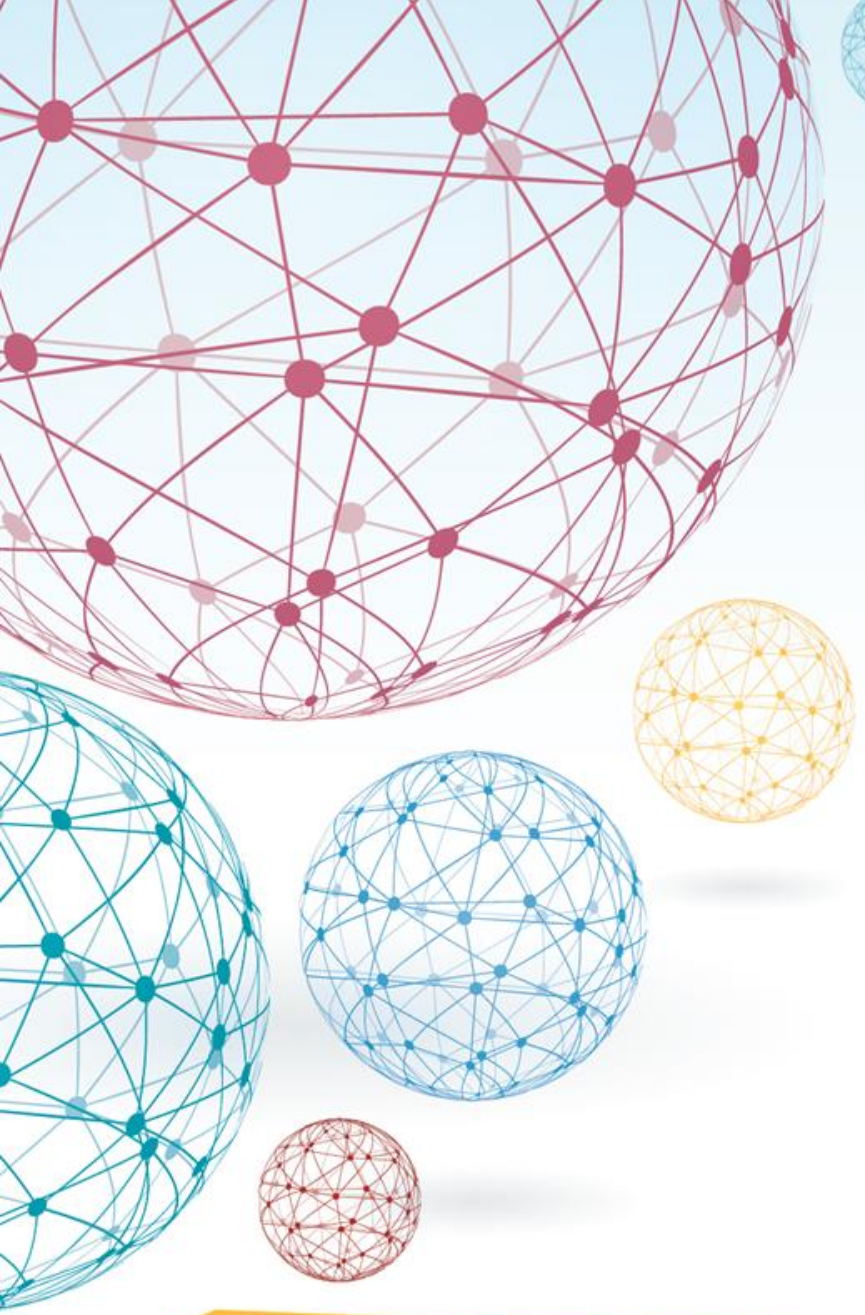


FIDO AS REGTECH – ADDRESSING GOVERNMENT REQUIREMENTS

Jeremy Grant

Managing Director, Technology Business Strategy
Venable LLP

jeremy.grant@venable.com :: @jgrantindc

WHAT IS REGTECH?

