

FIDO Applicability to US Federal - Improved Security through Improved Management Capabilities

Jim Dickens
Sr. Product Manager – IAM,
Thales TCT

Thales Trusted Cyber Technologies

Phishing Attacks on the rise

Top Two Initial Attack Vectors for Data Breaches



Source: Verizon 2023 Data Breach Investigations Report, IBM 2023 Cost of a Data Breach Report

Top Three Raising Attacks

of respondents have seen an increase in phishing attacks



2023 Thales data threat Report Global Edition

Costliest Initial Attack Vectors



Source: IBM 2023 Cost of a Data Breach Report

Phishing-Resistant Authentication: Be prepared for the new norm



"Federal agencies must require their users to use a **phishing-resistant methods, FIDO2, PIV and derived PIV** to access agency-hosted account", [EO14028, May 2021](#)

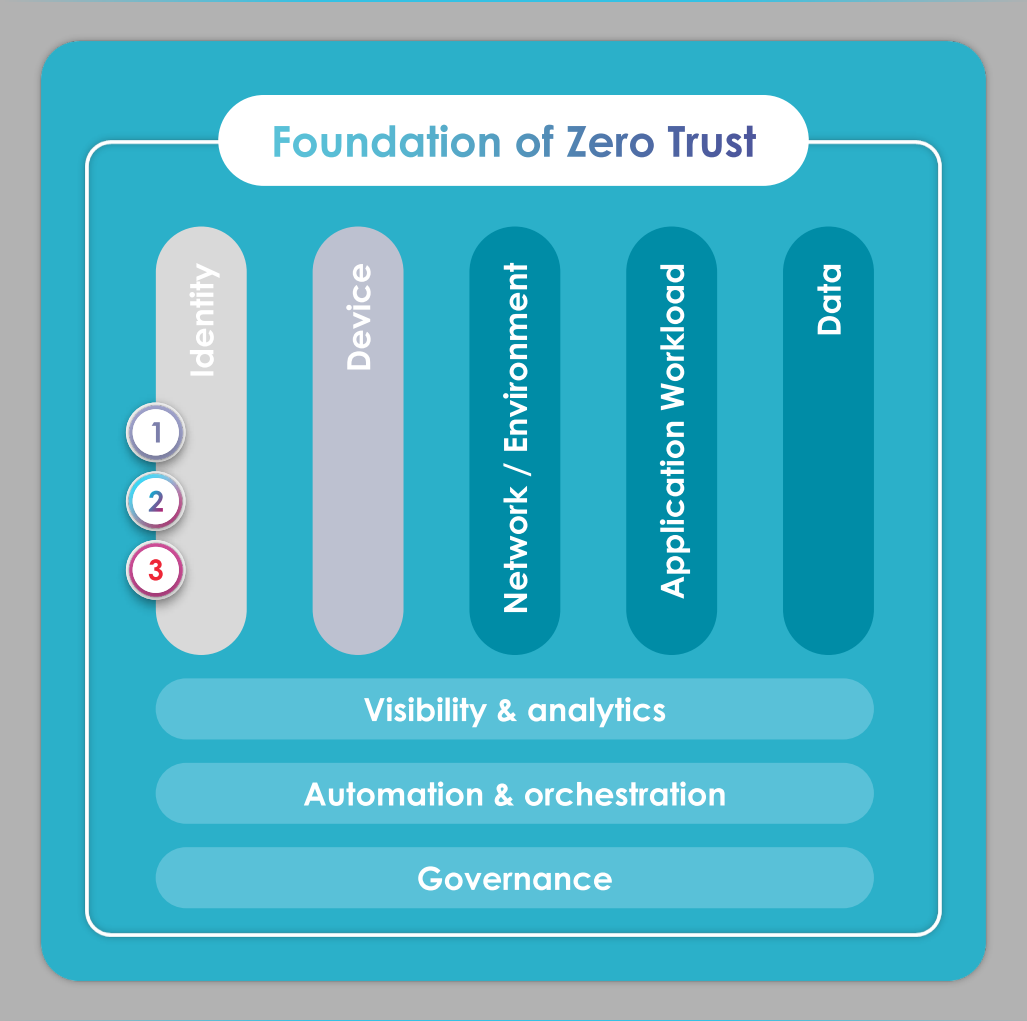


"Avoid using SMS and voice calls. Instead consider deploying **phishing-resistant** tokens such as **smart cards** and **FIDO2 security keys**", [ENISA, Feb 2022](#)

