FIDO Government Deployments and Recognitions

About the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance 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.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to the creation of standards for multi-factor authentication.

At the time of this publication, the FIDO Alliance has certified over 800 products.

Introduction

Secure access to online applications and services has evolved into a framework reliant on devices, public-key cryptography, and biometrics to replace the shared secrets of aging passwords.

Migrating away from static passwords and weaker forms of authentication to mitigate phishing and other cyberattacks, governments around the world have turned to FIDO's specifications for a variety of reasons, including:

- Standards-based, vendor-neutral, strong authentication
- A large ecosystem comprised of authentication technology vendors, handset and operating system manufacturers, relying parties, government agencies, and academia
- Privacy-enhancing
- Phish-resistant technology
- Scalable

Over the past few years, several governments have enacted data protection and privacy regulations. To comply, government agencies and the private sector have sought technologies that can protect and secure access to data while adhering to the data privacy provisions contained in many of the new laws and pending legislation. FIDO's privacy-preserving principles comprise a core part of the FIDO Alliance's technologies.

The following is a list of government deployments and recognitions by government agencies. As the adoption and deployment of FIDO technology continues to expand worldwide, please refer to the current list.

Australia

The Australian Signals Directorate (ASD), the Australian government's cybersecurity agency, published its Essential Eight Mitigation Strategies, which are a prioritized list of mitigation strategies to assist organizations in protecting their systems against a range of cybersecurity incidents. The mitigation strategies include application control, patch applications, configuring Microsoft Office macro settings, user application hardening, restricting administrative privileges, patch operating systems, multi-factor authentication, and daily backups.

To assist organizations in determining the maturity of their implementation of the Essential Eight, the Essential Eight Maturity Model provides guidance on maturity levels for each mitigation strategy and recommends all organizations aim to achieve Maturity Level 3.

For multi-factor authentication, although the ASD lists several authentication factors, the ASD points out that these factors should not be considered equal in terms of security effectiveness. The ASD points out that multi-factor authentication is most effective when one of the authentication factors is physically separate from the device from which the user is accessing the system or resource, such as using a physical token rather than a software certificate.

For Maturity Level 3, the ASD directs implementers to use at least two of the following authentication factors: passwords, (FIDO) Universal 2nd Factor security keys, physical one-time password (OTP) tokens, biometrics, or smartcards. FIDO2 Authentication is currently under evaluation.

Canada

Canadian Digital Service (CDS)

The Canadian Digital Service (CDS), the federal government agency "committed to making it easier to access and use government services", deployed two security keys supporting FIDO2 to every employee to protect user credentials and assets stored in the cloud.

Two security keys were deployed because the security keys are enrolled and bound to the user. If an employee forgets their security key at home or loses it, they have a backup and will not be "locked out" of the CDS' system.

In a blog post, the CDS reported that after deploying FIDO they have had zero reported account takeovers and that using security keys has helped keep it that way.

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 800,000 users.

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.

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

France

The National Cybersecurity Agency of France, ANSSI (Agence nationale de la sécurité des systèmes d'information), published a Zero Trust Model (Le modèle Zero Trust) guide in April 2021. In the guide, ANSSI identifies several areas to integrate the principles of Zero Trust into a "traditional" information system. One of the areas identified is using state-of-the-art authentication tools; while ANSSI acknowledges that not all two-factor authentication approaches are equal, noting that since two-factor authentication is generally a prerequisite for the implementation of the Zero Trust model, it is recommended to be careful in choosing authentication factors and favor, for example, certificates generated by a trusted key management infrastructure or FIDO tokens.

ANSSI also referenced FIDO2 and FIDO Universal 2nd Factor (U2F) in its published Recommendations Relating to Multifactor Authentication and Passwords. This updated document replaces guidance from 2012, intended to be used as a baseline/input to any security risk analysis addressing authentication.

Republic of South Korea

Korea Internet Security Agency (KISA)

The Republic of South Korea was an early adopter of FIDO. Realizing the security and usability enhancements FIDO could bring, the Korea Internet Security Agency (KISA) developed what is known as the K-FIDO specification. K-FIDO combines the FIDO Universal Authentication Framework (UAF) specification and Public Key Infrastructure (PKI) to enable authentication and ID verification at the same time for successful commercial fintech deployments. It enables biometric accredited certification services that provide accredited certificates without passwords.

