

How FIDO Addresses a Full Range of Use Cases

March 2022

Executive Summary

The FIDO standards, together with their companion WebAuthn specification, are on the cusp of an important new development: evolutionary changes to the standards proposed by the FIDO Alliance and the W3C WebAuthn community aim to markedly improve the usability and deployability of FIDO-based authentication mechanisms. As a result, FIDO-based secure authentication technology will for the first time be able to replace passwords as the dominant form of authentication on the Internet.

In this paper, we explain how FIDO and WebAuthn standards previously enabled low-cost deployments of authentication mechanisms with very high assurance levels. While this has proved an attractive alternative to traditional smart card authentication, and even opened the door to high-assurance authentication in the consumer space, we haven't attained *large-scale* adoption of FIDO-based authentication in the consumer space. We explain how the introduction of *multi-device* FIDO credentials will enable FIDO technology to supplant passwords for many consumer use cases as they make the FIDO credentials available to users whenever they need them—even if they replace their device.

A Brief History of Online Authentication

Authentication is crucial for everything that happens in a digital network, whether that's communication, social networking, financial transactions, other kinds of business, or anything else. For most of us, and for most of the history of the Internet, authentication has meant one thing: entering a username and password. In other words, most of us, for most of the history of the Internet, had to live with the security and usability shortcomings of passwords. But not everybody relies on passwords all the time. If you worked in certain sectors of the government as far back as 20 years ago, you likely used Personal Identity Verification (PIV) or other kinds of smart cards for authentication. While smart cards are much more secure than passwords, they require specialized reader hardware (as well as the smart card itself), and were never integrated into the Web platform, so their reach remained limited.

Later, hardware tokens that displayed a periodically-changing code to the user, thus turning them into a *second factor* that the user had to have in order to authenticate, no longer required dedicated reader hardware (and thus worked well on the Web), but still required the physical token itself—an insurmountable hurdle for wide-spread adoption for consumer use cases. So, while these tokens (whether they used a standard like a time-based one-time password (TOTP), or were based on proprietary methods) had a somewhat broader reach, most of us, most of the time, were still typing passwords to authenticate.

As smartphones became ubiquitous, the need for specialized hardware tokens faded. Instead, the smartphone could display the TOTP code, a secret sent over SMS, or—simpler still—implement two-factor authentication through a confirmation prompt pushed to the phone. This finally opened more secure authentication mechanisms to consumer use cases (such as online banking). But there are notable trade-offs: While two-factor authentication with a dedicated TOTP token or smartphone is more secure than a password by itself, such a mechanism—unlike smart cards—is still susceptible to phishing and other attacks.

NIST, the National Institute of Standards and Technology, reflects this situation in its Digital Identity Guidelines, outlining three different levels of security (“AAL”, or “authenticator assurance level”) in NIST Special Publication 800-63B: AAL1—the lowest level—roughly corresponds to passwords, AAL2 to multi-factor authentication (without requiring phishing resistance), and AAL3 to hardware-based phishing-resistant authentication mechanisms. Based on these levels of security, most consumers, most of the time, still use AAL1 when authenticating online. Many end users will sometimes be asked to engage in AAL2 (e.g., for online banking), but very few end users have ever encountered an AAL3 authentication mechanism.

FIDO: Starting from the Top

This was the situation around 2010: phishing-resistant, hardware-bound authentication mechanisms (what would now be regarded as AAL3) were relegated to niche use cases in high-security government and enterprise settings. Those deployments required dedicated reader hardware in addition to the authenticator (the smart card), and one-off integrations with the Web platform if that was desired. On the other end of the security spectrum was password-based authentication, which was used in the overwhelming majority of (consumer) use cases, worked on the Web, but offered low security (corresponding to AAL1). Between those two, we had two-factor authentication mechanisms that were rarely used by consumers, and susceptible to man-in-the-middle and other attacks.