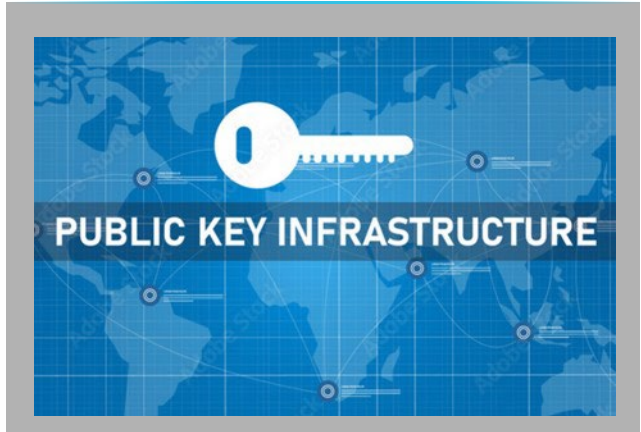


"**Enforce phishing-resistant MFA** to the greatest extent possible", [CISA, Feb 2023](#)
CISA Guidance on **Phishing-Resistant and Number Matching MFA**, [CISA, Oct 2022](#)

Critical Piece of Zero Trust



Combined PKI and FIDO worlds



PKI CBA & FIDO Authentication



> PKI CBA

- ▶ Strong Authentication, Digital Signature, Encryption
- ▶ Phishing Resistant
- ▶ Central Issuance / Verifiable Trust Chain
- ▶ Enforceable PIN policies
- ▶ Secure Channel encryption




> FIDO

- ▶ Use Case: Authentication
- ▶ Public Key Cryptography
- ▶ Phishing Resistant
- ▶ Native OS/browser support
- ▶ Fast Deployment

FIDO vs. PKI

	PKI	FIDO U2F & FIDO2
Use Cases	<ul style="list-style-type: none">• Windows Logon• VPN• e-Signing• Encrypt/decrypt	<ul style="list-style-type: none">• Authentication to Web services supported with FIDO Mobile, Tablets and Desktop• Windows Logon (Azure AD)
Ecosystem	<ul style="list-style-type: none">• Certificate Authority• Minidriver/ MW• CMS	<ul style="list-style-type: none">• FIDO Server/ IDP or any web service that supports WebAuthn
Management Features	<ul style="list-style-type: none">• Full environment support for organization to manage his PKI devices	<ul style="list-style-type: none">• Mostly aimed for B2C market. B2B market is evolving but still lacking all the management and administration features supported in PKI
Supported Platforms	<ul style="list-style-type: none">• Windows, Linux, Mac, Mobile OS (with the supported MW)	<ul style="list-style-type: none">• Windows 7 (U2F), Windows 10, Mac• Android 7, iOS 13.3

