FIDO Alliance White Paper:
FIDO for e-Government Services

FIDO Government Deployment White Paper

December 2022

Editors:
FIDO Government Deployment Working Group

Abstract

The global COVID-19 pandemic closed offices and forced governments to rapidly move services online, if they weren't already, to serve its citizens. Although usernames and passwords are easy to deploy and easy for citizens to use, they leave systems and users vulnerable to cyberattacks. They are especially vulnerable to phishing attacks designed to steal login credentials and compromise legacy multi-factor authentication (MFA) tools like those using one-time passwords (OTP) and push notifications. With phishing attacks on the rise, it is imperative for governments to support "phishing-resistant" MFA technology that is also accessible, efficient, and cost-effective.

Enterprises and governments around the globe are turning to modern online authentication solutions featuring FIDO specifications based on public key cryptography. Governments and industries have embraced FIDO as the preferred way to deliver high-assurance MFA to consumers. Notably, the Cybersecurity & Infrastructure Security Agency (CISA), a component of the U.S. Department of Homeland Security (DHS), refers to FIDO security keys as the gold standard of MFA[1].

Several governments globally have deployed and/or supported FIDO authentication for citizens to securely conduct government transactions, including making tax payments and applying for and accessing government benefits. Governments leveraging FIDO authentication solutions have realized reduced operational costs and increased consumer satisfaction.

Audience

This white paper provides guidance for policymakers and department/agency heads seeking to learn about FIDO authentication to support or deploy FIDO for e-government services.

[1] See https://www.cisa.gov/mfa

Contents

Figures

1. Introduction[2]

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for MFA and passwordless authentication, as well as remote identity verification and secure IoT onboarding.

Our 40+ board members (see here for latest list), whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, and fintech, as well as those in security, health care, and information technology.

Figure 1 – FIDO Alliance Board Members as of 11/01/2022

Today, FIDO standards are being used across cloud services, banking, payments, fintech, health care, government, enterprises, and e-commerce to deliver authentication that is both more secure and easier to use. Increasingly, these standards are being used to control the authentication of people to systems controlling IoT devices.

The FIDO Alliance's work to standardize the use of on-device biometric matching coupled with authentication certificates using public key cryptography has transformed the identity and authentication market, creating a standards-based alternative to legacy authentication tools such as central-match biometric systems, one-time passwords (OTPs), and traditional PKI.

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

[2] Substantial content in the introduction is recycled from our prior publications.

2. What is FIDO?

MFA is the recommended method to augment or replace passwords as a more secure method for identity, credential, and access management (ICAM). The FIDO Alliance has created open MFA standards based on public key cryptography supported by a large global vendor and customer community. After enrolling a device, users can authenticate without a password using either a physical security key, a device-integrated biometric sensor, or a wallet app. FIDO specifications and related compliance certifications ensure uniform security across different hardware and software platforms, including all major browsers, mobile phones, laptops, and desktops.

All MFA options are not equal in terms of the security they provide. A variety of legacy authentication methods governments can consider are based on shared secrets—including Look-Up Secrets, Out-of-Band Devices (i.e., push notification), and OTP apps and tokens, which makes them inherently phishable. However, these methods are often coupled with phishing-resistant methods based on asymmetric public key cryptography, such as FIDO, as the same in terms of security. Given how attackers have caught up with the former legacy types of authentication, it no longer makes sense to combine these methods as a single designation, but rather to distinguish phishing-resistant authentication as a higher security option.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), a component of the Department of Homeland Security, has called FIDO the “gold standard”[3] of MFA in their MFA guidance and noted, “The FIDO protocol is built into all major browsers and phones. It can use secure biometric authentication mechanisms – like facial recognition, a fingerprint, or voice recognition – and is built on a foundation of strong cryptography. Often it uses a physical device – a key – essentially an encrypted version of a key to your house.”

2.1.1 Benefits of FIDO for e-Government Services

FIDO is the gold standard method for MFA based on several benefits:

- ***Phishing-resistance***: Unlike SMS or TOTP codes that can be phished by social attacks, a FIDO session cannot be intercepted by a man-in-the-middle (MiTM) attacker who simply replays the SMS or TOTP code.
- ***Standards-based***: FIDO is an open standard. All FIDO specifications are based on public key cryptography and are strongly resistant to phishing. FIDO’s latest set of specifications are W3C WebAuthn and FIDO CTAP, collectively known as FIDO2.
- ***Certification-backed***: Unlike authentication apps that use roll-your-own technologies with unknown vulnerabilities, FIDO certification ensures uniformity of implementation, quality and backward-compatibility across devices, platforms, and releases. The large number of certified vendors provides governments with a wide choice of solutions across many platforms, devices, and operating systems at competitive pricing while avoiding vendor-lock into any specific solution.
- ***Hardware Flexibility***: FIDO standards support a variety of hardware options, including on-device and cross-platform authenticators. This includes laptops, desktops, mobile phone, tablets and FIDO security keys.