By 2015, the FIDO Alliance had begun publishing a set of specifications (later followed by the companion W3C WebAuthn specification) for phishing-resistant authentication mechanisms. By the end of the decade, most major browsers had implemented the by-then finalized WebAuthn specification, for the first time making a standardized web-integrated, phishing-resistant authentication mechanism broadly available to relying parties and their users - without the need for special reader hardware, installation of drivers, etc. Furthermore, when implemented in hardware, FIDO-based authentication could reach security equivalent to AAL3-level smart cards. This had two important effects:

1. High-security use cases requiring hardware-based authenticators and phishing-resistant authentication mechanisms could now be satisfied by the standard Web platform, with off-the-shelf operating systems, smartphones, and web browsers, drastically reducing the cost of such deployments. Often in these high-security use cases, the authenticators are required to resist extraction of their cryptographic key material¹. FIDO offers a certification program that allows customers to select FIDO security keys that meet these strict hardware-based security requirements.
2. Use cases that previously had to make do with phishable two-factor authentication could now consider stronger security. For example, Google was able to build its Advanced Protection Program around phishing-resistant FIDO authentication, offering users at risk of targeted attacks a level of security that went beyond Google’s regular 2-Step Verification product. Note that for this particular

¹ In fact, an authenticator isn’t considered AAL3 by NIST 800-63B unless it also offers at least FIPS-140 Level 2 General and Level 3 physical security, which precludes extraction of key material.

use case (where phishing attacks are the main concern) hardware-based FIDO security keys are attractive not so much because they preclude extraction of their cryptographic key material, but because they provide a convenient form factor for users to carry their phishing-resistant sign-in credentials around (or store them in a safe place).

To summarize, FIDO both revolutionized the deployment of high-security hardware-based authentication mechanisms in government and enterprise settings, and also enabled better alternatives to two-factor authentication options in the consumer space, which at that point consisted purely of phishable mechanisms (SMS, TOTP, push notifications, etc.). The FIDO-based two-factor alternatives were at *least* phishing-resistant, and often phishing resistant *and* hardware-based (i.e., resistant to key extraction).

But FIDO's aim was always higher: Its mission is to "help reduce the world's over-reliance on passwords." In other words, the objective is to improve the security of users who aren't (yet) using two-factor authentication or smart cards. With the current FIDO/WebAuthn specifications and the corresponding implementations in major browsers and operating systems, this proves tricky: While FIDO supports the concept of *platform* authenticators, i.e., authenticators built into devices that the user already owns—their smartphone, their laptop, etc.—in addition to *roaming* authenticators (security keys), credentials managed by those platform authenticators are lost when the user replaces their laptop or loses their phone. Consequently, the user can't rely on platform authenticators to always be there for them when they need to sign in (e.g., think of a user trying to sign into their online banking system for the first time from their brand-new phone). This leaves the user with a choice of either having to buy a security key, or fall back to less secure, non-FIDO authentication whenever they sign in from a new device.

However, it is unrealistic to expect that every consumer of online services be able and willing to purchase and carry a specialized hardware device for the purpose of signing-in on the Internet, even if it offers stronger security. We know this from experience: the earlier era of specialized hardware TOTP (or similar) tokens never made inroads at scale in the consumer world. While products like Google's Advanced Protection Program (which do require security keys) are popular amongst those users that are willing to pay an extra price for higher security, and hardware wallets are popular amongst some early adopters of cryptocurrencies, these examples are an exception to the rule in the consumer world: authentication has to "just work", without requiring additional devices or inconveniences.

WebAuthn Level 3: Bringing up the Bottom

Today, FIDO-based solutions are a great alternative to traditional AAL3-style smart card deployments that require hardware-based authenticators and phishing resistance. In addition to being used as a secure second-factor, FIDO can also offer phishing-resistant multi-factor authentication in a single authenticator, thus offering a path toward eliminating passwords for these high-security use cases. Reducing reliance on passwords and eliminating phishing within the enterprise removes two of the most prominent attack vectors.

FIDO-based solutions can also increase the security of consumer two-factor authentication by providing phishing resistance, regardless of whether those use cases care about hardware-based sign-in credentials

or not. However, we have observed limited adoption in this latter category, especially in the consumer space, because of the perceived inconvenience of physical security keys (buying, registering, carrying, recovering), and the challenges consumers face with platform authenticators (e.g., having to re-enroll each new device; no easy ways to recover from lost or stolen devices) as a second factor. While these drawbacks can make FIDO-based solutions (whether based on physical security keys or platform authenticators) a tricky proposition for users already accustomed to two-factor authentication, they present an even higher barrier to adoption for users who don't (want to) use two-factor authentication at all, and are stuck with passwords.

