

FIDO Alliance Input to the Drug Enforcement Administration (DEA)

Request for Comments on the Interim Final Rule for Electronic Prescriptions for Controlled Substances (EPCS)

June 2020

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on Docket No. DEA-2181, the Drug Enforcement Administration's (DEA) Request for Comments on the Interim Final Rule for Electronic Prescriptions for Controlled Substances (EPCS)

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 and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication.

Our 40 board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership.



Up front, it is worth noting that FIDO Alliance – and the FIDO MFA standards – did not exist when the DEA published its Interim Final Rule ten years ago. The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO Authentication standards over the eight years that have followed – has helped to transform the MFA market, addressing concerns about the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today FIDO standards are being used across banking, health care, government, and e-commerce to deliver authentication that is both more secure and also easier to use.

As we detail in this response, FIDO standards offer both DEA and the medical profession new tools to better minimize the potential for the diversion of controlled substance through misuse of electronic prescription applications. Furthermore, attackers have caught up with some of the requirements from the 2010 IFR, making it easier for them to compromise electronic prescription applications.

Given the focus of the FIDO Alliance on authentication, our comments here are largely focused on the portions of the request for comment that focus on authentication requirements in the interim final rule.

We have organized our comments in four parts:

1. Observations on current regulations and how technology has evolved over the last ten years
2. An introduction to FIDO Authentication and FIDO Alliance certification programs
3. Answers to specific DEA questions from the Request for Comments
4. Suggestions on ways DEA can ensure revised EPCS regulations stay current as technology and threat evolve

1. Observations on current regulations and how technology has evolved over the last ten years

The current EPCS regulations are outdated – creating security risks as regulations have not caught up with evolving threat vectors, as well as implementation barriers that create disincentives to physician adoption of EPCS.

Technology and threat are constantly evolving, and security policy needs to evolve with them. Unfortunately, the interim final rule locked industry into a set of regulations based largely on NIST publications that have since been updated and replaced – in some cases more than once.

The impact of this approach has been to preclude industry from implementing new security technologies that can better mitigate modern attack vectors on identity and authentication. The good news is that the identity and authentication markets have responded to the shortcomings of earlier approaches, and DEA can now point to newer technologies that can both increase security and be easier for physicians to use.

The table below outlines some of the key changes over the last 10 years:

2010	2020
<p>Malware on a device is a major concern – if authentication factors are embedded in a device, it might be taken over if compromised.</p> <p>This led to requirements from DEA and other agencies such as OMB that authentication tokens be physically separate from the device.</p>	<p>Phishing has replaced malware as the top threat – in large part thanks to the emergence of secure architectures in devices that use “restricted execution environments” to isolate and protect biometrics and cryptographic tokens used in authentication. These architectures ensure that even if a device is compromised with malware, the independence and security of these authentication factors are still protected.</p> <p>OMB and NIST have both repealed previous guidance and policy calling for physical separation of authentication tokens.¹</p>
<p>OTP is considered secure and is a “state of the art” authentication technology.</p>	<p>OTP is routinely phishable, as attackers have figured out ways to phish OTP codes from users. Attackers have also found ways to phish authentication based on push notifications.²</p> <p>The security community has begun to move away from OTP and other authentication tools based on “shared secrets.” Industry is shifting toward “high assurance” MFA where at least one factor is based on public key cryptography, and thus cannot be phished. Authentication using the FIDO standards is one such example.</p>
<p>Biometrics are still an early-stage technology and are not always considered reliable for authentication.</p>	<p>Biometrics have advanced significantly. It is rare to buy a laptop, tablet, or smartphone that does not include biometric technology – typically a fingerprint sensor or camera that can be used for face recognition.</p>

¹ See NIST ITL Bulletin for December 2014 on Derived PIV Credentials detailing how OMB will update guidance on remote electronic authentication” to remove OMB M-06-16 requirements that one factor be separate from the device accessing the resource, as well as OMB M-17-15, which formally repealed these requirements.

