1KOSMOS

Exploring FIDO2 and 1Kosmos

Implementation and Security Considerations for Stronger User Authentication with FIDO2 and 1Kosmos.

Whitepaper

About the FIDO Alliance

In the early 1970's Robert Morris developed a system of storing login passwords for Unix. Shortly after that users began selling their passwords so others could access the systems. The issues with passwords began. A case can certainly be made to crown the password the Achilles heel of security. Despite the ever-growing discussion that they need to be replaced if not eliminated, passwords persists.

There are very few approaches to eliminating passwords worth investigating. However, one such approach to eliminating passwords has been agreed upon by a consortium of market leaders. FIDO ("Fast IDentity Online") Alliance is an open industry association, of which 1Kosmos is a member, whose goal is to set an agreed-upon set of standards to reduce the password reliance impacting the security and usability of applications, data, and services.

The FIDO Alliance developed an agreed-upon way to handle cryptographic authentication through public and private key pairs. The FIDO specifications standardized an authentication capability that enabled users to prove they are in possession of the private key. The combination of the private key and public key stored in a small form factor provided a high level of security to transactions and was easy to use.

Launched in February 2013 by leading tech companies, the new FIDO Alliance set out to standardize the interoperability of strong authentication and reduce the user experience problems when creating credentials (usernames and passwords) and remembering them across multiple instances. Ultimately the difference with the FIDO approach to authentication is that it recognized that security, implementation, and usability are equally important.

There is a negative security impact if the user experience is poor.

Organizations do not want the cost and complexity of building and maintaining a dedicated authentication service.

Security is and always has been a concern, but balancing implementation and experience makes that difficult especially as services moved online and to the cloud.

The original FIDO specifications were FIDO UAF (Universal Authentication Framework) and FIDO U2F (Universal Second Factor) for simpler, stronger user authentication. The difference between the two is based on the use case needed. UAF is a single-factor authentication standard whereas U2F is a second-factor authentication standard.

FIDO UAF - Users register their device with a service so that they can log in by swiping a finger, looking at the camera, speaking into the mic, tapping a card, or entering a PIN. Organizations implementing the FIDO UAF have control over which method they implement to authenticate the user.

FIDO U2F allows organizations to implement a second-factor authentication to their existing password infrastructure. The user authentication journey is augmented after they log in with their username and password. The FIDO U2F service will prompt for another authentication method such as a FIDO Security Key. The addition of the second factor allows organizations to secure passwords without compromising security.

Recently, in 2018 the FIDO Alliance released a new set of specifications, FIDO2. This new specification encapsulates three elements:

1. **W3C WebAuthn** is a standard API that enables FIDO Authentication via a web browser.

2. **CTAP1** is an update to FIDO U2F. This update enables FIDO2-enabled browsers and operating systems to utilize FIDO U2F devices (such as FIDO Security Keys) for authentication via USB, NFC, or BLE for a second-factor or multi-factor experience devices.

3. **CTAP2** Similar to CTAP1 however, CTAP2 enables users to authenticate with a passwordless experience in addition to second-factor or multi-factor experience.

The FIDO Alliance has quickly become an industry standard with authentication providers leveraging the specifications to deliver secure access with a user experience that doesn't treat a user like a criminal. This is highlighted by the FIDO Alliance mission:

- **Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users.**
- **Operating industry certification programs to help ensure successful worldwide adoption of the specifications.**
- **Submitting mature technical specification(s) to recognized standards development organization(s) for formal standardization.**

Recently the three big technology leaders - Apple, Google, and Microsoft - announced plans to expand support for FIDO authentication on their platforms. Relying on passwords as the primary authentication is one of the biggest security problems on the web. The issue remains that organizations place all of the responsibility for securing a service on the user. With these three leaders pushing toward a passwordless future, users could securely access web-based services without a password.

Considering passwords are cumbersome for users to manage (and remember), this will eliminate users reusing and/or creating poor passwords and provide a superior user experience across multiple devices overall. By providing FIDO2 functionality, organizations will be able to deliver websites and apps with consistent, secure, and easy passwordless experiences. Not to mention this will make the web more secure and usable for everyone.

Expanding on the FIDO User Experience

There are many FIDO authentication form factors for organizations (and end-users) to choose from. The most common of those are:

Key

USB port enabled

Card

PIV, credit card form factor, NFC enabled

Mobile App

Device TPM-based authentication, NFC QR code, or push notifications enabled

Biometric

Voice, touch, or face recognition

Compatible Browser

Current browsers from Google, Apple, and Opera comply. Microsoft only supports WebAuthn via Edge on Windows 10

To register and begin using a FIDO authentication, users follow a few simple steps. The FIDO specifications require little input from the end-user. There are two steps.

Step One.

Registration:

This one-time step is required on each site the user wishes to use the FIDO authentication service if supported. This is to register a key with each site. Within a workforce, the registration would most often happen one time.