The FIDO Alliance and the W3C WebAuthn working group are proposing to address these gaps in a new version ("Level 3") of the WebAuthn specification. Two proposed advances in particular bear mentioning:

1. **Using your phone as a roaming authenticator:** a smartphone is something that end-users typically already have. Virtually all consumer-space two-factor authentication mechanisms today *already* make use of the user's smartphone. The problem is that they do this in a phishable manner: You may inadvertently enter an OTP on a phisher's site, or you may approve a login prompt on your smartphone not realizing that your browser is pointed at the phishing site and not the intended destination. The proposed additions to the FIDO/WebAuthn specs define a protocol that uses Bluetooth to communicate between the user's phone (which becomes the FIDO authenticator) and the device from which the user is trying to authenticate. Bluetooth requires physical proximity, which means that we now have a *phishing-resistant* way to leverage the user's phone during authentication. With this addition to the FIDO/WebAuthn standards, two-factor deployments that currently use the user's phone as a second factor will be able to upgrade to a higher security level (phishing resistance) without the need for the user to carry a specialized piece of authentication hardware (security keys).
2. **Multi-device FIDO credentials:** We expect that FIDO authenticator vendors (in particular those of authenticators built into OS platforms) will adapt their authenticator implementations such that a FIDO credential can *survive device loss*. In other words, if the user had set up a number of FIDO credentials for different relying parties on their phone, and then got a new phone, that user should be able to expect that all their FIDO credentials will be available *on their new phone*. This means that users don't need passwords anymore: As they move from device to device, their FIDO credentials are already there, ready to be used for phishing-resistant authentication. Note that this change is not a change in the standard—it is a change we expect authenticator vendors to make in their authenticator *implementation*. There *are* proposed changes to the WebAuthn and FIDO specifications that would enable a better user experience around FIDO credentials (including multi-device FIDO credentials), in particular for those relying parties that need to serve password-based and FIDO-based users at the same time. The user experience around FIDO credentials would be very similar to that of using a password manager that helps the user sign in, but the level of security is better than even traditional two-factor authentication—all without requiring any additional steps or devices during authentication: Typically, all a user would have to do on a new device to sign into

a relying party is to pass the built-in biometric challenge² on the device from which they're trying to sign in (as we'll explore further below).

For these multi-device FIDO credentials, it is the OS platform's responsibility to ensure that the credentials are available where the user needs them. (Note that some companies are [calling](#) FIDO credentials "passkeys"³ in their product implementations, in particular when those FIDO credentials may be multi-device credentials.) Just like password managers do with passwords, the underlying OS platform will "sync" the cryptographic keys that belong to a FIDO credential from device to device. This means that the security and availability of a user's synced credential depends on the security of the underlying OS platform's (Google's, Apple's, Microsoft's, etc.) authentication mechanism for their online accounts, and on the security method for reinstating access when all (old) devices were lost. While this may not always meet the bar for use cases that require, say, AAL3, it is a *huge* improvement in security compared to passwords: each of the referenced platforms apply sophisticated risk analysis, and employ implicit or explicit second factors during authentication, thus giving AAL2-like protections to many of their users. This shift from letting every service fend for themselves with their own password-based authentication system, to relying on the higher security of the platforms' authentication mechanisms, is how we can meaningfully reduce the internet's over-reliance on passwords at a massive scale.

Syncing FIDO credentials' cryptographic keys between devices may not always be possible, for example if the user is using a new device from a different vendor, which doesn't sync with the user's other existing devices. In such cases, the existence of the above-mentioned standardized Bluetooth protocol enables a convenient and secure alternative: if the FIDO credential isn't readily available on the device from which the user is trying to authenticate, the user will likely have a device (e.g., phone) nearby that *does* have the credential. The user will then be able to use their existing device to facilitate authentication from their new device.

We believe that the syncing of FIDO credentials, together with the Bluetooth alternative, allows FIDO authentication to not only be a suitable alternative for existing two-factor deployments, but for the first time, be a viable solution for use cases where deployments of two-factor authentication methods have proven difficult, and where consequently consumers are stuck with passwords. This approach reflects an evolutionary step in the FIDO ecosystem, delivering phishing-resistant authentication at a scale that rivals that of password-based authentication deployments.