[3] See https://www.cisa.gov/mfa

- ***Privacy respecting***: The FIDO standard specifically defines aspects of the security, biometric storage and encryption levels required by global privacy and data security regulations like GDPR.
- ***Cost Reduction:*** You might want to consider cost savings as described in the GSA example below, OTP via SMS is expensive for agencies and is mitigated via FIDO.
- ***Accessible***: A wide range of implementations and platforms also affords a choice of authenticators for those with disabilities who require a preferred choice of authentication methods with specific devices.
- ***Legacy compatibility:*** Adoption of FIDO-based authentication is not an all-or-nothing proposition. FIDO-based authentication can be adopted side-by-side with existing authentication solutions with migration plans to match compliance schedules.

As a standards-based technology, FIDO Certified solutions offer governments authentication solutions that increase security over shared secrets such as passwords and OTP solutions, with strong authentication based on public key cryptography.

After having their identity verified, citizens can securely establish a trusted digital Identity that government agencies can rely on to deliver services or benefits. Without a robust user authentication method like FIDO, government agencies cannot reliably establish secure and reliable eGov services.

Moreover, since many citizens seldom interface with government departments, forgotten passwords are commonplace. FIDO improves the user experience via eliminating the frustrating password reset process. These benefits exceed many of the current cybersecurity, privacy, and regulatory identity requirements by governments around the globe undergoing digital transformation projects and similar migrations away from password-based authentication. In the face of evolving threats and complex changes to digital ecosystems, the FIDO Alliance continues to support users, the vendor community, and their customers with the highest standards for modern authentication.

2.1.1.1 FIDO e-Government Deployments and Integrations[4]

Government departments and agencies should consider leveraging shared services for authentication to improve fraud mitigation, improve user experiences, and reduce costs. Doing so may require some agencies to separate account management from benefits eligibility management within agency applications.

In many ways, reducing friction during application onboarding is strategically more important to government adoption than reduced friction for user onboarding.

Government agencies from more than 10 countries have recognized and included references to FIDO standards in policy documents and/or regulations pertaining to online authentication[5]. In this paper, we collect several practical use cases from government agencies of Czech Republic, Taiwan, United Kingdom, and United States.

[4] Substantial content in this section is recycled from our prior publications.
[5] See https://fidoalliance.org/fido-government-deployments-and-recognitions/

Czech Republic

CZ.NIC is the DNS domain registry in the Czech Republic and they operate the national identity provider (IdP) called mojeID. The goal of mojeID is to make it easier for users to browse the internet and log in to websites that require registration, and to verify users for the providers of these services. mojeID has over 800,000 users.

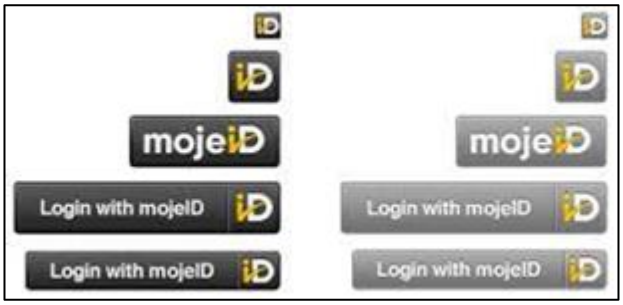


Figure 2 - mojeID

In August 2020, CZ.NIC received accreditation from the Czech Ministry of the Interior that the IdP mojeID with support for FIDO is approved as an eIDAS eID scheme on Level of Assurance (LoA) Substantial for services integrated with the Czech e-government system. In September 2020, the service was launched.[6]

In March 2021, the Czech Ministry of the Interior also issued eIDAS accreditation for mojeID's IdP with eIDAS LoA High, under the following conditions:

- Username and password are used
- The FIDO2 Authenticator is FIDO® Certified at Level 2 (or higher)
- The FIDO2 Authenticator is based on a secure element that is certified for FIPS 140-2 Level 3 or Common Criteria EAL4 + AVA_VAN5
- The FIDO2 Authenticator must have PIN set and PIN is required for all transactions at LoA High

Taiwan - Ministry of the Interior, Ministry of Health and Welfare, Financial Supervisory Commission

Launched in 2019, Taiwan FidO, or TW FidO, is a UAF-based mobile authentication service deployed by the Ministry of the Interior.[7] It is used by employees to securely access the Ministry's intranet and by citizens for e-government services. Citizens can register for the Taiwan FidO service with personal citizen certificates and log in to many e-government services using a registered Taiwan FidO account. After identity verification via inserting a MOICA (Citizen Digital Certificate) card, a QR code is presented on a browser, then the user scans the QR Code with their mobile phone and enrolls using their fingerprint or face on the mobile phone.

[6] See https://www.mojeid.cz/documentation/singlehtml/

[7] See https://fido.moi.gov.tw/pt/

Figure 3 – Taiwan FidO

In November 2019, Taiwan's government authorized TW FidO as an authentication method for citizens to access the government's portal to pay land value tax. In May 2020, the Ministry of Finance added individual income tax filing for use with TW FidO. As of September 2022, there are 55 systems using TW FidO, including tax filing, accessing the government's MyData service, voting at stakeholder meetings of listed companies, portals of ministries and local governments, etc.

In February 2022, TW FidO merged with the newly announced "Mobile Citizen Digital Certificate" service. This new service can support digital authentication and digital signing within the same mobile App.