Korea National Intelligence Service (KNIS)

The Korea National Intelligence Service (KNIS) recognized FIDO's specifications in its third version of Security Requirements for Government Agencies, which recommends FIDO Authentication as a strong cryptographic second-factor option for end-user security.

Ministry of Interior and Safety (MOIS)

Government 24 is the official portal of the Korean government, providing e-government services to citizens. The portal was developed and is operated by the Ministry of Interior and Safety (MOIS) and as of March 2020, provides over 90,000 services to over 14 million registered users. Prior to deploying FIDO, Government 24 relied upon username and passwords and ActiveX-based public certificates, posing security vulnerabilities and hindering widespread use. The government was interested in adding support for several biometric authentication methods, such as facial matching and fingerprint, to enhance user experience and security for smartphone users. For users with a fingerprint reading device, the government needed to authenticate users based on 6-digit PIN. The government did not want to store biometric data in a database for "one-to-many" matching and instead required a solution to implement 1:1 matching.

The government added support for the FIDO UAF specification, leveraging secure 1:1 matching of fingerprint templates for authentication when it launched in 2019.

Sweden

eduID

eduID is a Swedish identity system that is a member of SWAMID, which is an identity federation that includes most higher education institutions and government agencies and is involved in higher education and research in Sweden. The basic idea is that a given user, who is authenticated with an organization, is automatically authenticated with other organizations in the federation.

eduID is operated by SUNET, the organization that provides the Swedish higher education sector with access to well-developed and effective national and international data communication and the national academic identity infrastructure.

eduID supports a variety of authentication mechanisms, including FIDO U2F as a two-factor authentication protocol.

Taiwan

Ministry of the Interior (MOI)

Launched in 2019, Taiwan FidO or TW FidO is a mobile authentication service deployed by the Ministry of the Interior. It is used by employees to securely access the Ministry's intranet and by citizens for e-government services. Citizens can register for 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.

In November 2019, the Taiwan 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 May 2021, there are nine services using TW FidO, including tax filling, accessing the government's MyData service, voting at stakeholders' meetings of listed companies, portals of ministries and local governments, etc.

In February 2022, TW FidO was 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. For updated information on the status and deployment of Taiwan FidO, please visit https://fido.moi.gov.tw/.

Thailand

Electronic Transactions Development Agency (ETDA)

Thailand's Electronic Transactions Development Agency (ETDA) is developing a FIDO UAF system that will provide enterprises or organizations with a reference site to deploy their mobile authentication applications with a passwordless experience. The reference site also uses OpenID Connect to allow cross-government agency login integration.

The system consists of: (1) FIDO UAF Server deployed at ETDA that allows citizens to onboard their mobile phone as first factor after identifying themselves with legacy digital IDs, (2) Identity Federation Server built with OpenID Connect that can allow other SMEs and government web services to utilize underlying FIDO UAF Authentication services, and (3) Authenticator built with Flutter to allow cross-platform UAF compatibility.

As of June 2021, both the UAF Server and UAF Authenticator already pass self-validation as tested by the FIDO conformance tool. The proof of concept (PoC) and trial run will be carried out in H2 2021 to collect benchmark metrics and to fine-tune the service. The ETDA's target is to roll out the solution in H1 2022.

United Kingdom

Department of Digital, Culture, Media and Sport (DCMS)

DCMS is responsible for digital identity policy and strategy for the UK economy. In February 2021, DCMS published the UK digital identity and attributes trust framework alpha for organizations that want to provide or consume digital identity and attribute products and services.

The trust framework has been published as a first stage industry prototype (or 'alpha') so that DCMS can test it with services, industries, organizations, and potential users.

The trust framework includes a variety of rules for organizations to follow, including the UK Government's good practice guides for "How to prove and verify someone's identity" (Good Practice Guide 45 or GPG 45 and relevant to the FIDO IDWG) and "Using authenticators to protect an online service" (Good Practice Guide 44 or GPG 44).

Cabinet Office

The Government Digital Service (GDS) is responsible for the development of digital identity strategy for government services. In May 2020, the GDS published updated guidance, "Using authenticators to protect an online service" (Good Practice Guide 44 or GPG 44). 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 is easy for someone to steal, guess or copy. A token is high quality if it has been independently tested to prove it meets industry standards, such as the Common Criteria guidelines, FIDO or NIST FIPS 140-2."