RegTech: Technology that helps businesses comply with regulations efficiently and inexpensively.

-Australian Securities and Investments Commission (ASIC)

-Or-

RegTech: technology that seeks to provide “nimble, configurable, easy to integrate, reliable, secure and cost-effective” compliance solutions

-Deloitte

AUTHN IS REGTECH…RIGHT?

Nimble?

Reliable?

Easy to integrate?

Configurable?

Secure?

Cost effective?

OLD AUTHENTICATION - OTPS

Old strong authentication required a separate channel or device…

ONE-TIME PASSCODES

Improve security but aren't easy enough to use

SMS RELIABILITY[1]

TOKEN NECKLACE

USER CONFUSION

STILL PHISHABLE

[1]*NIST SP800-63-3: "Out-of-band authentication using the [public switched telephone network] (SMS or voice) is discouraged and is being considered for removal in future editions of this guideline."*

OLD AUTHENTICATION – SMART CARDS

Old strong authentication required a separate channel or device…

SMART CARDS

Offer strong cryptographic security but are:

- COSTLY
- INCONVENIENT
- POOR BYOD SUPPORT

THE AUTHN CHALLENGE

Nimble

Reliable

Easy to integrate

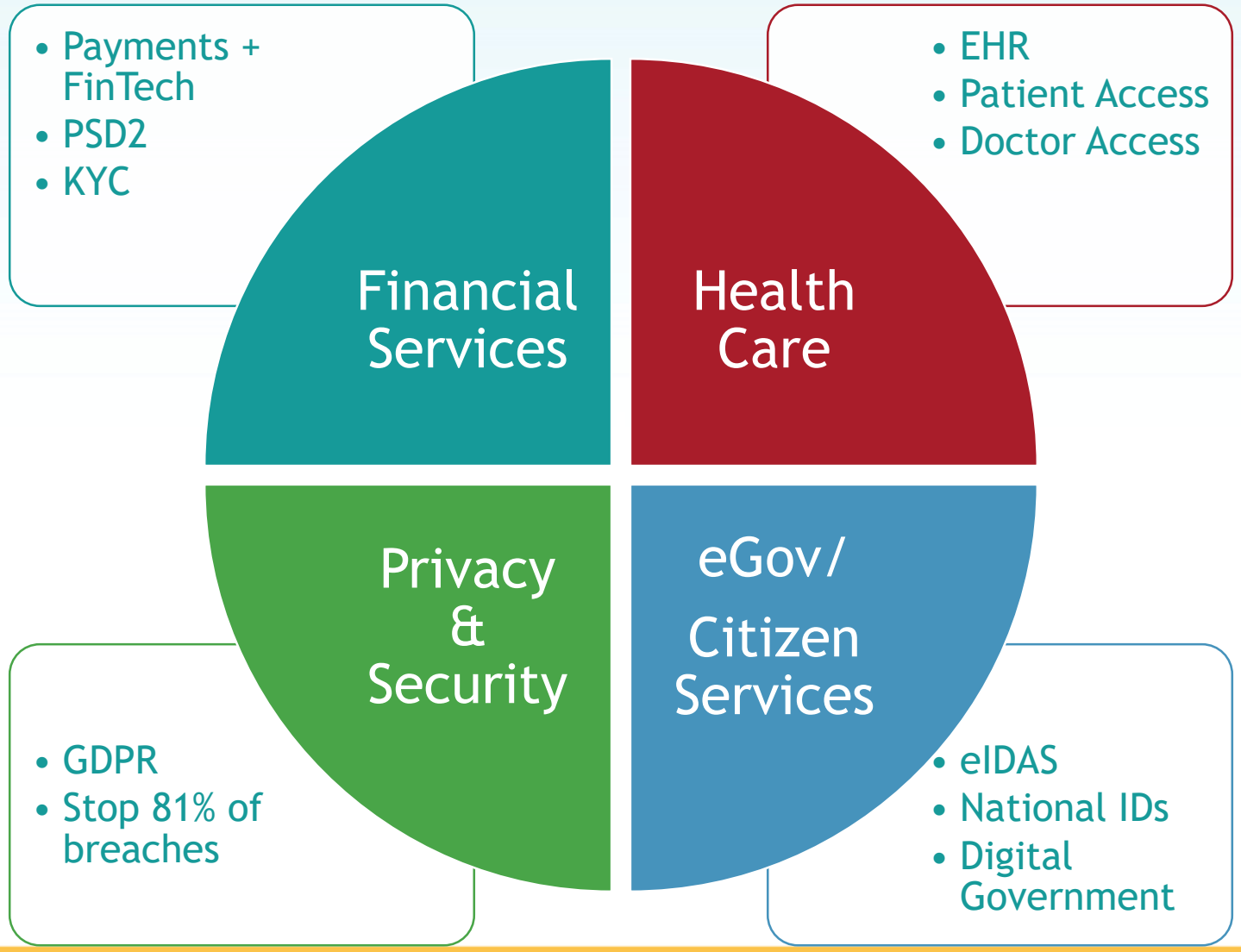
Configurable

Secure

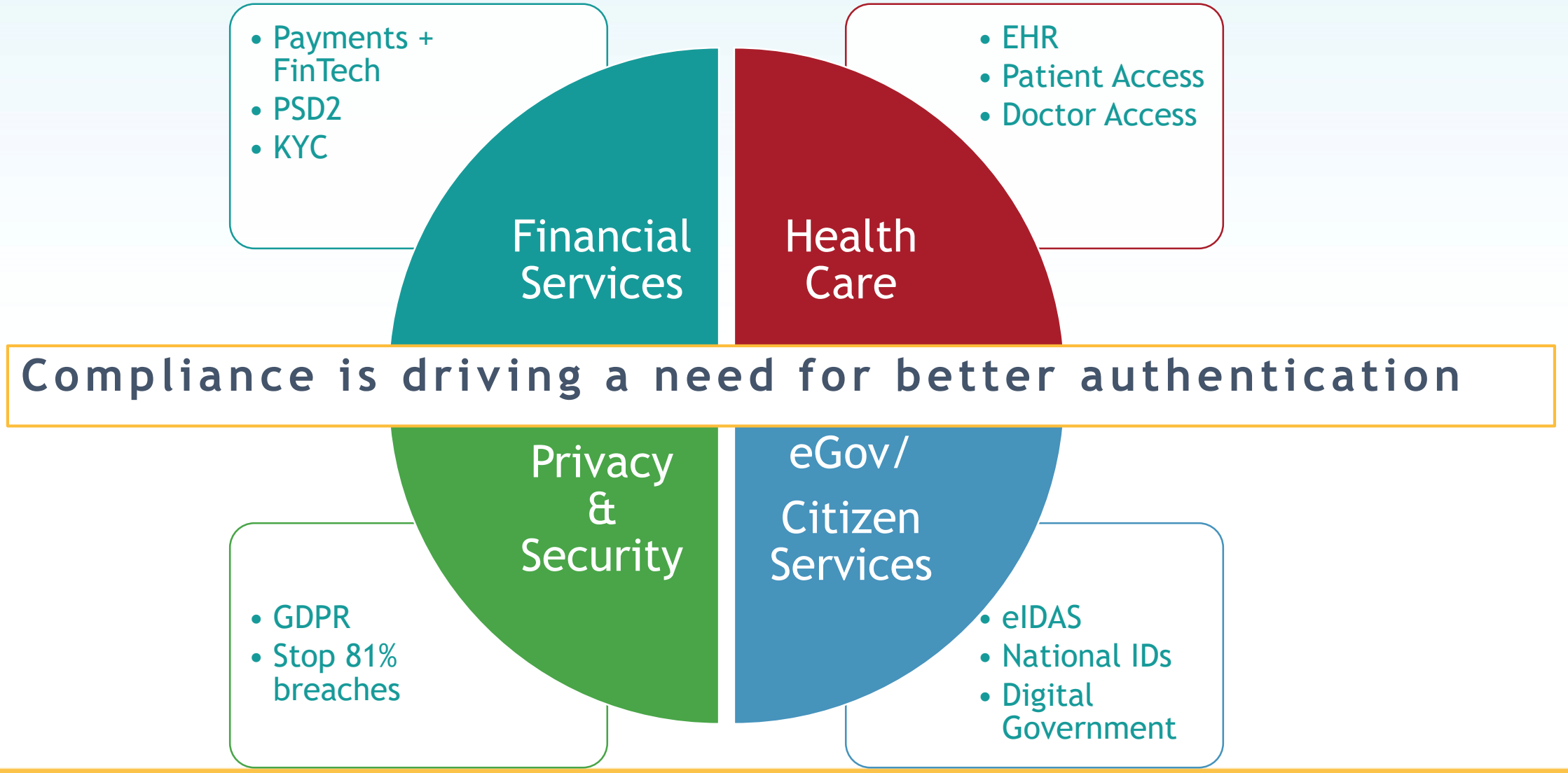
Cost effective

We need authentication solutions that can meet the “RegTech” definition - allowing better business models and customer experiences to flourish - without concerns about security, privacy and other compliance requirements

AREAS OF INNOVATION + REGULATION



AREAS OF INNOVATION + REGULATION



FIDO AS REGTECH

FIDO delivers on key priorities

Security

Usability

Privacy

Interoperability

FIDO IMPACT ON POLICY

FIDO specifications offer governments newer, better options for strong authentication – but governments may need to update some policies to support the ways in which FIDO is different.

As technology evolves,
policy needs to evolve with it.

FIDO IMPACT ON POLICY

