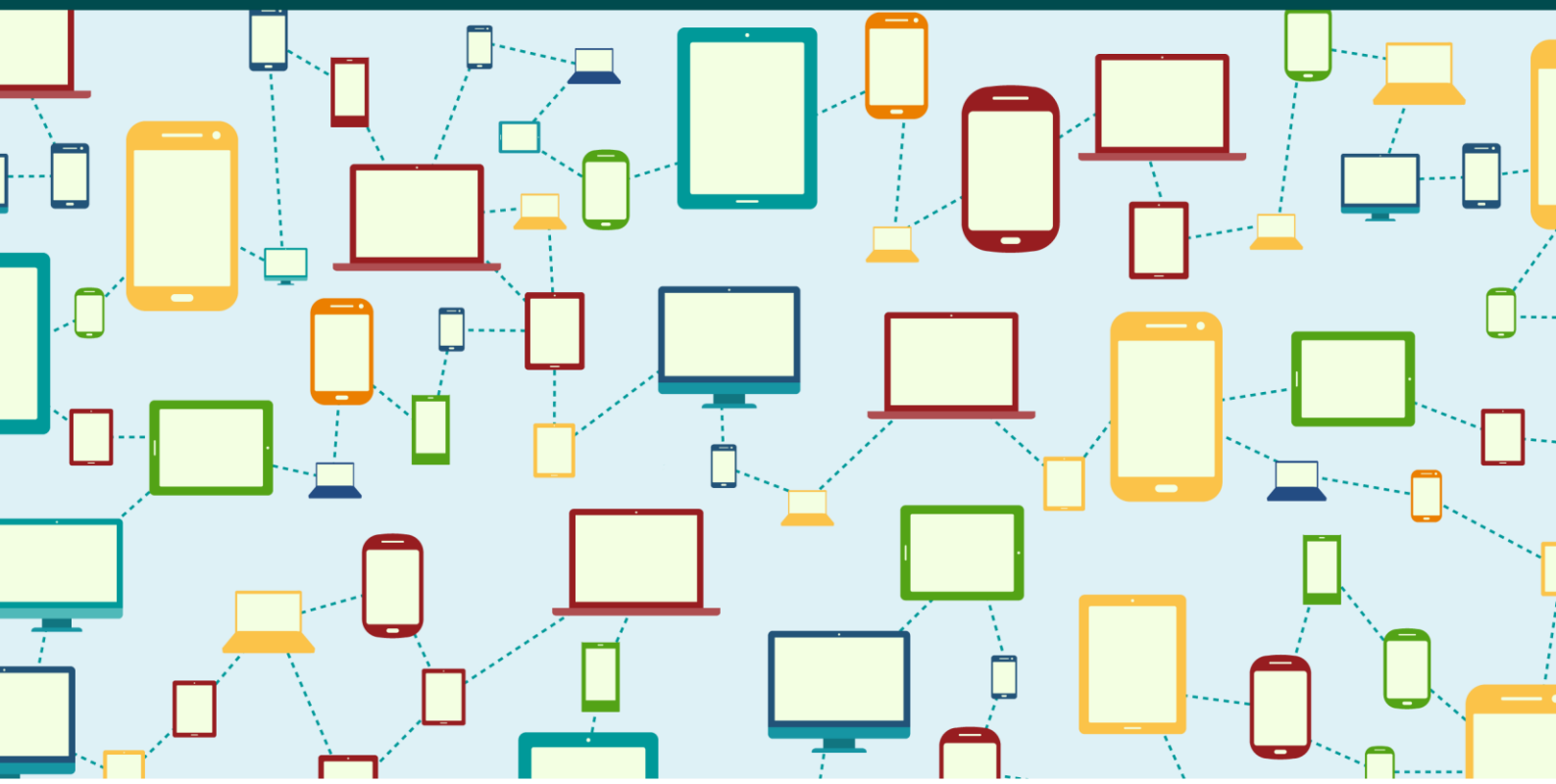
fido alliance | simpler stronger authentication



FIDO Alliance White Paper: Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies

Abstract

Governments and businesses around the world are looking to enhance Public Key Infrastructure (PKI)-based authentication systems with complementary, comparable technologies such as those built around the FIDO Alliance specifications. This approach can extend the benefits of authentication rooted in public key cryptography to a wider array of applications and users without sacrificing the well-known benefits of PKI.