As previously mentioned, the security of a synced FIDO credential depends on the account security of the underlying OS platform. Relying parties may or may not want to rely on this dependency. At the very least, however, the verification of a synced FIDO credential represents a very strong signal to a relying party that the user is who they say they are. In fact, for many relying parties we expect that this is all they need to

² Note that none of the proposals for the WebAuthn Level 3 spec assume a change in how biometrics are used today: we assume that as before, the biometric template to authenticate the user on a device does not leave that device.

³ Note that any use of the term "passkey" in this document refers to such third-party usage of the term and is not a formal term of FIDO Alliance or its specifications.

sign in the user. However, a relying party can choose, for additional security or regulatory reasons, to go beyond trusting the synced FIDO credential on the new device and perform further user verification steps whenever the user signs in from a new device. We accommodate this through a proposed new extension, which will allow relying parties to recognize when a user presents an existing FIDO credential from a new device, and to create an additional device-bound cryptographic key on that new device. This device-bound key can later be used to (re-)authenticate the user on this device without extra verification steps, and without depending on the account security mechanisms of the underlying OS platform.

The figure below summarizes the idea of multi-device FIDO credentials (with device-bound keys), and how they are different from traditional FIDO credentials.

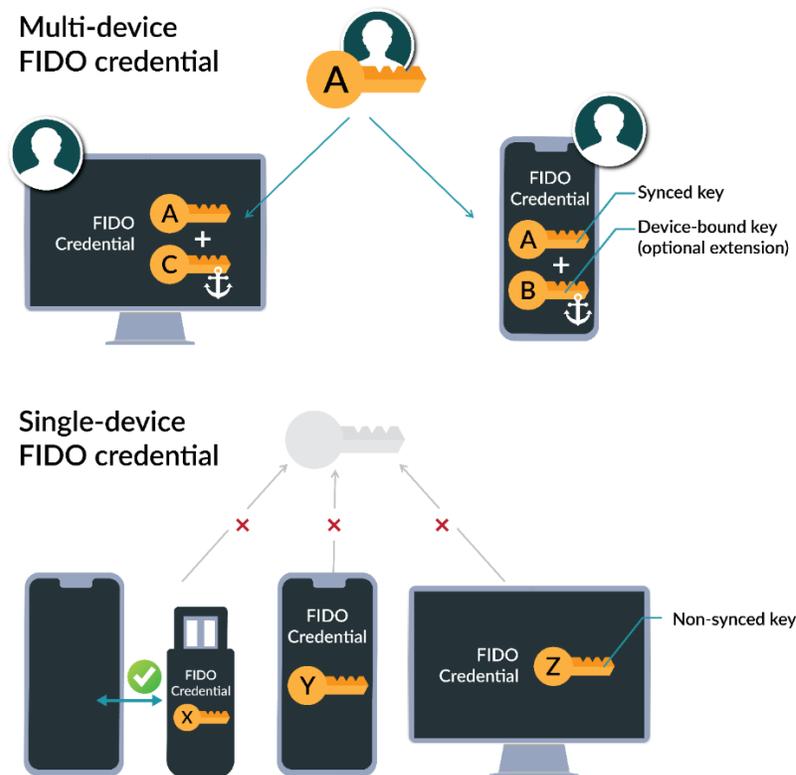


Figure 1: Multi-device vs. single-device credentials

Multi-device vs. single-device credentials: An authenticator implementation may choose to sync a FIDO credential's cryptographic key across multiple devices belonging to the same user (key A). Authenticators that do support syncing may also support an extension that creates an additional device-bound key that is guaranteed to not be synced across devices (key B and key C), and that can be used to detect if a credential is coming from a new device or an already-accepted device (shown above). Other implementations may not support syncing, or the key syncing might be turned off for some other reason, e.g., turned off by the user (shown below). Such single-device credentials may still be usable across devices, for example, when a security key is used with a mobile phone during user authentication (shown in the lower left).

Note that the WebAuthn/FIDO specifications have never precluded credentials from being synced - and that is also not what the proposed specification changes are about. Rather, the proposed changes to the WebAuthn/FIDO specifications are designed to deliver a better user experience in a world where FIDO credentials might be synced from device to device.