Also, Taiwan's digital COVID vaccination certificate has been available since December 2021. The digital certificate, accepted by 60 countries, including EU nations and the US. Taiwan FidO is one of the citizen's identification options to apply for this certificate. Furthermore, FSC (Financial Supervisory Commission) will run a proof of concept of FIDO (Taiwan Financial FIDO) for financial agencies, including holdings, insurance companies, banks, and securities companies, etc., to deploy FIDO in the second half of 2022.

United Kingdom - National Health Service (NHS)

To support citizen access to healthcare services, the UK's National Health Service (NHS) created NHS login, an authentication and identity verification service based on OpenID Connect that allows the public to access NHS resources with a single login. The NHS App, which provides access to a range of services such as booking medical appointments and ordering repeat prescriptions on iOS and Android, was the first service to use NHS login to identify and verify users. The NHS' digital team initially deployed multi-factor authentication for users logging into websites displaying the NHS login button and the NHS App. They required both a password and a one-time SMS password and were becoming a significant barrier for users trying to access medical information and services.

Figure 4– NHS Login

To mitigate the barriers, NHS Digital decided that biometric authentication would best address its needs and, following a search of platforms that complied with their requirements, FIDO UAF was selected to best fulfill the criteria, including open and scalable standards and support for mobile browsers.[8]

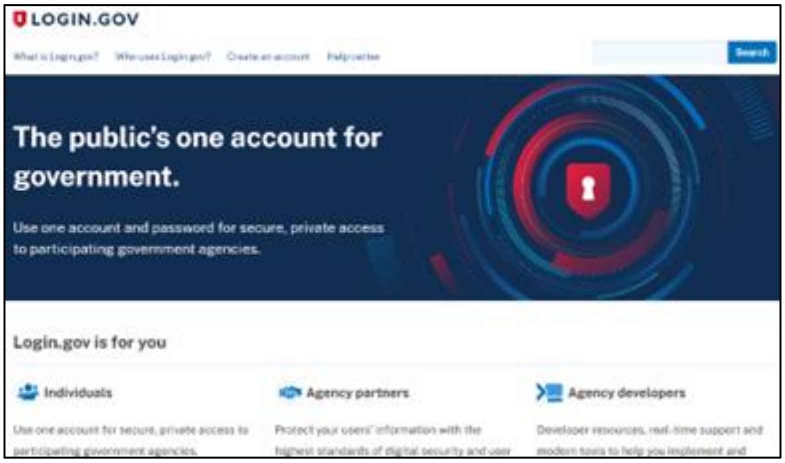
According to the FIDO Alliance case study on the NHS deployment, "As of December 2020, the NHS App with the option for biometric authentication login has a user base of approximately 1.2 million and is growing at an average rate of 32,000 new users per week. The number of SMS OTPs that NHS Digital has needed to send to users dropped by nearly two-thirds, to about 1.5 per user per month, down from about four per user per month, which represents a significant cost savings for the NHS."[9]

United States General Services Administration

The General Services Administration (GSA) developed and manages login.gov, a portal for single sign-on (SSO) across different agency applications used by both federal employees and citizens. With phishing attacks on the rise, it was imperative for the government to support "phish-proof" multi-factor authentication technology.

[8] See https://fidodev.wpengine.com/national-health-service-uses-fido-authentication-for-enhanced-login/

[9]More information on the NHS deployment can be found at https://media.fidoalliance.org/wp-content/uploads/2021/02/FIDO-Alliance-case-study_NHS-FINAL.pdf



The public's one account for government.

Use one account and password for secure, private access to participating government agencies.

Login.gov is for you

Use one account for secure, private access to participating government agencies.

Protect your users' information with the highest standards of digital security and user

Developer resources, real-time support and modern tools to help you implement and

Figure 5 - Login.gov

The GSA evaluated several options for authentication for login.gov with three main priorities: security, cost, and compliance. Although popular with end-users, GSA wanted to offer a secure alternative to SMS OTPs that could prevent phishing and began evaluation of the FIDO2 Authentication standards.[10] After review, the GSA found that FIDO2's phishing resistance made it the most appropriate approach to address its security challenges, but security was not the only factor in selecting FIDO2; cost was another important factor.

The GSA found SMS OTPs quite expensive to manage. Without alternatives, those expenses would continue to escalate as more and more users are onboarded to login.gov. With FIDO2, GSA could leverage a "bring your own FIDO security key" approach, making it more cost-effective.

3. FIDO Is a Global Standard Supported by Every Major Platform

Over the last five years, the FIDO Alliance has delivered a comprehensive framework of open industry standards for MFA that addresses key security and usability shortcomings in previous authentication tools and provide practitioners with new options for crafting digital identity solutions.

FIDO standards have delivered improvements in online authentication by means of open, interoperable technical specifications that leverage proven public key cryptography and on-device match of biometrics for stronger security and device-based user verification for better usability. The impact of FIDO standards, and formal certification testing to those standards, is notable:

- Firms including Google, Microsoft, PayPal, Apple, Amazon, Verizon, Facebook, ING Bank, Bank of America, USAA, NTT DOCOMO, Yahoo Japan, Aetna, Intuit, Cigna, eBay, Dropbox, Salesforce, and their peers around the world have deployed authentication solutions based on FIDO standards.