Follow a Hybrid Approach to Go Passwordless

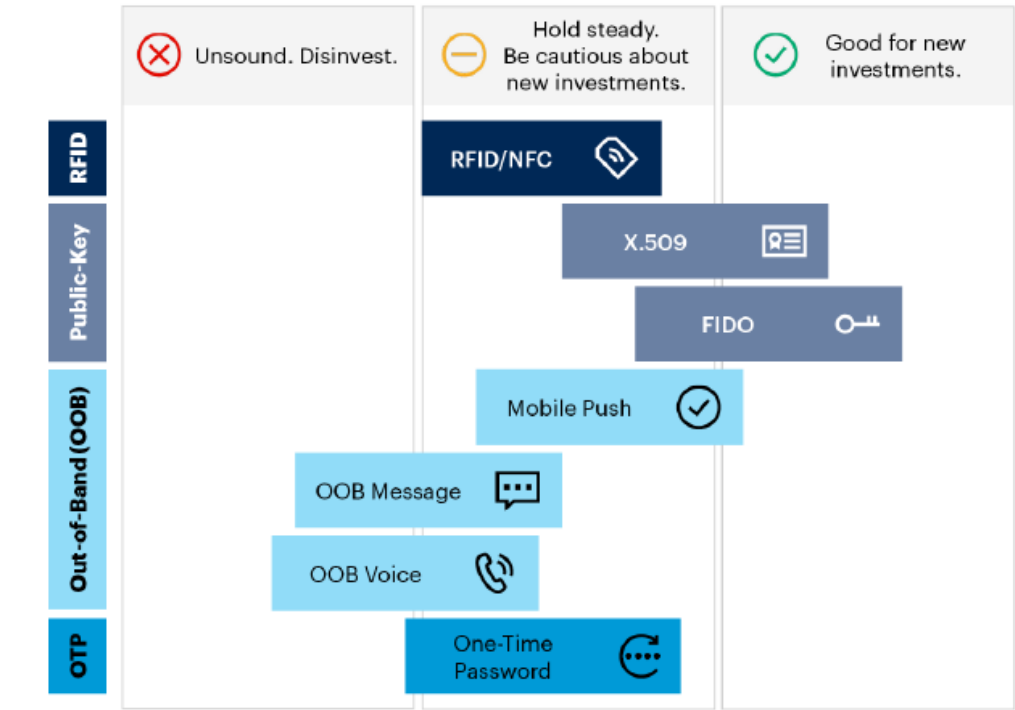


FIDO2 promises a universal, standardized approach to passwordless authentication, but in at least the near term, **alternative and hybrid approaches** will be needed.

27 © 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

The Strategic Value of Different Flavors of Authentication Token



Source: Gartner
778753_C

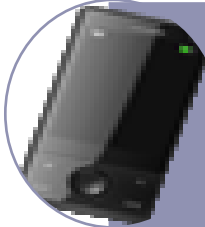
Allan Ant, Gartner IAM Summit, March 2023, “Go Passwordless Whenever You Can Wherever You Can”

Gartner

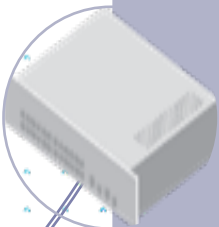
Limitations of PKI Security in supporting Cloud and Mobile Access



PKI authentication cannot be easily used for cloud applications



PKI authentication cannot be easily used on mobile devices



PKI security schemes are limited to legacy use cases and applications (VPN)