- **The user begins by entering their unique username at the website.**
- **The FIDO server will send a challenge to the user. Depending on the FIDO protocol/method in use, the challenge is handled through their web browser or web application. However, if the authenticator is more modern there may be input required from the user to provide a biometric, interact with an app, etc.**
- **After completing the challenge and validating the requirements of the authentication requirements, a pair of cryptographic keys: a public and private key, are generated for the authenticator plus metadata which includes the user ID, and the RPID (the site in which the user is registering).**
- **The private key is stored on the TPM of the authenticator and the public key is returned to the website, along with other encrypted metadata needed for authentication.**
- **This takes very little time and now the user is able to authenticate.**

Step Two.

Authentication:

The next step is using the authenticator. Each time the user wants to access the site they will leverage their FIDO authenticator.

- **The user is asked for a unique username.**
- **A randomly generated challenge is sent from the FIDO server to the user.**
- **The user receives and needs to comply with the challenge (provide a fingerprint, enter the key into the USB port, etc). The challenge is digitally signed along with the metadata.**
- **The response is returned.**
- **The signed challenge is verified with the public key and the user is authenticated.**

The impact of using the FIDO specifications is minimal to the end-users. Once registered the user can authenticate from anywhere. For instance, the FIDO authenticator on compatible hardware like the fingerprint available on today's Apple and Windows laptops. These types of FIDO authenticators are limited to the device as the private key is stored on the local TPM and therefore are not "portable" like other FIDO authentication methods (keys, mobile devices, cards). However, this could change with the expanded support mentioned above.

Recommendations for Administering FIDO Authentication

Administration of a FIDO deployment and day-to-day management can vary wildly; this can be dependent on the vendor selected to provide the FIDO solution. While the FIDO capabilities are certainly easy to use, building one is not something organizations will take on often.

In most cases, the solution is delivered via a cloud service. This means that all of the benefits of moving to a SaaS environment apply. Lower operational cost, scalability, and accessibility are all natively part of the solution. For organizations of any size, the benefits of a hosted FIDO service makes sense. For comparison, the benefit to organizations implementing a FIDO approach, as opposed to code generating tokens, is that organizations do not need to deploy a huge infrastructure and issue and validate the authenticity of a token. This is because public and private keys are stored on the FIDO authenticator and sign the authentication request and therefore require a very small overhead when deploying.

Deployment starts with the connection of the target application or server to the FIDO server. The connection is most often made through the use of REST endpoints to communicate with clients. Because the FIDO server is cloud-based, proper firewall configurations will be required to ensure secure communication. Due to the security requirements of the standards, HTTPS communication is required and therefore a valid TLS certificate must be in place.

A connection to a user data store and policy configurations should also be considered. If there are policies to determine how, when, and potentially where users can authenticate, this will need to be integrated into the FIDO deployment. Typically this is managed through the FIDO Metadata service (MDS). As for the user data store, the server will need to be configured for an LDAP, ActiveDirectory, MySQL, MongoDB, etc. data store all of which are easily configurable.

The choice of authenticator will determine the vendor selection and will either be included when negotiating the contract or purchased on an as-needed basis. Authenticators can always be purchased through an e-commerce site or through the selected vendor. However, organizations like 1Kosmos have moved to an app-based FIDO approach which eliminates the need to purchase an authenticator. Optionally, devices ship with built-in FIDO authentication, like a fingerprint reader on modern desktops, to handle the FIDO authentication.

Typically a proof-of-concept (POC) can be deployed and tested for usability in a few days depending on the complexity of the environment (at least that is what we see here at 1Kosmos). It is recommended that a test be run to ensure the usability, security, deployment, and maintenance are acceptable. This will require input from key stakeholders like - DevOps, Admins, Security Officers, End-Users, Support Teams, etc. Feedback and lessons learned while setting up the test will ensure a successful deployment.

The final consideration for deployment is the experience that will be provided to the end-users. The authentication method and the user experience should be where organizations start. The consideration of the two will ensure adoption and, as a result, increase security.

Deploying a FIDO method is most often dependent on the FIDO protocol used. Considerations are scale and usability based on the risk factors organizations need to secure.

- **FIDO UAF protocol:** service providers determine what types of authentication mechanisms are appropriate and provide a list of available options, which might include facial or voice recognition, fingerprint reading or entering a PIN. Users must have a personal device, like a computer or smartphone that they register. During the registration process, users are asked to choose the method provided by the service provider. Once registered, users will log in with their username and the FIDO authenticator.
- **FIDO U2F protocol:** organizations/service providers will be using the protocol as a step up to a username and password. Users will need to provide something they know with something they have, the FIDO authenticator. The authenticator can be an authentication token or security key, and can use USB, NFC (near-field communication) or Bluetooth technology.
- **CTAP1 FIDO protocol (an updated U2F protocol):** is also a second-factor authenticator, which requires a user to plug a security device into their computers, or tap their devices near an NFC reader.
- **CTAP2 protocol:** provides organizations/service providers the ability to implement a passwordless environment. The FIDO authenticator is the first and second factor authenticator. Optionally, CTAP2 can be implemented as a two-factor and multifactor authenticator if additional protection is needed based on risk profiles.