This paper outlines how an expanded authentication ecosystem incorporating both PKI and FIDO authenticators can be incorporated across the U.S. government – enabling the U.S. to more effectively secure digital assets by embracing a wider array of strong, cryptographic authentication technologies beyond the PKI-based Personal Identity Verification (PIV) cards that are commonly used today. An interoperable infrastructure – leveraging FIDO Alliance specifications and PKI – could augment the current base of PIV credentials to more efficiently converge agencies with the goals of HSPD-12.

Introduction

In 2016, the U.S. Commission on Enhancing National Cybersecurity[1] highlighted the importance of identity and cybersecurity in its recommendations for the incoming President, writing:

> *"An ambitious but important goal for the next Administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack."*

As part of this, the Commission recommended a specific "Short Term Action Item" – that all agencies require the use of strong authentication across all government systems – and pointed out that the tools used to fulfill this requirement should not be limited to the government's PKI-based Personal Identity Verification (PIV) credentials. Instead, the Commission recommended that when it comes to authentication:

> *"The requirements should be made performance based (i.e., strong) so they include other (i.e., non-PIV) forms of authentication, and should mandate 100 percent adoption within a year."*

Of note, the U.S. government's FY 2017 FISMA Metrics[2] specifically allow agencies to use non-PIV solutions for both privileged and unprivileged users, noting that agencies will be measured on how well they are protecting systems by looking at:

> *"Number of users technologically required to log onto the network with a two-factor PIV card or other NIST Level of Assurance (LOA) 4 credential."*

While 100% PKI authentication, via PIV (or its Defense Department counterpart, the Common Access Card (CAC)), has proven difficult to achieve, a move to additional authenticators does not mean that agencies must forego the benefits of using asymmetric, public-key (PK) cryptography for authentication.

As this paper details, authentication solutions using specifications crafted by the members of the Fast Identity Online (FIDO) Alliance present one of the best options for agencies who need to complement PKI with other strong authentication approaches. The security characteristics of the FIDO specifications have been evaluated by NIST and included as a valid LOA4[3] authenticator in the Draft NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management.

There are compelling reasons for agencies to look to FIDO solutions aside from its security characteristics: its standards-based approach, adoption by key industry players, ease of use, and privacy-respecting architecture and design. FIDO's lightweight approach to asymmetric public-key cryptography offers agencies a way to extend the security benefits of public-key cryptography to a wider array of applications, domains and devices – especially where traditional PKI has proven difficult or impossible. To be clear, FIDO is not a replacement for PKI but rather complements it, enabling greater number of users and applications to be protected using asymmetric encryption. This is especially important in situations where the alternative has been username and password.

[1] https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf

[2] https://www.dhs.gov/sites/default/files/publications/FY%202017%20CIO%20FISMA%20Metrics-%20508%20Compliant.pdf

[3] In the draft revision of NIST SP 800-63-3, NIST uses the term Authenticator Assurance Level (AAL) to indicate the strength of the authentication mechanism. "AAL3" is equivalent to OMB M-04-04 "LOA 4." https://pages.nist.gov/800-63-3/sp800-63b.html

In addition, this approach can allow agencies to abide by the original intent of the 2004 directive that created the PIV (HSPD-12) – achieving improved security metrics for privileged and non-privileged network and application access – while also enhancing security by streamlining integration challenges and delivering an enhanced user experience.