Summary

The current FIDO and WebAuthn specifications deliver very high levels of authentication assurance (on par with AAL3 when using hardware-based FIDO authenticators) at a much lower cost of deployment and better usability, compared to traditional smart card deployments.

Use cases that are at a lower level of security (including password-only and phishable two-factor deployments), however, currently face the traditional security-versus-usability trade-off when considering FIDO: FIDO can deliver better security, but that higher security comes at a price—the user has to adopt a special purpose authentication device (security keys). As a result, many relying parties keep their users in a password-only mode, or at best, offer phishable second factors.

The proposed WebAuthn changes improve on this situation by

1. Turning the user's existing smartphone into a roaming authenticator, and
2. Providing better support for authenticator implementations (in particular platform authenticators) that sync FIDO credentials between the user's devices.

This makes FIDO the first authentication technology that can match the ubiquity of passwords, without the inherent risks and phishability.

The proposed WebAuthn changes also include a new extension that allows relying parties to request device-bound cryptographic keys on roaming or platform authenticators (which will never be synced across devices), further improving support for use cases that require device-bound key material.

To summarize, relying parties would have a choice: rely on synced FIDO credentials (and, in effect, on the authentication security and account recovery procedures of platform providers), or use FIDO with device-bound signals such as the proposed new device-bound-key FIDO extension (and implement their own account recovery mechanism). As a result, the anticipated evolution of FIDO authenticator implementations to allow credential syncing, along with the proposed FIDO and WebAuthn spec changes, are poised to offer, for the first time, attractive alternatives to the status quo for a whole spectrum of use cases, ranging from consumer deployments of two-factor authentication or even password-only systems (where FIDO substantially improves security without sacrificing usability or deployability) to high-security government or enterprise systems (where FIDO meets stringent AAL3-like security requirements through simpler deployments). This is summarized in the following picture.

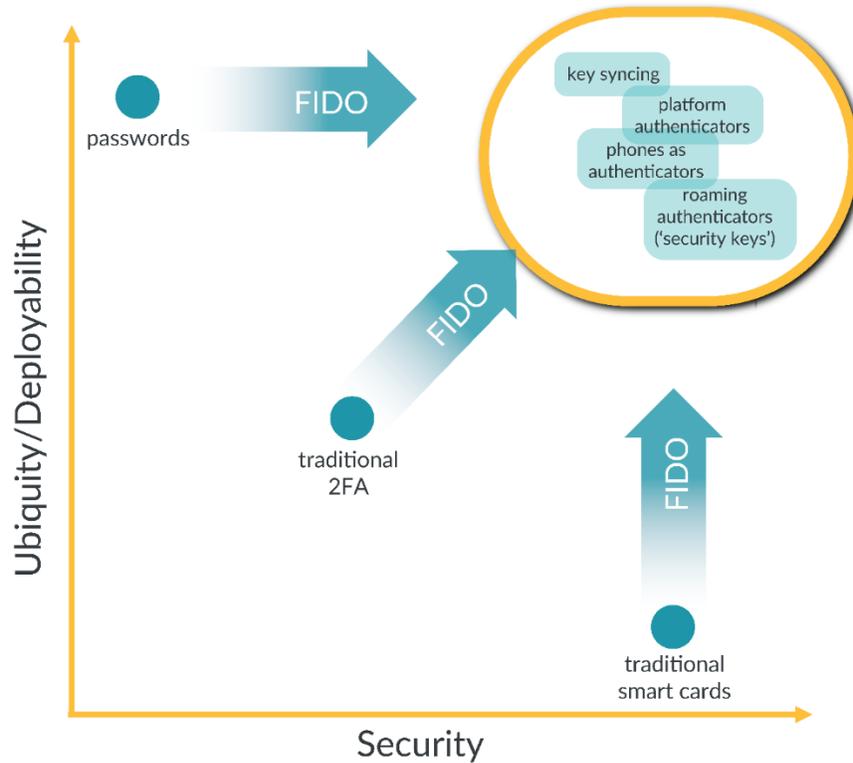


Figure 2: Anticipated evolution of FIDO authenticator implementations

About the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO authentication is stronger, private, and easier to use when authenticating to online services.

References

- [FIDO2: WebAuthn & CTAP](#)
- [Explainer: broadening the user base of WebAuthn](#)
- [FIDO Alliance White Papers & Public Documents](#)