² Google (a FIDO Alliance member) discussed the extent of the problem in 2015 (see <https://www.youtube.com/watch?v=UBjEfpfZ8w0>), noting that these days, a “phisher can pretty successfully phish for an OTP just about as easily as they can a password” and noted their shift to FIDO hardware-based solutions as the way to stop these targeted phishing attacks. Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflect their experience with this technology.

2010	2020
<p>It is rare for a reliable, high-assurance biometric sensor and system to ship in a commercially available laptop, tablet, or smartphone.</p> <p>There is very little guidance on how to reliably use biometrics in an authentication system – DEA was among the first to create requirements.</p>	<p>Platform vendors and manufacturers have begun to use on-device biometric matching to replace passwords, as well as in MFA solutions like FIDO Authentication where a biometric match unlocks the private key of an asymmetric cryptographic key pair to deliver “single gesture” high assurance MFA.</p> <p>Commercially available biometric sensors certified against the FIDO Biometric Component Certification Program deliver a False Match Rate (FMR) of 1 in 10,000 – or 10x more accurate than current DEA requirements.³</p> <p>NIST has created guidance on use of biometrics in its updated digital identity guidelines (SP 800-63B), allowing for some limited use if certain requirements and guidelines are followed.⁴</p>
<p>MFA adds additional security – but at the expense of user experience. The additional cost, hassle and friction involved with using MFA creates disincentives to its adoption.</p>	<p>Industry has innovated to create MFA solutions such as FIDO that improve both security and user experience.</p> <p>FIDO Authentication delivers the core security benefit of PKI – (authentication based on asymmetric public key cryptography) without the hassles, complexities, and overhead traditionally associated with PKI.</p>

2. An introduction to FIDO Authentication and FIDO Alliance certification programs

As we detail in this paper, 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 presents identity practitioners with new options that improve security, privacy and usability.

FIDO is a global standard embraced by every major platform

Over the last five years, the global leaders in security, technology, banking, payments, health care, telecommunications, and government that collectively comprise the FIDO Alliance has delivered a comprehensive framework of open industry standards for multi-factor authentication (MFA) that addressed key security and usability shortcomings in previous MFA tools, and that 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, Aetna, Cigna, eBay, Dropbox, Salesforce and their peers around the world have deployed authentication solutions based on the FIDO standards; in total, FIDO solutions are available to protect more than 3 billion accounts worldwide.

³ See <https://fidoalliance.org/certification/biometric-component-certification/>

⁴ See pages 26-28 of <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>.

- 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.
- The W3C has finalized a formal new Web Authentication standard (WebAuthn)⁵ that is part of the FIDO2 standards. This standard enables FIDO functionality to be embedded in major browsers (i.e., Chrome, Edge, Firefox, Safari) – meaning that FIDO-standard MFA can be deployed for any web application without any significant burden on the part of an implementer.
- 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 730 products have been FIDO-certified – demonstrating a mature, competitive, interoperable authentication ecosystem. Many of these products are smartphones and laptops where FIDO Authentication is built in natively into browsers and platforms – meaning that implementers do not need to buy a separate technology to enable MFA.

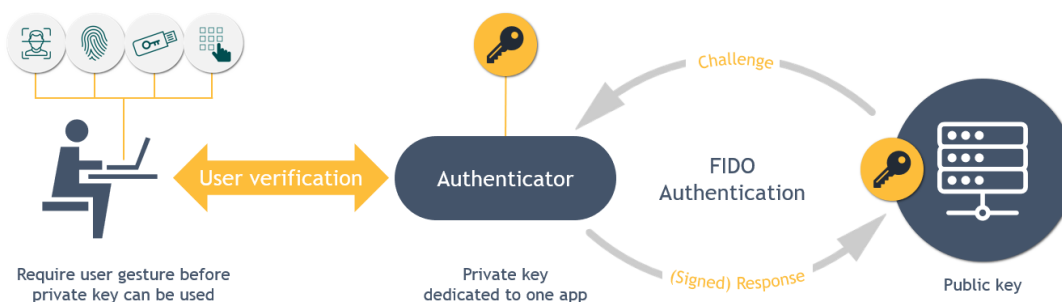
For example, Microsoft has embedded FIDO at the OS level in Windows 10, where it provides the basis for the Windows Hello passwordless login solution.⁶