Why New Options Are Important

PKI – while secure – has also presented a number of challenges and shortcomings in implementation and deployment. As a result, there are still many spots where strong authentication is not ubiquitous, including:

1. Legacy systems where PIV/CAC (or PKI) can't be easily integrated: PKI is complex to implement, which has hindered adoption of PIV-based authentication and limited the number of applications that are PKI-enabled. NIST has previously addressed this issue, noting in its *"Best Practices for Privileged User PIV Authentication"* cybersecurity white paper4 that there are some valuable non-PKI approaches to leverage a primary credential without directly PK-enabling individual applications and systems.
2. Not everyone is required to get a PIV5. For example, many high risk employees and contractors, such as those overseas or deployed at laboratory or medical facilities, legitimately do not have a PIV. At best they get an LOA3 authenticator; more commonly, they only get a username/password, or some other proprietary one-off credential that does not interoperate across their agency or with other agencies. Likewise, employees serving undercover may not be in a position to carry an ID card that says "US Government."
3. Mobile devices. Government has struggled to use PIV cards with mobile devices; among other things, most mobile devices lack traditional smart card readers, and efforts to leverage NFC for mobile authentication have struggled. In part because of these challenges, the U.S. government crafted the Derived PIV Credential (DPC) initiative6 – focused on extending the security model of PKI to mobile devices. While launched in 2014, DPC is still in early adoption mode and has proven complex to deploy. In practice, this means that millions of mobile devices across the U.S. government are not protected with strong authentication.
4. Meanwhile, the mobile devices the U.S. government is purchasing increasingly have support for FIDO specifications built into them7 – meaning federal employees have strong mobile authentication capabilities that are not in use because of the restriction that derived credentials are "PIV interoperable" or PKI-based. A simple change to this paradigm can markedly improve the federal cybersecurity posture.
5. Cloud applications. More and more agencies are shifting to the cloud and SaaS-based applications, many of which do not support PIV.

While the challenges with PKI persist, the default guidance to most agencies over the last decade has been "PIV or bust" – which has had the practical effect of leaving` many devices and applications protected with nothing more than a password. In a post-OPM-breach world, that is unacceptable.

[4] http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

[5] Per OMB Memorandum M-05-24

[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

[7] More than 300 FIDO-certified products are in the marketplace today, see https://fidoalliance.org/certification/fido-certified-products/

While PIV should remain the credential of choice for eligible employees or contractors, in instances where PKI authentication is not pragmatic, alternatives should exist. Given the limitations of non-PKI authentication tools that rely on antiquated, phishable "shared secrets," any PKI alternative should be one that addresses the challenges described above while still leveraging asymmetric, public key cryptography.

The FIDO Alliance specifications – supported by more than 300 certified products – represent the best alternative to complement the PIV/PKI model and get to 100% strong authentication.

What is the FIDO Alliance?

The Fast Identity Online (FIDO) Alliance was formed in 2013 to revolutionize online authentication by developing open, interoperable industry standards that leverage proven public key cryptography for stronger security and device-based user verification for better usability. Today FIDO has more than 250 members representing a "who's who" in information technology, communications, hardware and software manufacturers, finance, health care, government and other sectors.

Through the collaborative efforts of FIDO, new standards and specifications have emerged that enable strong, easy-to-use authentication to be built into devices such as computers, tablets and smartphones. Today, thanks to the FIDO specifications, many devices running major operating systems such as Windows, Android and iOS can support issuance of a strong, multi-factor credential – built around asymmetric, public key cryptography – as part of the device itself.

In a typical deployment of these standards, a user swipes a finger, speaks a phrase, or looks at a camera on a device to login, pay for an item, or use another service. Behind the scenes on that device, the biometric is used as an initial factor to then unlock a second, more secure factor: a private cryptographic key that works "behind the scenes" to authenticate a user to the service. Since biometrics and cryptographic keys are stored on local devices and never sent across the network – eliminating shared secrets – user credentials are secure even if service providers get hacked, thereby eliminating the possibility of scalable data breaches.

FIDO solutions can alternately be deployed via a standalone "security key" token that contains a chip similar to the secure hardware embedded in devices. With the security key architecture, a user can use a single token across several different devices, leveraging common interfaces such as USB, NFC and Bluetooth.