**As technology evolves,
policy needs to evolve with it.**

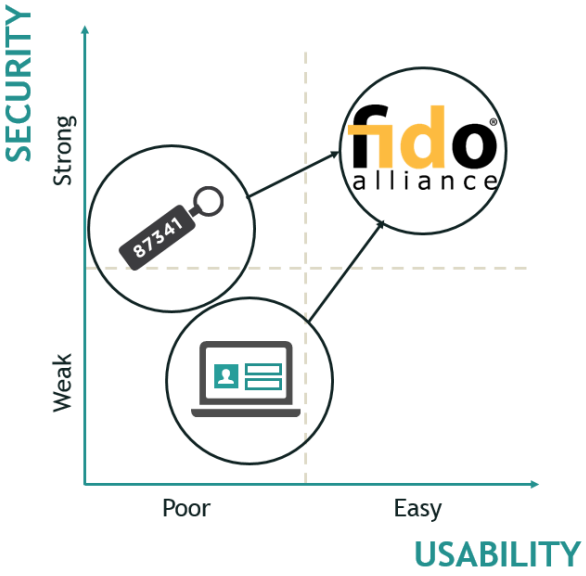
Governments are just starting to figure this out.

AS TECHNOLOGY EVOLVES, POLICY NEEDS TO EVOLVE WITH IT

1) Recognize that two-factor authentication no longer brings higher burdens or costs

> *"another commenter pointed out that current approaches to multi-factor authentication are costly and burdensome to implement"*
>
> *–US Department of Health and Human Services 2015 Edition Health Information Technology (Health IT) Certification Criteria, October, 2015*

- While this statement was true of most "old" MFA technology, FIDO specifically addresses these cost and usability issues
- FIDO enables simpler, stronger authentication capabilities that governments, businesses and consumers can easily adopt at scale



AS TECHNOLOGY EVOLVES, POLICY NEEDS TO EVOLVE WITH IT

2) Recognize technology is now mature enough to enable two secure, distinct authn factors in a single device

