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; board members leading the Alliance include technology and service providers such as Microsoft, Google, Samsung, Fujitsu, Amazon, Mastercard and Visa. Daon has been a FIDO board member since 2014 and is heavily involved in the technical working groups that create the FIDO specifications.

What are the FIDO specifications?

The FIDO Alliance specifications are comprised of FIDO2, FIDO Universal Authentication Framework (FIDO UAF) and FIDO Universal Second Factor (FIDO U2F). FIDO UAF supports passwordless authentication experiences, commonly utilizing a mobile device's biometric capabilities. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP). FIDO2 supports passwordless and second-factor use cases, enabling users to leverage biometrics and/or FIDO security keys to easily authenticate to supported web browsers and platforms such as Google Chrome, Microsoft Edge, Mozilla Firefox, Android and Windows. FIDO U2F, which supports the use of a strong second factor such as a FIDO security key, is now part of FIDO2.

How does FIDO work?

FIDO brings the tried-and-true concept of public key cryptography to mobile devices and the web. For each user, there's an interlocking pair of cryptographic keys, one public and one private. When you "sign" data using the private key kept secret on your device, anyone can then verify the authenticity of the data by referencing your public key. In the traditional paradigm, you send your private data off to a relying party's server for authentication, which places your private data in transit (where it can be stolen or phished.) With FIDO, the private data never leaves your device. Rather, your device or browser itself performs the authentication locally, then reports confirmation back to the relying party's server.

What are the key benefits of FIDO?

As mentioned, transmitting private data to a relying party's server introduces an element of risk while the data is 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 private user data, 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.

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 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. As a relying party, your in-house developers (while likely quite skilled) cannot realistically create code with the same rigor and exacting security assurances. Second, 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. Third, 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. Furthermore, in the event 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 data 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 bring some added efficiencies 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.

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.

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.

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.

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 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
11911 Freedom Drive, Suite 900 | Reston, VA 20190