And, Google has embedded support for FIDO in at 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.⁷

How FIDO Works

At its core, FIDO Authentication is based on the use of authentication certificates using asymmetric public key cryptography. Authentication keys can either be standalone “Security Key” devices or embedded inside devices like laptops or smartphones. Regardless of the form factor, a FIDO authenticator requires that the user makes some sort of gesture – touching the key, matching a biometric, or authenticating a PIN – before the private key can be used.

How FIDO authentication works



Sometimes FIDO Authentication is used as a second factor to augment passwords – this is how it is commonly used in the “Security Key” model popularized by Google and other firms.

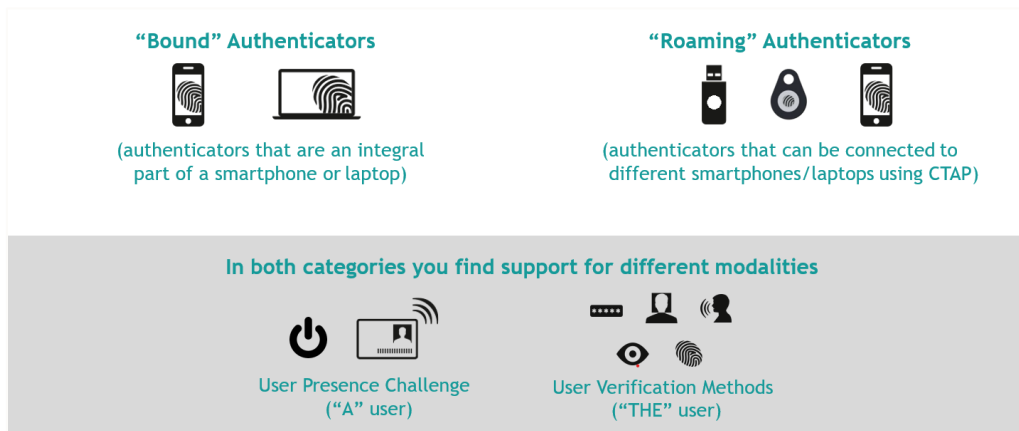
⁵ See <https://www.w3.org/TR/webauthn/>

⁶ 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/>

⁷ More details on the Google announcement are at <https://threatpost.com/google-ditches-passwords-in-latest-android-devices/142164/>

Sometimes FIDO Authentication is used to provide two separate factors to enable a true “passwordless” experience. For example, patients log into Aetna’s smartphone app by first authenticating their fingerprint or face on the device; that biometric factor then unlocks the cryptographic key.

As the graphic below details, the introduction of the FIDO2 standards is creating additional ways to use FIDO Authentication, including ways that the secure hardware in smartphones themselves can be used as Security Keys.



FIDO Certification Programs

The widespread adoption of FIDO Authentication has been fueled in large part by its robust certification programs that test and confirm that FIDO solutions adhere to FIDO standards.

Note that the FIDO certification program is the largest and most recognized certification program for authentication products in the world. It has been developed over several years by both industry and government (in the U.S., NIST, DoD, NSA, Treasury and GSA are all FIDO Alliance members), ensuring that the certification requirements meet the needs of both the private and public sectors.