FIDO has provided a guideline for the user experience that provides detailed recommendations. A summary of those recommendations shows that there are 4 core areas to consider when building the UX:

Awareness

Increase user awareness of FIDO availability to drive adoption

Consideration

Invite users on devices that are capable to support the FIDO Authentication

Registration

Educate users on how to register and utilize FIDO authentication

Sign-On / Sign-Out

Allow users to authenticate via their FIDO registered device

Setting up a FIDO authentication service has very little overhead compared to traditional authentication services. It's lightweight and scalable, due to the small data footprint. Not to mention, the FIDO Alliance has provided ample details on how to successfully implement the technology.

Security Considerations for FIDO Authentication

Security is ultimately the reason the FIDO Alliance exists. The goal was to make passwords more secure and to even eliminate them altogether. There are many security advantages of moving to a FIDO authentication environment.

FIDO is based upon an asymmetric cryptography protocol that uses separate keys to encrypt and decrypt data (public and private key). In comparison, symmetric cryptography uses a single key to decrypt data. The additional key in asymmetric protocol obviously makes a more secure form of cryptography.

The asymmetric encryption protocol is the foundation of public key infrastructure (PKI). As mentioned above, when a user registers their FIDO authenticator a public and private key pair are generated. By leveraging a FIDO-centric platform, the traditional management challenges of a PKI platform can be mitigated. The public key is stored with the service provider and used to verify users' identities and encrypt their information. The private key is stored in the TPM of the users' FIDO authenticator and used to sign the authentication challenge the service provider imposes to then validate users' identities and decrypt their information. The benefit of the PKI platform is that it prevents hackers from accessing user accounts or accessing the sensitive information they store because they would need both keys to do so.

To gauge the requirements for a FIDO authenticator, FIDO authenticators are certified on different levels, which specifies their level of security:

Level 1

The most basic implementation of FIDO authenticator and includes all software and hardware authenticators that implement the FIDO2, UAF, or U2F protocols. This protects users against phishing, server breaches, and man-in-the-middle (MitM) attacks.

Level 1+

Authenticators must have extra security measures that protect security keys against more advanced attacks. These measures leverage a hardware-based "Allowed Restricted Operating Environment" (AROE). Level 2 authenticators are resilient to software-based attacks like malware.

Level 2

Authenticators must have extra security measures that protect security keys against more advanced attacks. These measures leverage a hardware-based "Allowed Restricted Operating Environment" (AROE). Level 2 authenticators are resilient to software-based attacks like malware.

Level 3

Level 3 FIDO authenticators protect the user's keys against basic software and hardware-based attacks. These measures are also reliant on an Allowed Restricted Operating Environment (AROE).

Level 3+

This is the most secure type of FIDO authenticator. Level 3 authenticators store their keys in a TPM and are bound to that device thus preventing any type of physical tampering or data extraction methods.

Biometric authentication is not called out in the FIDO authentication certification. However, biometrics can be part of the authentication of the FIDO method in place. The need to call out biometrics on its own is simple - biometric authentication is more prevalent and easier to use as users authenticate daily into their mobile device with their face or fingerprint. Not to mention, biometrics are becoming a convenient, secure, and affordable option on many devices. Therefore vendors are taking advantage of the proliferation of biometric compatible devices. The benefit of biometrics is that authentication goes beyond something users know or have and now accounts for who users are and therefore is a more secure means of authentication.

1Kosmos and FIDO

1Kosmos has been supporting a multi-device, omni-channel experience for years. We are a FIDO Alliance member and are working to further their passwordless objectives. The 1Kosmos platform is FIDO certified and provides a combination of strong identity (government-certified biometric and document verification) and an easy-to-use, easy-to-develop platform.

The 1Kosmos platform adds tremendous value to FIDO authentication by adding the immutable identity layer on top of authenticating FIDO tokens. The 1Kosmos platform provides identity-based authentication to FIDO by proofing a user identity and reaching IAL2 per the NIST 800-63-3 guidelines. This makes credential sharing and identity impersonation impossible. The cost of deploying 2FA and MFA solutions that require hardware is also eliminated. The 1Kosmos platform app installed on the user's smartphone will be the primary means for physical and logical access to whoever authenticates successfully.

The 1Kosmos platform can be easily extended by partners to quickly add leading-edge identity and authentication capabilities to their products and offerings in a fraction of the time it would take to natively develop these capabilities. By integrating 1Kosmos FIDO2 identity and authentication capabilities, partners can provide differentiated levels of identity verification, ease of use, feature security, and conditional access, leveraging both identity proofing and FIDO2 authentication.

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.

1KOSMOS