Additionally, the UK government's GOV.UK Verify has supported FIDO Authentication for several years, enabling citizens to securely access and transact online with government departments.

National Health Service

To support citizen access to healthcare services, the 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 NHS 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.

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.

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.

For more information on NHS deployment, please read the case study at: https://fidodev.wpengine.com/national-health-service-uses-fido-authentication-for-enhanced-login/.

United States

The United States federal government has recognized FIDO Authentication in a variety of policy and guidance documents.

U.S. Cybersecurity and Infrastructure Security Agency (CISA)

CISA has called FIDO the "gold standard" 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."

CISA's MFA guidance also includes a direct link to the FIDO Alliance website for more information. The full guidance is at https://www.cisa.gov/mfa.

CISA had previously recognized the importance of FIDO Authentication in a September 10, 2020 advisory recommending cyberattack remedies for election-related activities including the use of FIDO Authentication to thwart phishing attempts and account takeover.

The advisory, entitled "Actions to Counter Email-Based Attacks on Election-Related Entities", noted that 78 percent of cyber-espionage incidents are enabled by phishing. CISA makes specific recommendations on protecting against cyberattacks to aid organizations involved in election-related activities.

Among other recommendations, FIDO Authentication was highlighted to thwart phishing attempts and protect against account takeover for cloud email and other high-value services. Specifically, CISA cites FIDO2 security keys as a tool that campaigns and organizations can, and should, use to protect themselves. The advisory also recommends that, when available, campaigns and organizations should enroll users in advanced protection services such as Google Advanced Protection, which leverages FIDO security keys as a best practice over other two-factor authentication methodologies to protect workforces from account takeovers related to malicious attacks.

CISA's advisory can be found here.

The White House

The White House released a Federal Zero Trust Strategy for U.S. government agencies in 2022 that mandates phishing-resistant authentication and calls on agencies to use the FIDO2 standards, including Web Authentication (WebAuthn).

- For government enterprise applications – for agency staff, contractors, and partners – phishing-resistant MFA is required.
- For public-facing applications, phishing-resistant MFA must be an option offered to members of the public.

The Strategy dives into the weaknesses with legacy MFA based on OTP or push approaches, noting:

> MFA will generally protect against some common methods of gaining unauthorized account access, such as guessing weak passwords or reusing passwords obtained from a data breach. However, many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale.

The Strategy then details how FIDO2 standards can address these weaknesses, noting:

> Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks. The Federal Government's Personal Identity Verification (PIV) standard is one such approach. The World Wide Web Consortium (W3C)'s open "Web Authentication" standard, another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services.
>
> Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts. For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications.
>
> This requirement for phishing-resistant methods is necessitated by the reality that enterprise users are among the most valuable targets for phishing. That problem can be mitigated by providing those users with phishing-resistant tokens, including the PIV cards that agency staff and partners are generally issued.
>
> However, PIV will not be a practical option for some information systems and situations. Agencies are permitted under current guidance to use phishing-resistant authenticators that do not yet support PIV or Derived PIV (such as FIDO2 and Web Authentication-based authenticators) in order to meet the requirements of this strategy. To the greatest extent possible, agencies should centrally implement support for non-PIV authenticators in their enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities.

With regard to public-facing applications, the Strategy notes:

> Systems serving the general public may not yet be able to rely on phishing-resistant authentication alone in providing users access to online services, as some users of online Government services may have limited access to up-to-date devices and security technologies. At the same time, online public services are a major target for phishing attacks and account takeover, and many users will expect Government services to give them tools they can use to protect themselves. To equitably balance security and usability, public-facing Government systems need to offer users more options for authentication.
>
> To that end, public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication within one year of the issuance of this guidance. Meeting this requirement for the general public will mean providing support for Web Authentication-based approaches, such as security keys.

In discussing authentication standards, the Strategy calls out the role of the FIDO Alliance, noting:

> Web Authentication, also known as WebAuthn, was developed as part of the FIDO Alliance's FIDO2 standards, and is now published by the World Wide Web Consortium (W3C) as a free and open standard.