FIDO standards are currently being used to enable simpler, stronger authentication in offerings from Google, PayPal, Bank of America, NTT DOCOMO, BC Card (Korea), Microsoft, Dropbox, GitHub, AliPay, eBay, Samsung, FaceBook, and other leading firms. In each of these deployments, end-users do not have to know how the authentication works or why it's more secure – they are getting login experiences that are easier to use, with great security baked in behind the scenes.

The FIDO approach has been embraced by the World Wide Web Consortium (W3C), which is expected to finalize a formal new "Web Authentication" standard built on FIDO specifications in 2017. The emergence of this new standard, combined with the wide industry and government support of the growing FIDO ecosystem, makes it an important tool in efforts to improve authentication.

Sidenote: HSPD-12 envisioned an array of solutions

As background, the U.S. government's creation of the PIV program was launched in August, 2004 when President Bush signed Homeland Security Presidential Directive (HSPD) 12, entitled "Policies for a Common Identification Standard for Federal Employees and Contractors."

Like many HSPD's, a primary focus was around eliminating terrorist attacks – in this case, addressing the concern that "Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities" created significant risk. The directive called for the creation of a "mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors" and directed the National Institute of Standards and Technology (NIST) to create a standard solution that agencies would use to implement HSPD-12.

Note that HSPD-12 did not call for or mandate any specific technology, nor it did it state that the standard solution had to be limited to only one type of technology. On this latter point, HSPD-12 actually envisioned the use of multiple solutions to achieve the core objective, stating:

"The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application."

To that point, the directive focused on performance standards for *"Secure and reliable forms of identification"* – stating that this meant purposes of this directive means identification that:

(a) is issued based on sound criteria for verifying an individual employee's identity;

(b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

(c) can be rapidly authenticated electronically; and

(d) is issued only by providers whose reliability has been established by an official accreditation process.

In 2005, NIST issued FIPS 201, calling for the creation of Personal Identity Verification (PIV cards) – smart cards that used PKI for authentication. Since that time, the PIV card has been the "gold standard" for authentication in the U.S. government.

While there were good reasons in 2005 to limit the HSPD-12 standard to a single technology, twelve years have passed, and authentication technology has evolved and improved significantly – creating an opportunity for agencies to leverage the flexibility that was originally called for in the 2005 directive.

As this paper details, the emergence of FIDO Alliance specifications – supported by more than 300 certified products – provides a unique opportunity for the U.S. government to diversify the types of solutions used for enterprise authentication, while still staying true to its commitment to authentication solutions rooted in asymmetric, public key cryptography.

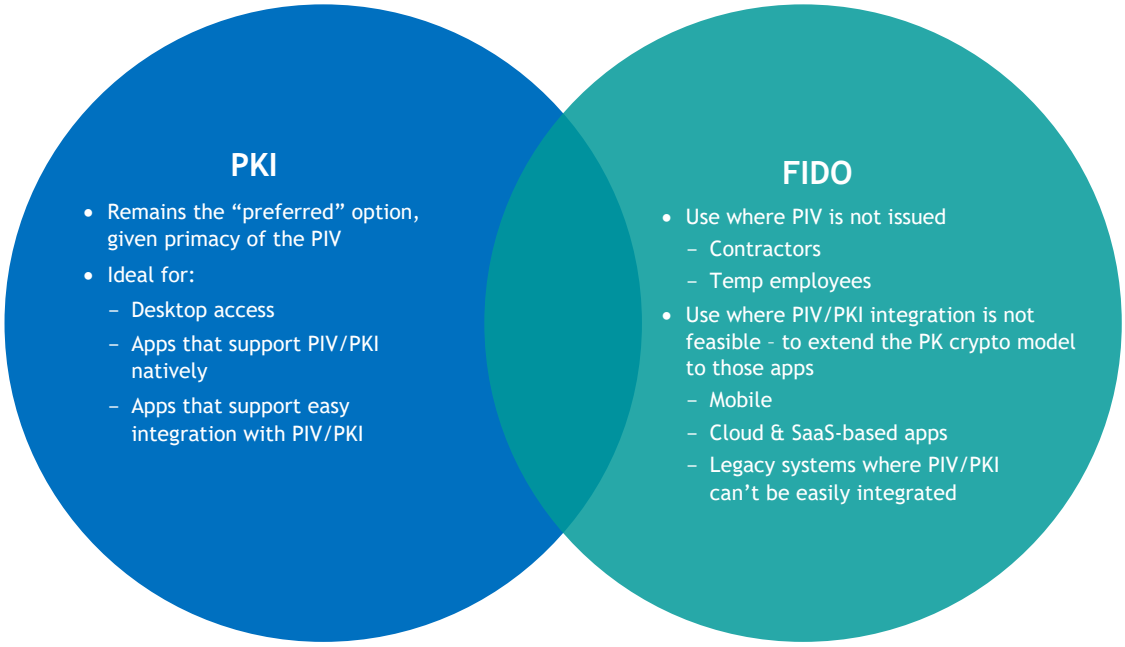
How can FIDO and PKI be used in a common identity ecosystem?