- Recognized by the U.S. government (NIST) in 2014; again in 2017 in SP-800-63-3
- "OMB (White House) to update guidance on remote electronic authentication" to remove requirements that one factor be separate from the device accessing the resource
- The evolution of mobile devices – in particular, hardware architectures that offer highly robust and isolated execution environments (such as TEE, SE and TPM) – has allowed these devices to achieve high-grade security without the need for a physically distinct token

ITL BULLETIN FOR DECEMBER 2014

RELEASE OF NIST SPECIAL PUBLICATION 800-157,
GUIDELINES FOR DERIVED PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS

Hildegard Ferraiolo, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

Members of the federal government are increasingly using Personal Identity Verification (PIV) cards that uniquely identify the cardholder through verification of electronically stored credentials. PIV smart cards are used to allow the cardholder access to government facilities or to access federal computer systems (e.g., desktops and laptops) equipped with smart card readers. In the last decade, the mobile computing device market has skyrocketed, with a resulting desire by both employers and employees to enable remote access from these devices.

NIST has recently released Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, to provide the technical details for a system by which mobile devices such as smart phones and tablets are provisioned with PIV credentials, allowing these credentials to take the place of the smart card for remote authentication to federal systems. The publication describes how a user with a valid PIV card could obtain a derived credential on an integrated security token using either hardware or software cryptographic modules. This approach is in response to the mobile device authentication credential outlined in Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, published in August 2013.

NIST SP 800-157 does not address use of the PIV Card with mobile devices, but does provide an alternative in cases where using a PIV Card would be impractical. In lieu of the PIV Card, the alternative security token described in SP 800-157 can be implemented and deployed directly with mobile devices. The PIV credential associated with this alternative token is called a Derived PIV Credential. The use of a different type of token greatly improves the usability of electronic authentication from mobile devices to remote IT resources.

Introduction to Special Publication 800-157

The new Special Publication describes the life-cycle activities associated with derived PIV credentials, including aspects of issuance, usage, and maintenance. It describes the methods for adhering to Homeland Security Presidential Directive 12 (HSPD-12), including the requirement that the credential be established through an official accreditation process.

SP 800-157 Chapter 3 describes the technical requirements related to certificate policies, cryptographic specifications, and the security token types that may be used with mobile devices. It lists guidelines for cases in which the use of PIV Cards with mobile devices—using either contact card readers or Near Field Communication (NFC)—is deemed impractical. The guideline specifies the use of tokens with alternative form factors to the PIV Card that may either be inserted into mobile devices—such as Secure Digital (SD) cards, Universal Serial Bus (USB)

1

AS TECHNOLOGY EVOLVES, POLICY NEEDS TO EVOLVE WITH IT

2) Recognize technology is now mature enough to enable two secure, distinct authn factors in a single device

Article 9
Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 shall be subject to measures in terms of technology, algorithms and parameters, which ensure that the breach of one of the elements does not compromise the reliability of the other elements.

2. Where any of the elements of strong customer authentication or the authentication code is used through a multi-purpose device including mobile phones and tablets, payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.

3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:

   (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

   (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.


FINAL REPORT ON DRAFT RTS ON SCA AND CSC

EBA

EBA/RTS/2017/02
23 February 2017

Final Report

Draft Regulatory Technical Standards

on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

1

AS TECHNOLOGY EVOLVES, POLICY NEEDS TO EVOLVE WITH IT

3) As governments promote or require strong authentication, make sure it is the "right" authentication

- Taiwan's Financial Supervisory Commission (FSC) in December 2016 changed its e-Banking Security Control regulations to make clear: Client-side biometrics are appropriate to use for e-Banking applications
- Previous version: Pointed only to server-side biometric match