General Services Administration (GSA)

The 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. 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 FIDO2 Authentication standards. After reviewing FIDO2, GSA found that FIDO2's phishing resistance made it the most appropriate approach to address its security challenges.

Security was not the only factor in selecting FIDO2; cost was another. 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. The federal government does not sell or provision authenticators, but enables the use of authenticators that were previously provisioned.

For further information, please see a detailed case study highlighting GSA's support for FIDO2 at https://fidodev.wpengine.com/u-s-general-services-administrations-rollout-of-fido2-on-login-gov/.

National Institute of Standards and Technology (NIST)

In 2017, NIST updated its 800-63 suite of guidance, "Digital Identity Guidelines", which includes Enrollment and Identity Proofing (SP 800-63A), Authentication and Lifecycle Management (SP 800-63B), and Federation and Assertions (SP 800-63C). To support the guidance, NIST published an Implementation Resource Guide in 2020.

The Resource Guide highlights the use of FIDO U2F Authenticators in meeting Authentication Assurance Level 2 (AAL2) requirements for a single factor cryptographic device.

NIST also delivered on one of its tasks from the President's Executive Order (EO) on Improving the Nation's Cybersecurity, publishing a new guide on "Security Measures for EO-Critical Software Use." This NIST guidance focuses not on government, but on companies that are supplying software to the government – this is part of the U.S. government's focus on improving software supply chain security. It will apply to "all software designated as EO-critical software or to all platforms, users, administrators, data, or networks (as specified) that are part of running EO-critical software."

NIST & National Cybersecurity Center of Excellence (NCCOE)

In May 2019, NIST and the NCCOE published the practice guide "Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders (SP 1800-13)".

First responders need to access public safety information quickly and securely from a variety of devices, including laptops, tablets, mobile phones, and other portable devices. Given the sensitivity of the personally identifiable information (PII), criminal records, and protected health information (PHI), authentication is a major component.

The practice guide demonstrates how commercially available technologies, standards, and best practices implementing SSO, identity federation, and multi-factor authentication can meet the needs of public safety first responder communities when accessing services from mobile devices. FIDO's specifications are referenced throughout the guide.

Office of Management and Budget (OMB)

In 2019, the OMB issued memorandum M-19-17 updating the Federal Identity, Credential, and Access Management (FICAM) policy. The updated policy details innovating capabilities and updating Federal PKI to provide government with a trust framework and infrastructure to administer digital certificates and other authentication solutions, such as those based on public key cryptography. FIDO's specifications are based on public key cryptography.

The memo also updates the PKI shared service provider approach to enable strong government oversight of service providers, including procurement and cost controls through GSA acquisition solutions as applicable.

Drug Enforcement Administration (DEA)

In 2021 the DEA published an interim final rule (IFR) permitting prescriptions for controlled substances to be prepared by DEA-registered healthcare providers and electronically sent to pharmacists to be fulfilled for patients. The IFR contains strict requirements for identity proofing of providers and requiring multi-factor authentication to access electronic prescription software and when signing the controlled substance prescription. In April 2020, the DEA began the process of updating the IFR and issued a Request for Information (RFI) containing a series of questions on how providers are e-prescribing controlled substances, including the use of FIDO U2F Authenticators.

Resources for Government Departments and Agencies

FIDO Authenticator Lifecycle Management for IT Administrators

Guidance for IT administrators and Enterprise Security Architects considering deploying FIDO Authenticators across their enterprises and defining lifecycle management policies.

Considerations for Deploying FIDO Servers in the Enterprise

Intended for IT professionals and identity architects to guide them in choosing the right FIDO server implementation and deployment architecture when integrating and enabling FIDO Authentication in enterprise applications.

Multiple Authenticators for Reducing Account-Recovery Needs for FIDO-Enabled Consumer Accounts

When a service deploys FIDO Authentication, it must have a secure account recovery process to address lost, damaged, or stolen FIDO Authenticators. Requiring the user to register multiple authenticators to reduce the need for account recovery may be preferred compared to requiring the user to onboard again. This paper provides guidance on how to deploy FIDO Authentication with multiple authenticators.

Enterprise Adoption Best Practices – Integrating FIDO & Federation Protocols

Provides guidance to architects and developers on how to integrate FIDO Authentication and existing federation protocols, namely SAML and OpenID Connect.