In Australia, the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) published guidance on *Implementing Multi-Factor Authentication*⁸ that recommended “For maximum security and effectiveness...use (FIDO) U2F security keys that have been certified to the latest U2F specification version.” The guidance then referenced the FIDO Alliance’s website that lists all FIDO Certified products.⁹

ACSC’s reference to the FIDO certification program has been helping implementers in Australia by 1) steering them to higher assurance MFA (rather than SMS or OTP) and 2) steering them to a certification program that has certified more than 730 authentication products, demonstrating a mature, competitive, interoperable authentication ecosystem. DEA recognition of the FIDO certification program as one such industry program would have a similar positive effect.

In recent years, FIDO Alliance has moved beyond conformance testing to launch new certification programs testing the security of FIDO authenticators, as well as biometric components.



Security Certification Program

FIDO’s Certified Authenticator Level program introduces Authenticator Security Requirements to the FIDO Certification Program, looking at how authenticators protect cryptographic key material. This program was launched, in part, to satisfy requests from high assurance communities including government for additional security certifications in FIDO Authenticators.

⁸ See *Implementing Multi-Factor Authentication* at https://acsc.gov.au/publications/protect/multi_factor_authentication.htm

⁹ See <https://fidoalliance.org/certification/fido-certified-products/>

As detailed below, FIDO has established six different levels of security requirements.¹⁰

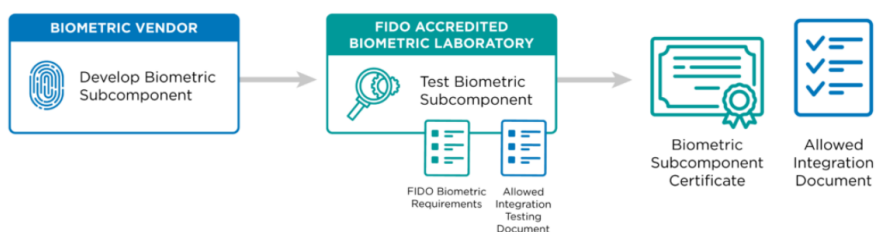
	SAMPLE DEVICE HARDWARE & SOFTWARE REQUIREMENTS		DEFENDS AGAINST	
	Protection against chip fault injection and invasive attacks	L3+	Chip level attacks on captured devices	
	Circuit board potting, package on package memory, encrypted RAM...	L3	Circuit board attacks on captured devices	
	Device must support allowed Restricted Operating Environment (ROE) (e.g., TEE, Secure Element...), or intrinsically be an ROE (e.g., a USB token or Smart Card...)	L2+	Device OS compromise	
		L2		
	Any device HW or SW	L1+	White Box Cryptography to defend against OS compromise	
		L1	Phishing, server credential breaches and MITM attacks (better than passwords)	

Biometric Component Certification Program

In 2018, FIDO launched a Biometric Component Certification Program, the first independent program to validate biometric technology performance claims that in the past led to concerns over variances in the accuracy and reliability of these solutions.

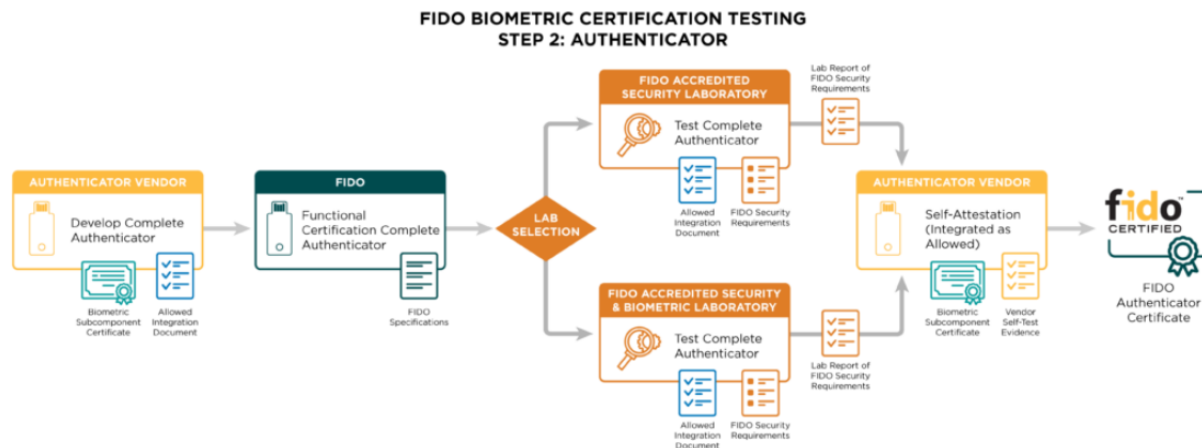
The program utilizes accredited independent labs to certify that biometric subcomponents meet globally recognized performance standards for biometric recognition performance and Presentation Attack Detection (PAD) and are fit for commercial use. It certifies biometric sensors with a false match rate of 0.0001 or lower (10 times more accurate than current DEA requirements) and was developed in part with input from NIST.¹¹