[10] See https://fidodev.wpengine.com/u-s-general-services-administrations-rollout-of-fido2-on-login-gov/

- Governments around the world that are either using FIDO today for citizen identity or have announced plans to modernize citizen identity systems around a FIDO-centric architecture include Korea, Thailand, Taiwan, the United Kingdom, and the United States. In the U.S. CISA has advised election officials to adopt FIDO security keys.[11] The UK's Government Digital Service (GDS) published updated guidance, "Using Authenticators to Protect an Online Service." The guidance differentiates and defines the quality of authenticators as low, medium, and high and recognizes FIDO as high-quality authenticators. The GDS defines a high-quality authenticator as "if it could not belong to anyone other than the user who created the account. A secret cannot be a high-quality authenticator because it's easy for someone to steal, guess or copy."[12]
- In September 2022, the US General Services Administration (GSA) released a new RFI for the next generation of the USAccess Program, which is the governmentwide managed service program that is used by most civilian US government agencies to issue PIV smart cards across the Federal enterprise. As part of this new program scope, GSA published a draft Performance Work Statement (PWS) that lays out the requirements for the soon-to-be-updated system. The updated system envisions a wide role for FIDO2 in the new PIV architecture.
- FIDO Alliance worked with the World Wide Web Consortium to make FIDO an official web standard. The resulting W3C Web Authentication standard (WebAuthn)[13], which is part of the FIDO2 standards, enables FIDO functionality to be embedded in major browsers (i.e., Chrome, Edge, Firefox, Safari). Therefore, FIDO-standard MFA can be deployed for any web application without any significant burden on the part of an implementer and is now widely available in the browser.
- The ITU has formally adopted the FIDO specifications as standards through ITU X.1277 (FIDO Universal Authentication Framework) and ITU X.1288 (FIDO Client to Authenticator Protocol (CTAP)/Universal 2-factor Framework).
- More than 900 products have been FIDO Certified—demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.
- All core device platforms from Apple, Google, and Microsoft now support FIDO. This means that FIDO Authentication is now natively built into browsers and platforms on most smartphones and laptops— meaning that neither implementers nor their customers need to buy a separate technology to enable MFA.

  For example:

  - Microsoft has embedded FIDO at the OS level in Windows 10 and Windows 11, where it provides the basis for the Windows Hello passwordless login solution.[14]

[11] See https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Actions_to_Counter_Email-Based_Attacks_on_Election-Related_S508C.pdf

[12] See https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services

[13] See https://www.w3.org/TR/webauthn/

[14] More details on the Microsoft announcement are at https://www.microsoft.com/en-us/microsoft-365/blog/2018/11/20/sign-in-to-your-microsoft-account-without-a-password-using-windows-hello-or-a-security-key/

- Google has embedded support for FIDO in both the OS level (Android) and the browser (Chrome). All devices running Android 7 and above (more than 1 billion in total across the globe) are now FIDO Certified to serve as authenticators.[15]
- Apple has embedded support for FIDO in both the OS level (iOS and MacOS) and the browser (Safari).

All told, we estimate that well over 4 billion devices on market today have built-in support for FIDO Authentication.

3.1 FIDO Specifications

FIDO protocols, including the FIDO2 specifications, use standard public key cryptography techniques instead of shared secrets to provide stronger authentication and protection from phishing and channel attacks.

The protocols are also designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services, and biometrics, when used, never leave the user's device.

This is all balanced with a user-friendly and secure user experience through a simple action at log in, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device, or pressing a button.

FIDO specifications support a variety of different form factors and use cases including both "roaming" and "bound" authenticators, as well as models where a multi-purpose device like a smartphone can serve as both, depending on the authentication use case. The one theme that unites all FIDO implementations is their reliance on asymmetric public key cryptography paired with a secure user experience through a simple action at log in, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device, or pressing a button.