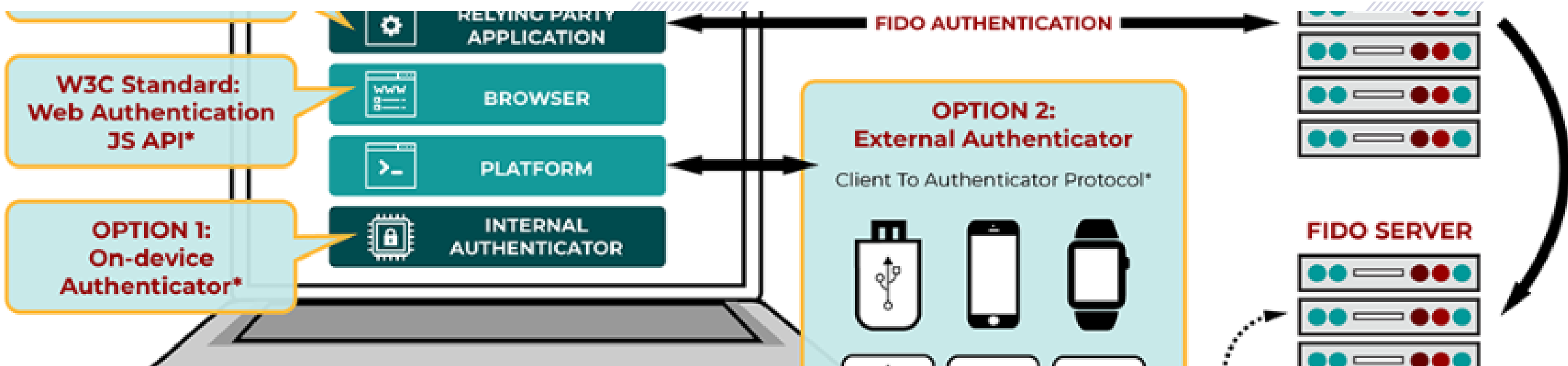
FIDO2 – Fast Identity Online

FIDO Universal Second Factor (FIDO U2F),
FIDO Universal Authentication Framework
(FIDO UAF) specification

Client to Authenticator Protocols (CTAP)
Specification

W3C's Web Authentication (WebAuthn)
specification (CTAP being complimentary)

<https://fidoalliance.org/specifications/download/>



FIDO Adoption, Complexity?

Complexity & cost!

Legacy Systems!

User resistance!

Lack of Standard implementations!

Not enough management control!

Why NOT FIDO

> Complexity & Cost

- FIDO is arguably less complex & costly than existing MFA methods!

> Legacy systems?

- FIDO is built into all operating systems and integrated into browsers, web servers, online services, and SSO systems.

> Stubborn Users?

- If Legacy means Username/password...

> Standards?

- FIDO has been around since 2013
- More applications are integrating FIDO every day

> Management Control?

- We'll come back to this!!

FIDO Deployment Pain Points

Enterprises Challenges to deploy FIDO in their organization

Configuration Management

- How to manage a persistent security policy?
- How to associate a FIDO key to a user?
- How to unblock a FIDO key?

IDP Registration/ Revocation

- Multiple IDPs deployed
- Users' self-service is a pain
- How to revoke a FIDO key ?

Hybrid IT / Ecosystem

- How to use non-FIDO applications?
- How to combine with physical access?

FIDO Adoption, Compliance

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-092², which included requirements for the federal government to implement phishing-resistant MFA.

Why FIDO

> Prevents Credential Phishing

- FIDO and PKI are the only non-proprietary MFA methods that prevent malicious actors from tricking users into revealing authentication secrets.

> Organizations already have it.

- FIDO is built into all operating systems and integrated into browsers, web servers, online services, and SSO systems.

> It is a minimum consideration for Zero Trust efforts.

- Phishing-resistant authentication is a foundational capability in building zero trust maturity.

Source: CISA Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's Fast IDentity Online (FIDO) Implementation



Why FIDO?

Strong Security in Authentication

- Asymmetric Public Key Cryptography
- Possession Based Authentication


Anti Phishing

- Keys bound to a domain; if fake, authentication fails

Prevent MIM (Man in the Middle Attacks)

- Keys stored locally in the FIDO device
- Eliminates dependence on server-side credentials

Simple to set up and use

- Single gesture, password removed or replaced by PIN
 - Open standards, no infrastructure to deploy
- 

FIDO Reference Implementation



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾SpotlightResources & Tools ▾News & Events ▾Careers ▾About ▾National Council of Statewide Interoperability Coordinators

[Home](#) / [Resources & Tools](#) / [Resources](#) / [Phishing-Resistant Multi-Factor Authentication \(MFA\) Success Story: USDA's Fast IDentity Online \(FIDO\) Implementation](#)

SHARE:    