FIDO BIOMETRIC CERTIFICATION TESTING STEP 1: BIOMETRIC SUBCOMPONENT



¹⁰ See <https://fidoalliance.org/certification/authenticator-certification-levels/> for more details.

¹¹ Details at <https://fidoalliance.org/certification/biometric-component-certification/>



FIDO Alliance would be happy to brief DEA on any or all of our certification programs.

3. Answers to specific DEA questions from the Request for Comments

In response to DEA's specific questions, we offer the following responses to Questions 1, 2, 7 and 8:

Question 1:

Is there an alternative to two-factor authentication that would provide an equally safe, secure, and closed system for electronic prescribing of controlled substance while better encouraging adoption of EPCS? If so, please describe the alternative(s) and indicate how, specifically, it would better encourage adoption of EPCS without diminishing the safety and security of the system.

Answer: 2FA is still the most effective authentication technology for safe and secure EPCS solutions – but all 2FA is not the same. DEA should update its regulations to recognize how 2FA has evolved.

1. Requirements that authentication factors be physically separate from the device running the EPCS application have become outdated.

The emergence of secure architectures in devices that use “restricted execution environments” to isolate and protect biometrics and cryptographic tokens used in authentication enable to independent authentication factors to be contained in a single device. These architectures ensure that even if a device is compromised with malware, the independence and security of these authentication factors are still protected.

As noted on page 3, this innovation has led to OMB and NIST both repealing previous guidance and policy calling for physical separation of authentication tokens.

2. To the point above, the biggest threat to compromise of 2FA is not whether authentication factors are physically separate from a device, but rather whether there are phishable. OTP codes are shared secrets, and thus even if they are generated in a secure FIPS 140 validated hardware token, the code can be compromised if a user is tricked via a phishing attack into entering the code into a hostile site.

Are practitioners using universal second factor authentication (U2F)? If so, how (e.g., Near-Field Communication (NFC), Bluetooth, USB, or Passwordless)?

Answer: We note that FIDO Alliance created the U2F standard. While U2F is still widely used, the emergence of a newer version of FIDO standards known as FIDO2 has started to replace FIDO U2F, and provided a wider array of ways to use FIDO authentication both as a second factor to augment passwords, as well as to enable passwordless

authentication.

FIDO2 contains two specifications:

- Client-to-Authenticator Protocol (CTAP) – governing how a computing device (client) communicates with an authenticator (such as a Security Key)
- Web Authentication (WebAuthn) – governing how FIDO is used in browser-based applications, and how a FIDO authenticator interacts with the browser.

Collectively, FIDO2 allows authentication devices to work in a way similarly to FIDO U2F tokens, but creates additional options as well.