Much as the Derived PIV Credential (DPC) program allows for a separate PKI certificate to be issued by proving possession of a PIV Card, the DPC workflow specified in NIST 800-157[8] could also be used to issue a FIDO public/private key pair, linked to the same identity record the PIV card is linked to. The primary difference is that the key pair is not part of a "full" public key infrastructure, but rather a "lightweight" key pair.

The benefits of FIDO-inclusive approach are to offer additional authentication solutions that are easier to use and easier to integrate with legacy applications, but still retain the core security associated with asymmetric public key cryptography.

Relying Parties in government would be free to choose which type of technology makes most sense for a particular application. And given that many agencies already employ Web Access Management (WAM) tools for single sign-on (SSO) or PK-enablement of non-PK applications, allowing FIDO authenticators to be used alongside PKI in these tools can make it much easier to integrate with many agency applications.

Moreover for the portion of the government ecosystem that is not required to get a PIV, FIDO offers an alternative that is cheaper to issue and maintain and easy to use – ensuring that individuals have at least some sort of strong authentication based on public key cryptography.



Working Together to Achieve HSPD-12

Once a decision is made to expand the range of authenticators beyond PIV, the most important aspect is to ensure that the infrastructure is in place to support this expanded ecosystem.

The federal government has embraced federation and standard profiles such as SAML[9] to assert identity across agency boundaries – providing alternatives to PKI. An approach rooted in an interoperable federation allows any authenticator, such as PKI and FIDO, to achieve – and expand upon – the original goals of HSPD-12 and the policies that underpin it. Namely: Allowing employees and contractors to use their government issued or approved credential everywhere in and out of their sponsor agency.

[8] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf
[9] https://www.idmanagement.gov/IDM/s/article_search_detail?KID=ka1t0000000TND6AAO&Type=Site_Article__kav

- For example, a Justice Department employee (if authorized) can log into a GSA system with her Justice-issued PIV card.
- Or, a Department Energy (DoE) contractor – who is actually an employee of a private company – uses his FIDO credential to access the DoE VPN and then browses to a SaaS-based shared service hosted by another agency to enter time.

This solution is agnostic to the type of authenticator individuals use at their home agency, and would support wider deployment and interoperability of credentials.

The proposal discussed herein would achieve the goal of allowing home agencies to issue other authenticators when the PIV is not required, per OMB M-05-24. It also allows for agencies to move beyond user names and passwords for those that are not PIV-eligible, representing a significant enhancement to the security of authentication events.

Conclusion

There is an opportunity today to leverage what already exists within agency infrastructures to achieve interoperability among a range of LOA4 authenticators. PIV remains the gold-standard, and will remain a core component of the federal enterprise. Augmenting PIV solutions with FIDO will improve cyber hygiene across the Federal enterprise and help agencies better adhere to the goals of HSPD-12.