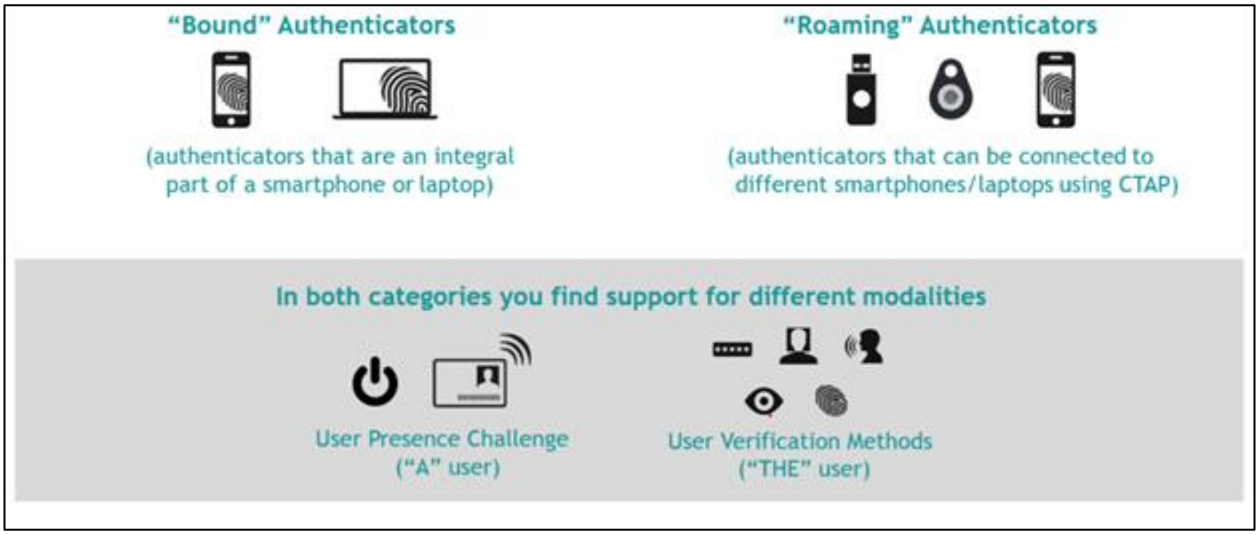

"Bound" Authenticators
(authenticators that are an integral part of a smartphone or laptop)
"Roaming" Authenticators
(authenticators that can be connected to different smartphones/laptops using CTAP)
In both categories you find support for different modalities
User Presence Challenge ("A" user)
User Verification Methods ("THE" user)

Figure 6 - Bound v. Roaming Authenticators

[15] More details on the Google announcement are at https://threatpost.com/google-ditches-passwords-in-latest-android-devices/142164/

The FIDO Alliance has published three sets of specifications for simpler, stronger user authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and the Client to Authenticator Protocols (CTAP). CTAP is complementary to the W3C's Web Authentication (WebAuthn) specification; together, they are known as FIDO2.[16]

FIDO2, the latest specification, is comprised of the W3C Web Authentication specification and corresponding Client-to-Authenticator Protocols (CTAP) from the FIDO Alliance. FIDO2 supports passwordless, second factor and multi-factor user experiences with embedded (or bound) authenticators (such as biometrics or PINs) or external (or roaming) authenticators (such as FIDO Security Keys, mobile devices, wearables, etc.).

- All FIDO protocols are based on public key cryptography and are strongly resistant to phishing (for more information, see "How FIDO Works"). They provide for a wide range of use cases and deployment scenarios.
- All technical specifications are open and available on the specifications download page.[17]

In addition to meeting the technical requirements, the FIDO Alliance developed further security requirements that need to be implemented to enhance the security assurance of each device. These requirements are covered in the Authenticator Certification program found on the Certified Authenticator Levels page.[18]

4. Getting Started with FIDO

FIDO Alliance manages functional certification programs for its core specifications (UAF, U2F, and FIDO2) to validate product conformance and interoperability, and in addition has introduced programs to delineate security capabilities of FIDO Certified Authenticators as well as to test and validate the efficacy of biometric components.

For governments, the FIDO Certification program enables them to build and/or buy best-of-breed authentication solutions that are proven to be interoperable and adhere to FIDO specifications. Likewise, end users will be able to simply leverage authenticators that work across devices and websites.

Government agencies and departments should consider leveraging shared services for authentication to improve fraud mitigation, improve user experiences, and reduce costs. Doing so may require some agencies to separate account management from benefits eligibility management at agency applications. In many ways, reducing friction during application onboarding is strategically more important to government adoption than reduced friction for user onboarding.

At the time of the release of this paper, over 900 products have been certified by the FIDO Alliance.[19]

[16] See https://www.w3.org/TR/webauthn-1/
[17] See https://fidoalliance.org/specifications/download/
[18] See https://fidoalliance.org/certification/authenticator-certification-levels/
[19] See https://fidoalliance.org/certification/fido-certified-products/

5. Deployment Considerations

Like all security technology, the way FIDO authentication is implemented influences the overall security stance of the deployed system. This section covers security considerations when deploying, implementing, or selecting a FIDO server.[20] There are two issues we highlight:

1. The FIDO server stores no permanent secrets, nor does it require storage of private data, only public keys. However, there is, in theory, an attack where an adversary might attempt to take over a FIDO server and substitute public keys.

   If the database server housing registered FIDO public keys is breached, an attacker may substitute their own public key into one or multiple user entries. In this way, the attacker may compromise and take over any account or choose to delete the registration data altogether and create a denial of service. A FIDO server must store the public key (and other user registration data) in permanent storage and therefore must protect that data from being compromised. Protecting the integrity of data at rest is a topic beyond the scope of this document, but many companies, including members of the FIDO Alliance, have expertise in this field. If you are deploying a commercial FIDO server for government agencies, make sure to study the implementation of the user registration data storage. The vulnerability described in this section is real and in the worst case can result in a major breach.

   Note that it is relatively easy for users to self-register FIDO keys with each agency or centralized portal (e.g., a site like the U.S. government's Login.gov). It is not advisable to distribute pre-registered keys. One of the drawbacks is the implementation of centralized user impersonation for registration.

2. For enterprise use cases, it's important to maintain visibility of user behaviors across sensitive resources to perform access accountability. In these cases, centralization of authentication through an identity provider (IdP) can simplify FIDO2 adoption and the transition away from less secure MFA.