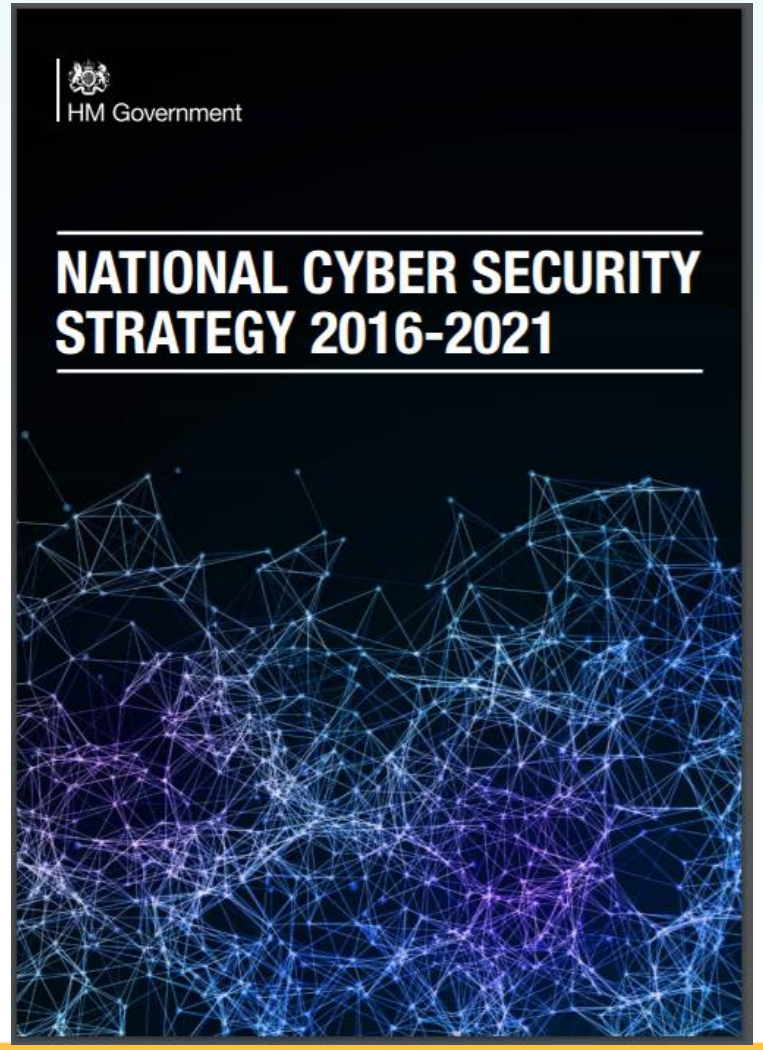
Financial Supervisory Commission
Republic of China (Taiwan)

AS TECHNOLOGY EVOLVES, POLICY NEEDS TO EVOLVE WITH IT

3) As governments promote or require strong authentication, make sure it is the "right" authentication

- The market is in the midst of a burst of innovation around authentication technology—some solutions are better than others. Don't build rules focused on old authentication technology
- Old authentication technologies impose significant costs and burdens on the user—which decreases adoption
- Old authentication technologies have security (i.e., phishable) and privacy issues—putting both users and online service providers at risk

FIDO IS IMPACTING HOW GOVERNMENTS THINK ABOUT AUTHENTICATION



Priorities:

- Ensuring that future online products and services coming into use are "secure by default"
- Empowering consumers to "choose products and services that have built-in security as a default setting."

*"[We will] invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as **Fast IDentity Online (FIDO)**, which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate.*

The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience."

