Daon
Information Briefs

Here's what you need to know about:

FIDO and FIDO2

Frequently asked questions and straightforward answers on why, how, and when to deploy a FIDO® Certified platform like IdentityX.

What is the FIDO Alliance?

The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords and other "shared secrets." FIDO standards provide login experiences that are more secure than passwords and SMS OTPs, simpler for consumers, and easier for service providers to deploy and manage. The FIDO Alliance is driven by the hundreds of global tech leaders; members leading the Alliance include technology and service providers such as Microsoft, Google, Samsung, Fujitsu, Amazon, Mastercard and Visa. Daon has been a member since 2014 and is heavily involved in the technical working groups that create the FIDO specifications.

What are the FIDO specifications?

FIDO is comprised of two discrete but related specifications: UAF (Universal Authentication Framework), which addresses mobile device and app use cases and CTAP (Client to Authenticator Protocol) which addresses how external second factor devices can be accessed by client applications (such as web browsers). CTAP can be combined with the W3C's Web Authentication (WebAuthN) specification to provide FIDO-based authentication in the web channel. The combination of CTAP and WebAuthN is known as FIDO2 and replaces the legacy U2F specification.

What are the key benefits of FIDO

The principal benefit of FIDO is that unique public/private key pairs are generated for each relying party that a user registers with. This concept is termed "origin bound keys" and means that a key can only be used by the original website/application that generated it—thus, even if a user is duped by a phishing attack, the authentication on the fake website will be foiled. Secondly, whether using U2F tokens or device-based biometrics in conjunction with FIDO, the verification of a human presence is always required, meaning that a remote hacker, bot, or Trojan cannot masquerade as a genuine user. Third, FIDO does not require secrets to be shared between the user and the relying party's server, which eliminates the risk of secrets being stolen while in transit. With FIDO, the only data in transit is a string of random characters which, even if stolen, cannot be used to reconstruct anything of value. This also relieves the relying party of having to possess a "honey pot" of shared secrets, which can then become the target of a breach. Last but not least, the user experience of FIDO is significantly faster, since the cryptographic work is being done locally as opposed to on a distant server. By leveraging the compute power of the user's device, relying parties reduce the strain on their own servers, cut costs, and conserve operational resources.

How does FIDO work?

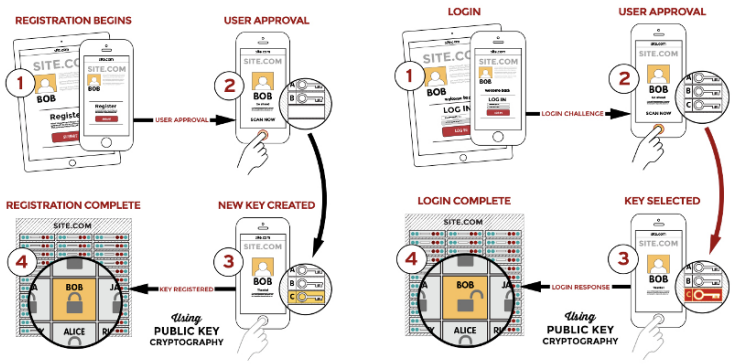

Image Source: https://fidoalliance.org/how-fido-works

As a relying party, why bother with FIDO when I could simply integrate my mobile app with the native biometric readers on iOS and Android devices?

Sounds logical, but it's a bad idea. First, the key to anti-spoofing in biometrics is **liveness detection**; you need it, and native biometric readers don't have it. Second, FIDO specifications have been peer-reviewed by many of the world's top public- and private-sector security experts over a period of several years. While your in-house developers are likely quite skilled, they can't realistically create code with the same rigorous security assurances. Third, new authenticators are being introduced almost daily, and they're being written to the FIDO specifications, which makes FIDO Certified deployments futureproof, while direct integrations with an operating system would need to be perpetually reworked as the market changes. Fourth, the FIDO specifications allow for users to choose between several biometric authentication methods (face, voice, fingerprint, palm, etc.), whereas native device authenticators typically push users to a single modality. Moreover, if a certain biometric modality is ever comprised, FIDO deployments can instantly switch to an alternate authentication method, or layer several biometrics together for added security.