   To aid an agency's long-term strategy to add phishing-resistant MFA options and eventually retire legacy authenticators, IdPs must be expected to deliver a specified strength of authentication, to include phishing resistance, as a part of requests from relying parties.

   IdPs need to convey rich identity and authentication assurance information to the RP about the authentication event it performed on its behalf. This includes the quality of the proofing that bound the authenticator to the user's identity, the strength of the authenticator, and the assurance conveyed by the IdP's token or assertion. IdPs and RPs, and the vendor products they rely upon, will need to harmonize their support for "rich assurance claims" within the federated authentication protocols they use. Enriching assertion claims and logs can help agencies understand their progress toward MFA goals, especially implementation of phishing resistance, in a way that's shared with IdPs, RPs, and risk executives. Large agencies should consider adopting profiles of OIDC and OAuth 2.0 to facilitate interoperability, and security and may need to modify long-standing SAML service implementations before phasing them out.[21]

   Agencies can add existing identity and authentication assurance claims, such as authentication method reference, to federated authentication implementations as a first step that can enrich requests, transparency, and metrics for their phishing resistance deployment.

[20] See https://media.fidoalliance.org/wp-content/uploads/2020/10/Considerations-for-Deploying-FIDO-Servers-in-the-Enterprise.pdf

[21] See https://www.mitre.org/news-insights/publication/enterprise-mission-tailored-oauth-20-and-openid-connect-profiles; https://openid.bitbucket.io/fapi/fapi-2_0-message-signing.html; https://openid.net/wg/igov/status/

Agencies should also establish and oversee assurance requirements for IdPs, whether they're leveraging existing capabilities to add FIDO2 or adding new ones. IdPs need to be accredited and protected at a high level and need to be operated with formal third-party oversight according to clear service descriptions for RPs, the RPs' security operations, and the RPs' risk executives. Enterprise IdPs must protect signing keys using HSMs.

6. Registration and Binding

The Digital Identity Guidance published by the Financial Action Task Force (FATF) paved the way for "non-face-to-face" onboarding of financial customers.[22] Although in development for over a year, the March 2020 release aligned with the onset of the COVID-19 pandemic, which shuttered financial institution branches and equipped global regulators with guidance to rapidly expand or adopt branchless financial services.

The Digital Identity Guidance includes the diagram below, with the FATF noting that the stages of identity proofing and enrolment could occur in a different order, but the overall objective is to identify and verify the person and have that identity bound to an authenticator.

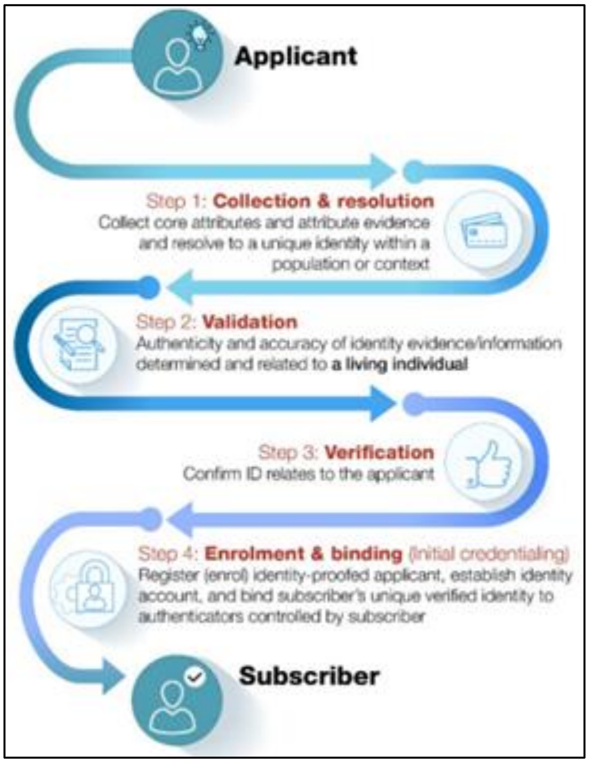

Applicant
Step 1: Collection & resolution
Collect core attributes and attribute evidence and resolve to a unique identity within a population or context
Step 2: Validation
Authenticity and accuracy of identity evidence/information determined and related to a living individual
Step 3: Verification
Confirm ID relates to the applicant
Step 4: Enrolment & binding (initial credentialing)
Register (enrol) identity-proofed applicant, establish identity account, and bind subscriber's unique verified identity to authenticators controlled by subscriber
Subscriber

Figure 6– Stages of Identity Proofing

Per the FATF, some possible examples of actions taken within Component One could include:

[22] See https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

- ***Collection:*** Present and collect identity attributes and evidence, either in person and/or online (e.g., by filling out an online form, sending a selfie photo, uploading photos of documents such as passport or driver's license, etc.).
- ***Validation:*** Digital or physical inspection to ensure the document is authentic and its data or information is accurate (e.g., checking physical security features, expiration dates, and verifying attributes via other services).
- ***De-duplication***: Establish that the identity attributes and evidence relate to a unique person in the ID system (e.g., via duplicate record searches, biometric recognition and/or deduplication algorithms).
- ***Verification***: Link the individual to the identity evidence provided (e.g., using biometric solutions like facial recognition and liveness detection).
- ***Enrollment in identity account and binding:*** Create the identity account and issue and link one or more authenticators with the identity account (e.g., passwords, one time code (OTC) generator on a smartphone, PKI19 smart cards, FIDO certificates, etc.). This process enables authentication.