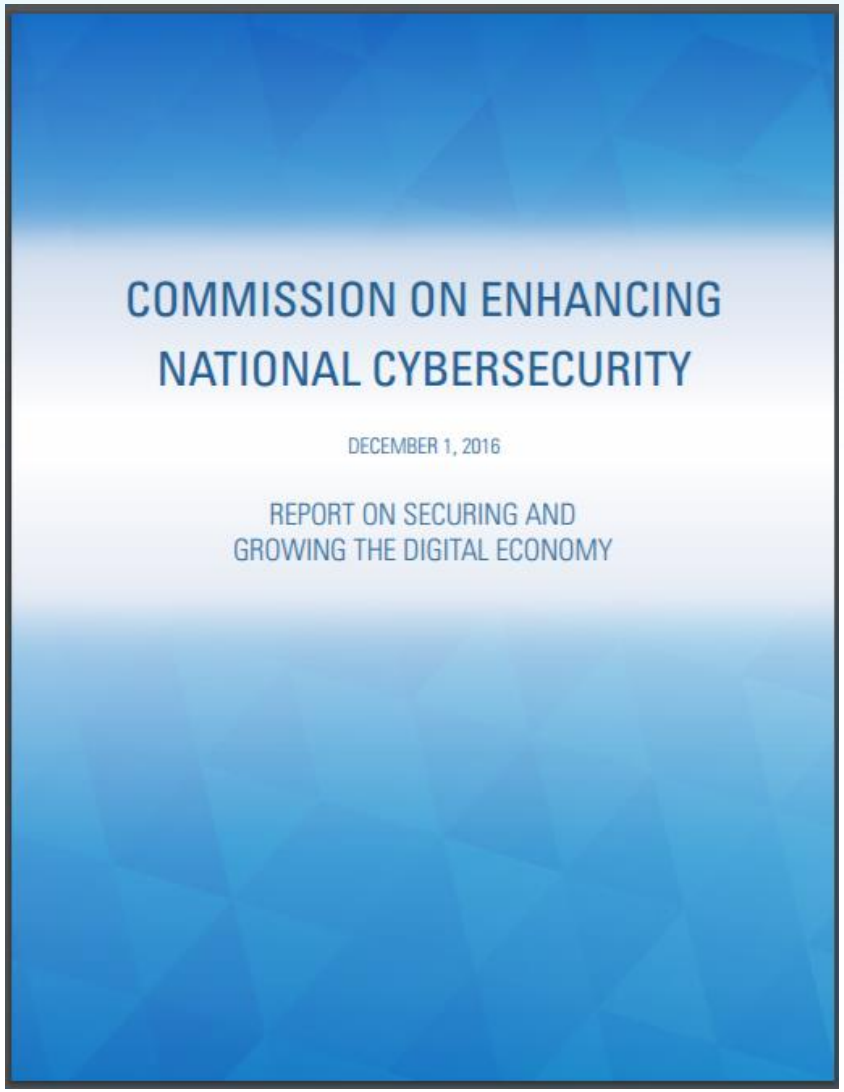
FIDO IS IMPACTING HOW GOVERNMENTS THINK ABOUT AUTHENTICATION

U.S. Commission on Enhancing National Cybersecurity:

- Bipartisan commission established by the White House in 2016- charged with crafting recommendations for the next President

- Major focus on Authentication

US COMMISSION ON ENHANCING NATIONAL CYBERSECURITY



*"Other important work that must be undertaken to overcome identity authentication challenges includes the development of open-source standards and specifications like those developed by the **Fast IDentity Online (FIDO) Alliance**. FIDO specifications are focused largely on the mobile smartphone platform to deliver multifactor authentication to the masses, all based on industry standard public key cryptography.*

Windows 10 has deployed FIDO specifications (known as Windows Hello), and numerous financial institutions have adopted FIDO for consumer banking. Today, organizations complying with FIDO specifications are able to deliver secure authentication technology on a wide range of devices, including mobile phones, USB keys, and near-field communications (NFC) and Bluetooth low energy (BLE) devices and wearables.

This work, other standards activities, and new tools that support continuous authentication provide a strong foundation for opt-in identity management for the digital infrastructure."

FIDO DELIVERS ON KEY PRIORITIES

Security

Usability

Privacy

Interoperability

QUESTIONS?

THANK YOU!

jeremy.grant@venable.com
@jgrantindc