Daon Information Briefs

fido ALLIANCE MEMBER

What will I need to deploy FIDO right away?

All you'll need is a FIDO Certified authentication platform like Daon's IdentityX. In fact, it's so easy to get started, we're offering a FIDO Quick Start program that gives qualifying organizations a 90-day free trial to test a working implementation of a FIDO UAF or FIDO2 server.

Is FIDO the right solution for everyone?

Certain customers and use cases will require that authentications take place on a server, and not (as with FIDO) on a local device. In some industries, the law mandates server-side authentications, exclusively, so that the audits can be stored and reviewed by regulators. In other cases, relying parties may be particularly concerned about potential collusion between two or more device holders sharing their biometrics on a single device. In addition, server-side authentication can enable additional use cases by allowing biometrics used for enrollment to be re-used across other channels and applications. For instance, if you've enrolled your voiceprint in a mobile banking app with server-side authentication, that bank's call center can now validate your identity over a landline phone by comparing your speech to the voiceprint on their server. The use of server-side authentication can also aid in identity verification during the FIDO registration process.

Is it common for relying parties to deploy both FIDO authentication and server-side authentication?

This is indeed very common and an excellent way to accommodate the widest range of needs and use cases. In some instances, relying parties will combine both types of authentication within a single user session. For instance, your bank might allow FIDO authentication for low-risk activities like checking your balance, but then require you to "step up" to server-side authentication before allowing a higher-risk activity like the transfer of funds—as the server provides a stronger chain of trust linking the authentication to the bank's identity and verification processes.

What is the special significance of FIDO2?

FIDO2 is the newest FIDO specification, and Daon is among the very first to be certified for the server component. With FIDO2, the advantages of FIDO are now available in web browsers such as Microsoft Edge, Mozilla Firefox and Google Chrome. FIDO2 is complementary to UAF, which is still required for the rich mobile application channel.

What's the business case for FIDO and IdentityX VS. direct integration with operating systems:

It's More Secure. FIDO (via the certified IdentityX platform) delivers true non-repudiation of identity credentials in accordance with the most widely adopted and thoroughly tested FIDO protocols for online authentication, which prevent both phishing and man in the middle attacks. Google, for instance, reports that not one of its 85,000+ employees has been successfully phished on a work-related account since early 2017.

It's Futureproof. FIDO ensures automatic compatibility with new authenticators and devices as they come to market, which futureproofs your investment and unlocks new capabilities without any additional coding. Furthermore, Daon's SDK-based authenticators can provide consistent authentication experiences on current and future devices without reliance on biometric hardware.

It's Easier. To implement FIDO, your app developers need only integrate with the Daon SDK once. From there, Daon handles the integrations into each and every platform, saving you time, money, and peace of mind.

It Costs Less. The cost of deploying FIDO via IdentityX as either a COTS product or as a service is significantly cheaper than the total ownership cost of developing a solution in-house and keeping it current with all the platforms and devices.

It Has a Management Console. Daon's FIDO Administration Management Console displays a full history of all user registrations, the authenticators used, and a non-repudiable audit trail of all authentications performed.

It's Flexible. Not only does IdentityX use the FIDO standard protocol for all communications during authentication, but it also utilizes vendor extensions to the protocol to offer features outside of the FIDO standard, such as device identification and server-side authentication. These features are policy-driven and can be enabled on a per-use-case basis via the easy-to-use administration console.

It's the New World Standard. FIDO has become the de facto industry standard in the Americas, Europe, and Asia Pacific. Of particular note, FIDO is fully compliant with key international regulatory requirements like PSD2 (dynamic linking) and GDPR.

Daon

sales@daon.com | 703-984-4000 | www.daon.com
4097 Monument Corner Drive, Suite 550 | Fairfax, VA 22030