To date we have not seen significant adoption of U2F or other FIDO standards in EPCS applications for two reasons:

- The FIPS 140 requirement: to date, only one vendor has taken a FIDO U2F security key through the FIPS 140 process, largely because commercial customers have not demanded it.
- Form factor challenges: the one FIPS 140 validated FIDO Security Key only supports a USB interface, which has proven impractical for physicians looking to run EPCS applications on a mobile device. We note that at least one vendor is taking a NFC-enabled FIDO security key through the FIPS 140 process right now, and the emergence of that product may lead to higher adoption of FIDO security keys in the EPCS market.¹²

Are practitioners using cellular phones as a hard token, or as part of the two-factor authentication? Is short messaging service (SMS) being used as one of the authentication factors used for signing a controlled substance prescriptions?

Answer: Based on our knowledge of the EPCS market, we believe that use of cellular phones as hard tokens is widespread in the EPCS market. Most commonly by using the phone as a hard token either with an OTP app or one that delivers a second factor via push notification.

As noted previously, both of these authentication approaches may be susceptible to phishing attacks.

Question 2:

As discussed, the IFR requires that a CSP or CA conduct identity proofing at Assurance Level 3 of the NIST SP 800-63-1, “Electronic Authentication Guideline.” As noted, because of updates in technology, NIST SP 800-63-3, “Digital Identity Guidelines,” now provides the most current relevant identity proofing guidelines. And, under NIST SP 800-63-3, the relevant assurance level is Identity Assurance Level 2. DEA believes that the ability to conduct remote identity proofing allowed for in Assurance Level 3 of NIST SP 800-63-1 and Identity Assurance Level 2 of NIST SP 800-63-3 ensures that practitioners in rural areas are able to obtain an authentication credential without the need for travel. DEA further believes that application providers work with CSPs or CAs to direct practitioners to one or more sources of two-factor authentication credentials that will be interoperable with their applications. Additionally, an IFR provision, 21 CFR 1311.105, requires that a CSP providing EPCS authentication credentials be approved by the General Services Administration Office of Technology Strategy/Division of Identity Management to conduct identity proofing at Assurance Level 3 or above of NIST SP 800-63-1 (i.e., Identity Assurance Level 2 or above of NIST SP 800-63-3). DEA has received questions asking for clarification of this requirement. DEA is seeking comment on this approach to identity proofing, as well as any more comments about whether clarification of the language regarding CSP approval would be helpful.

¹² See <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Modules-In-Process/IUT-List>

Answer: We offer two points for consideration:

1. GSA has for all purposes suspended its “Trust Frameworks Provider” program for certifying private sector identity solutions, so the requirement for CSPs to be approved by GSA no longer aligns with current GSA programs.

OMB in M-19-17 told GSA to work with NIST to create a new approach for certifying identity solutions, and work is underway in those two agencies to determine how they will proceed.¹³ Our understanding is that both agencies are considering whether the government itself will need to certify identity solutions, or whether in some cases government will be able to point to commonly recognized industry certification programs such as those run by FIDO Alliance.

2. On the identity proofing side, FIDO Alliance recently launched a new Identity Verification and Binding Working Group (IDWG) focused on creating both performance criteria for remote identity verification solutions, as well as a certification program – backed by independent labs – to test the performance of vendor solutions against these criteria.

This new working group is focused on tools used to 1) capture and authenticate physical identity documents such as driver’s licenses and passports, and 2) capture facial images and match them to the photo on those documents. The idea is to move from knowledge-based approaches to remote identity proofing to ones that are possession-based.

The certification program is still being created, but when launched, it may provide a tool which DEA and the EPCS community may be able to leverage.

Agencies including NIST, GSA and Treasury are participating in the IDWG through the US government’s membership. Should DEA wish to engage, you would be welcome.

Question 7:

DEA is generally seeking comment on any aspects of the IFR or other EPCS areas where further clarification would be helpful. For example:

Are there problems using two-factor authentication due to the method used to complete verification (e.g., prohibited or limited cellular service, restriction on external USB devices, offline system access)?

Has two-factor authentication caused barriers to efficient workflows?