It is strongly recommended that users are onboarded with two FIDO authenticators. Please refer to the Account Recovery section below.

Sample User Onboarding with FIDO2

The U.S. GSA's login.gov supports FIDO2 through the use of FIDO security keys and built-in FIDO authenticators like Windows Hello biometrics. For users, these are all referred to as "security keys" during user onboarding.

The process for setting up FIDO2 at login.gov works like this:

1. When a user is creating a login.gov account, they enter their email address and create a password. Login.gov will first send an auto-generated email for the new user to confirm their email address.
2. Then, they are instructed to select and set up MFA from a menu of options, including SMS OTP, FIDO2 security keys, and backup codes.
3. To set up FIDO2, the user will select the "Security Key" option.
4. The user can create a nickname for their security key.
5. They are prompted to either insert a hardware security key into their computer and touch it or, if their device has a supported built-in authenticator, be prompted to use it by looking into the camera or touching a biometric sensor (for two examples).
6. The user is presented with a "success screen," and then they can access their login.gov account.

Many users take advantage of the "Remember Device" option when signing in. For example, if the user is using a laptop and checks "Remember Device," they will not need MFA on that laptop again for another 30 days.

Account Recovery[23]

The primary mechanism to reduce higher-friction account-recovery mechanisms is by encouraging users to register multiple authenticators on their accounts. The loss or breakage of a single FIDO authenticator is minimally impactful to the user when an additional authenticator is readily available.

FIDO authenticators such as FIDO enabled USB keys (FIDO Security Keys) or mobile phones can be used for this purpose. For example, a user could have their personal computer and mobile device connected to their banking account. If one is ever lost, damaged, or replaced, the user can log in with the other device. Roaming authenticators, like USB keys, are particularly useful for this purpose. Users can register a FIDO Security Key as an additional authenticator across all their accounts but keep it locked in their desk drawer at home or another safe place. If they ever lose their primary authenticator (e.g., phone or security key), they can use the additional device to authenticate, retaining account access and avoiding further account-recovery mechanisms.

FIDO Member Google's Advanced Protection is a good example of this approach. The user is required to enroll two FIDO Security Keys for any given service to maintain consistent access. Note that the additional authenticators to be registered and the registration processes should ensure the resulting assurance level to be at the same or higher assurance level while satisfying a relying party's security policies and requirements.

If an additional authenticator is unavailable, lost, or broken, relying parties may fall back to identity proofing of their users using a mechanism at the same or higher assurance level as the initial account bootstrapping. This can be the same method used to create accounts or could be a mechanism set up after the account was created.

It ultimately is up to the government agency/department (relying party) to select the appropriate options that balance account risk and user experience while meeting security policies.

So how does it all work, technically?

Below are the necessary building blocks for FIDO authentication.

[23] Substantial content in this section is recycled from our prior publications. See https://media.fidoalliance.org/wp-content/uploads/2019/02/FIDO_Account_Recovery_Best_Practices-1.pdf

