process is certified (by the Kantara Initiative) to NIST Identity Assurance Level 2 and compliant with Identity Assurance 3, as per the NIST 800-63-3 digital identity guidelines. Using the expressions and a true-depth camera functionality 1Kosmos verifies that a live person is present. Second, a selfie is taken, compared to the picture taken at enrollment, and access is granted if they match. LiveID is over 99% accurate.
- **FIDO Platform Authenticators:** 1Kosmos appless authentication was developed for organizations or instances where a mobile app is unavailable. There are two options for authentication.

1. Users will still scan a QR code with their mobile camera, and they will be directed to a website where they will use device biometrics such as Face ID.

2. The 1Kosmos appless capability can also be used on laptops. A user can authenticate via laptop biometrics capabilities, like a camera or a fingerprint reader.

Conclusion

1Kosmos has been supporting a passwordless future through its FIDO2 certified BlockID platform. The platform provides strong identity verification and authentication capabilities, making it more secure and user-friendly. The user journey of 1Kosmos with FIDO2 authentication is simple and user-friendly, eliminating the need for passwords. The platform provides strong security measures, such as government-certified biometric and document verification, public-key cryptography, and conditional access mechanisms. Organizations can leverage 1Kosmos BlockID platform to strengthen their authentication mechanisms and protect their sensitive information and assets.

About 1Kosmos

 1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education and healthcare organizations in the world.

For more information, visit www.1kosmos.com or follow @1KosmosBlockID on Twitter.