Answer: As we have detailed elsewhere in this response, there are a number of barriers to using traditional, first-generation two-factor authentication, given challenges with usability, form factors, and specific DEA requirements.

FIDO Alliance is one place where industry and government have partnered together to innovate over the last several years to address these barriers, creating and delivering a comprehensive framework of open industry standards for multi-factor authentication (MFA) that addressed key security and usability shortcomings in previous MFA tools, and that provide identity practitioners with new options for crafting digital identity solutions.

Even more notable, many FIDO implementations do not require consumers to get any new authentication product at all – support for the FIDO standards is now built in to laptops, smartphones, and browsers. Every device running Android v7 or higher is now a FIDO-certified authenticator, as is every device running Windows 10. Apple has not yet gotten iOS certified, but they joined FIDO Alliance earlier this year and have been rolling out additional support for FIDO in iOS over the last year. Safari, Chrome, Firefox and Edge browsers also all ship with built-in support for

¹³ Per <https://www.nist.gov/topics/identity-access-management/roadmap-nist-special-publication-800-63-3-digital-identity>, “OMB Policy Memo M-19-17 assigned the Department of Commerce the responsibility to develop criteria for the “accreditation” of products and services to meet designated levels of assurance in SP 800-63-3. NIST will develop conformance criteria that can be used to determine if products and services meet/conform to the requirements found within SP 800-63-3.”

FIDO Authentication.

The practical impact: the majority of Americans are already carrying FIDO-capable devices today. By allowing for use of FIDO Authentication in updated EPCS regulations, DEA would make it much easier for the health sector to turn on support for strong, multi-factor authentication.

Question 8:

Many institutions have implemented biometrics as part of their authentication credentialing for electronic applications. DEA is seeking comments in response to the following questions:

What types of biometric authentication credentials are currently being utilized (e.g., fingerprint, iris scan, handprint)?

Answer: Based on our awareness of the market, we believe that biometrics are not being widely used in EPCS applications outside of desktop applications, in large part because the requirements in the regulations (especially adherence to NIST SP 800-76-1) are so restrictive that they make it difficult to use biometrics in mobile devices in a practical fashion.

Outside of EPCS, fingerprint and face recognition are the most commonly used biometrics in digital authentication, followed by iris recognition. These days, most laptops, tablets and smartphones come with one or more of these sensors built in.

How has the implementation of biometrics, as an option for meeting the two-factor authentication requirement, benefited the EPCS program?

Are there alternatives to biometrics that could result in a greater adoption rate for EPCS while continuing to meet the authentication requirements? If so, please describe the alternative(s) and indicate how, specifically, it would be an improvement on the authentication requirements in the IFR.

Answer: Per our previous statement, we don't think biometrics are significantly benefitting the EPCS program, in large part because the IFR requirements to use them are not aligned with modern security or performance requirements. While biometrics can offer great convenience and security, the EPCS community will not be able to take full advantage of biometrics until these requirements are modernized and revised.

To that point: there are not alternatives to biometrics that would result in a greater adoption rate for EPCS, but a refreshed approach to the requirements for biometrics in 21 CFR §1311.116 would allow modern biometric technology to be more widely used.

The EPCS regulations were written in 2010 – long before it was common for high-performance biometric sensors for fingerprint and face to be included in smartphones, tablets, and laptops. Today, Apple, Google and Microsoft all ship devices and operating systems that allow these sensors to be used in lieu of passwords, or as a “key” to unlock and automatically enter a password stored in protected environments in the device. They also use biometrics as an initial authentication factor to unlock cryptographic keys for authentication, enabling true multi-factor password-less authentication. This latter use case is a commonly-used implementation of the FIDO standards.