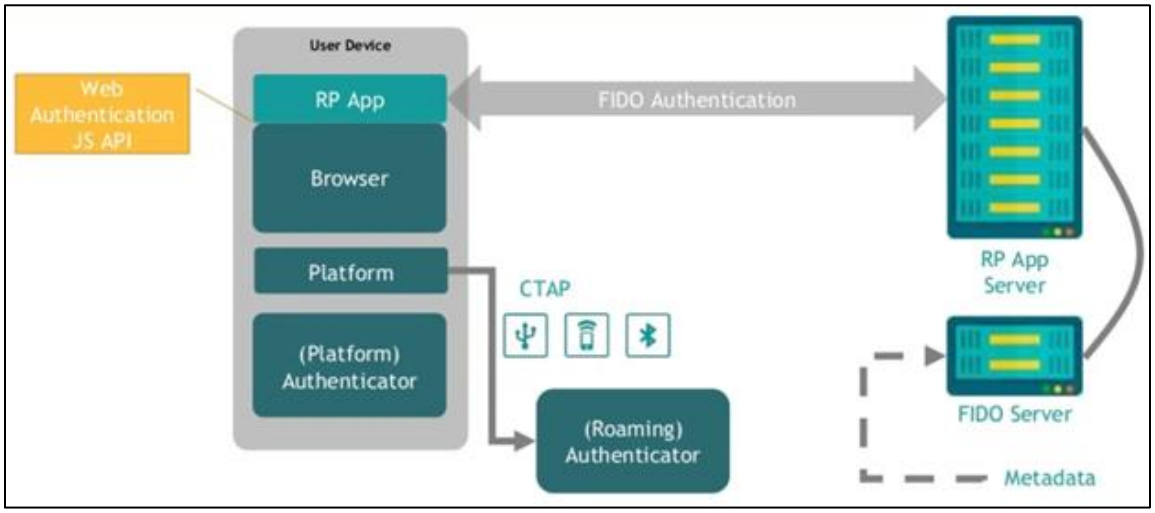


Figure 7– Building Blocks for FIDO Authentication

- Web Authentication (WebAuthn)
  WebAuthn enables online services to use FIDO Authentication through a standard web API that can be built into browsers and related web platform infrastructure. WebAuthn allows users to log into internet accounts using their preferred device. Web services and apps can turn on this functionality to give their users an easier login experience via biometrics, mobile devices, and/or FIDO security keys and with much higher security over passwords alone.
- Client to Authenticator Protocol (CTAP)
  CTAP enables external devices such as mobile handsets or FIDO security keys to work with browsers supporting WebAuthn, and also to serve as authenticators to desktop applications and web services.
- Authenticator Types
  FIDO Authenticators can be classified into two types: roaming authenticators and platform authenticators. While each of these authenticator types performs the same role in the FIDO standard, they appear quite different to the end user.
    - ***Roaming Authenticators***
      The roaming authenticator attaches to the client device over protocols such as USB, Bluetooth® low energy technology, or NFC. This means that even smartphones can act as authenticators for a separate client device. In this way, the roaming authenticator allows the user to carry the credentials associated with one relying party (RP) to authenticate on multiple computers.

- ***Platform Authenticators***
  Platform authenticators have the benefit of ubiquity. A platform authenticator is simply an authenticator implemented in a computing device playing the role of the client in the FIDO standard. Common implementations include biometrics for user verification as well as special hardware chips for protecting cryptographic key materials (e.g., Secure Execution Environment, Trusted Platform Module (TPM), or a Secure Element (SE)). If the user is performing the authentication gesture with the same device running the browser, that would be considered authentication with a platform authenticator.

7. Usability

The World Health Organization (WHO) estimates that 15% of the world population – over 1 billion people live with some form of disability.[24] In many countries, there are laws that prohibit discrimination against people with disabilities (PwD) and ensure PwD fully and equally participate in every aspect of the society.

To address this and meet the needs of PwD, the W3C, an international community that develops open standards to ensure the long-term growth of the web, Web Content Accessibility Guidelines (WCAG). Although WCAG was originally designed as web content standards, it has become well-recognized and accepted as an appropriate guide for non-web products as well.

Notable international laws include the United States' Section 508 of the Rehabilitation Act of 1973, European Accessibility Act (EAA) and Accessible Canada Act (ACA).

The FIDO Alliance's Consumer Deployment Working group will publish an in-depth white paper providing an overview of the WCAG, international laws and how FIDO authentication can allow governments and industry to comply.

User Experience

While usability requirements and best practices can help to meet the needs of PwD, not to be overlooked is the user experience for persons with and without disabilities. Another resource we encourage you to read is FIDO's User Experience (UX) Guidelines.[25] The document serves as best practices for relying parties and implementers of a FIDO desktop authenticator experience, based on a regulated industry (e.g., banking) use case. The guidelines aim to accelerate decision-making during FIDO implementation and specify what information and controls should be given to users.

The recommendations represent FIDO's perspective on how to implement FIDO authentication on desktop for consumers and should be used in tandem with other FIDO publications such as FIDO marketing guidelines, FIDO's logo usage guidelines, FIDO Privacy Principles, and other technical documentation. The intended audience is anyone responsible for implementing the interface or user experience of FIDO desktop authentication for a browser-based website – noting that these guidelines are based upon a regulated industry use case. This audience includes but is not limited to, user experience designers, product managers and software development teams.

[24] See https://www.who.int/news-room/fact-sheets/detail/disability-and-health
[25] See https://fidoalliance.org/ux-guidelines/ux-guideline-pdf/

Promotion and Education for Users

While many consumers are becoming accustomed to accessing devices, apps, and websites without relying on a password, many are not, and it is important to educate citizens on the benefits and security FIDO authentication provides to protect their privacy and security. The FIDO Alliance has developed a number of publicly available educational resources to introduce FIDO to consumers:

- The FIDO Alliance has launched a microsite, LoginWithFIDO.com, for high level, non-technical information about FIDO for consumers and service providers.[26]
- There is also a FIDO Alliance Consumer Education video available for viewing.[27]

Although the FIDO Alliance has not produced them, governments should consider producing public service announcements and posting information on social media to complement these resources.

8. Acknowledgments

The authors acknowledge the following people (in alphabetic order) for their valuable feedback and comments:

- Lorrayne Auld, The Mitre Corporation
- John Callahan, Veridium
- Karen Chang, Egis
- Wei-Chung Hwang, ITRI
- Tom Clancy, The Mitre Corporation
- Yao Ding, Meta
- Mike Engle, 1Kosmos
- Kevin Goldman, Trusona
- Jeremy Grant, FIDO Alliance/Venable
- Adrian Loth, FIDO Alliance
- Michael Magrath
- Zachary Martin, FIDO Alliance/Venable
- Aiki Matsushita, DDS
- Megan Shamas, FIDO Alliance
- Andrew Shikiar, FIDO Alliance
- Alastair Treharne, Ingenium Biometrics
- Mitch Tseng, Egis
- Jin Wen, JPMorgan Chase & Co.
- Teresa Wu, IDEMIA

[26] See https://loginwithfido.com/

[27] See https://youtu.be/k55tRpnI-6o