While many of the 2010 biometric requirements can be met by modern commercial computing devices that contain integrated biometric sensors, the one requirement that is not supported by biometric systems in these devices is the requirement for biometric subsystems to conform to NIST SP 800-76-1. Not only is this NIST document outdated – having been replaced in 2013 by NIST SP 800-76-2, but it is heavily focused on the technical requirements for capturing biometrics for inclusion on a government issued Personal Identity Verification (“PIV”) smart card. These PIV requirements are not aligned with what is commonly seen in commercially available biometric systems embedded in smartphones, tablets and laptops. Thus, their use would not be allowed under the current regulations.

This is disappointing, given that there are commercial, on-device biometric systems that have been certified as meeting accuracy specifications that are ten times stronger than the false match rate of 0.001 or lower called for in the EPCS regulations. For example, the FIDO Alliance’s Biometric Component Certification Program – which was developed with assistance and inputs from NIST – certifies biometric sensors with a false match rate of 0.0001 or lower and is backed by testing from independent security labs. However, this certification program is designed around testing commercial on-device biometric sensors, not ones that are used to integrate with PIV cards.

Two things DEA could do to promote the increased use of biometrics while also improving the security of biometrics used in EPCS systems:

1. Remove the requirement for compliance with NIST PIV biometric requirements and instead point to biometric requirements outlined in SP 800-63B.

The 2010 DEA regulation was ahead of its time in allowing the use of biometrics as an authentication factor. At the time, NIST had decided that biometrics should not be used as an authentication factor because biometrics were not secrets – and thus could be captured or replayed by an attacker. NIST also had concerns about the ability to measure authentication strength of biometric solutions.

Today, NIST has put out detailed requirements and guidance in SP 800-63-3 on how to use biometrics in a way that mitigates many of their original concerns. Much of this was driven by work NIST led in 2016 around Strength of Function for Authenticators (SOFA) with a focus on SOFA-Biometrics (SOFA-B).

One reason NIST stated they changed their approach was “due to increased availability of biometric sensors in the consumer space.”¹⁴ The way in which biometrics such as fingerprint and face have become ubiquitous in most consumer devices has transformed the authentication landscape.

2. Recognize external biometric certification programs that meet DEA performance requirements, such as FIDO Alliance’s Biometric Component Certification Program.

4. Suggestions on ways DEA can ensure revised EPCS regulations stay current as technology and threat evolve

One theme that should be apparent in our response is that technology and threat have both evolved significantly over the last ten years – and the IFR has not kept pace.

Going forward, we believe DEA should consider an approach to EPCS regulations that avoids locking down technical requirements in regulations. We suggest that a better approach would be for DEA to reference the latest version of NIST SP 800-63 or its successor. DEA could then allow regulated entities 18 months after a new version of SP 800-63 is published to update systems to achieve compliance. This approach would allow DEA to create a regulatory structure for EPCS that would refresh to meet new threat vectors without having to promulgate a new regulation.

Note that such an approach would not preclude DEA’s ability to create regulations that vary from the NIST guidance. If DEA objected to a proposed change by NIST, it could always respond with its own regulation to counter that aspect of the NIST guidance. However, our assumption is that the majority of NIST revisions to SP 800-63 will align with DEA requirements, and this approach would let those be reflected in the regulations without any further regulatory action.

We greatly appreciate DEA’s consideration of our comments. We look forward to further discussion with DEA on this topic and would welcome the opportunity to answer any questions.

¹⁴ As detailed in <https://www.nist.gov/blogs/cybersecurity-insights/sofa-talk-strength-function-authenticators-framework-now-open-comment>

In addition, if it would be helpful, FIDO Alliance would be happy to brief DEA staff on FIDO Authentication and certification programs, and dive into more technical details on how they work.

Finally, we note that the US government is a member of the FIDO Alliance, and as part of that membership, DEA would be welcome to engage in FIDO working groups and discussions as a FIDO Alliance member. NIST, NSA, DOD, GSA and Treasury Department representatives all participate in the Alliance today, as do officials from other countries including the UK, Germany, Australia, South Korea and Taiwan.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.