PUBLICATION

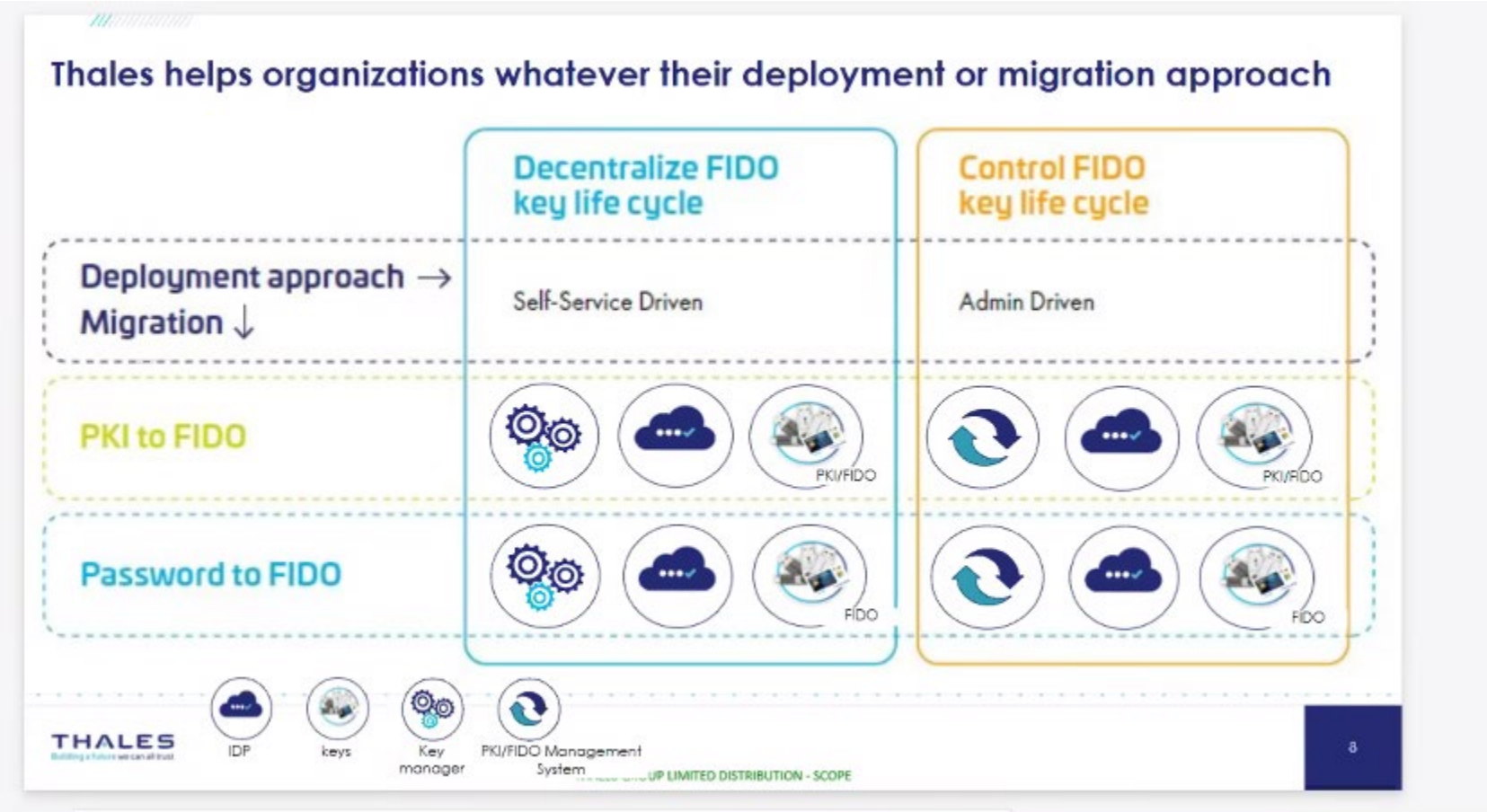
Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's Fast IDentity Online (FIDO) Implementation

Publish Date: November 20, 2024

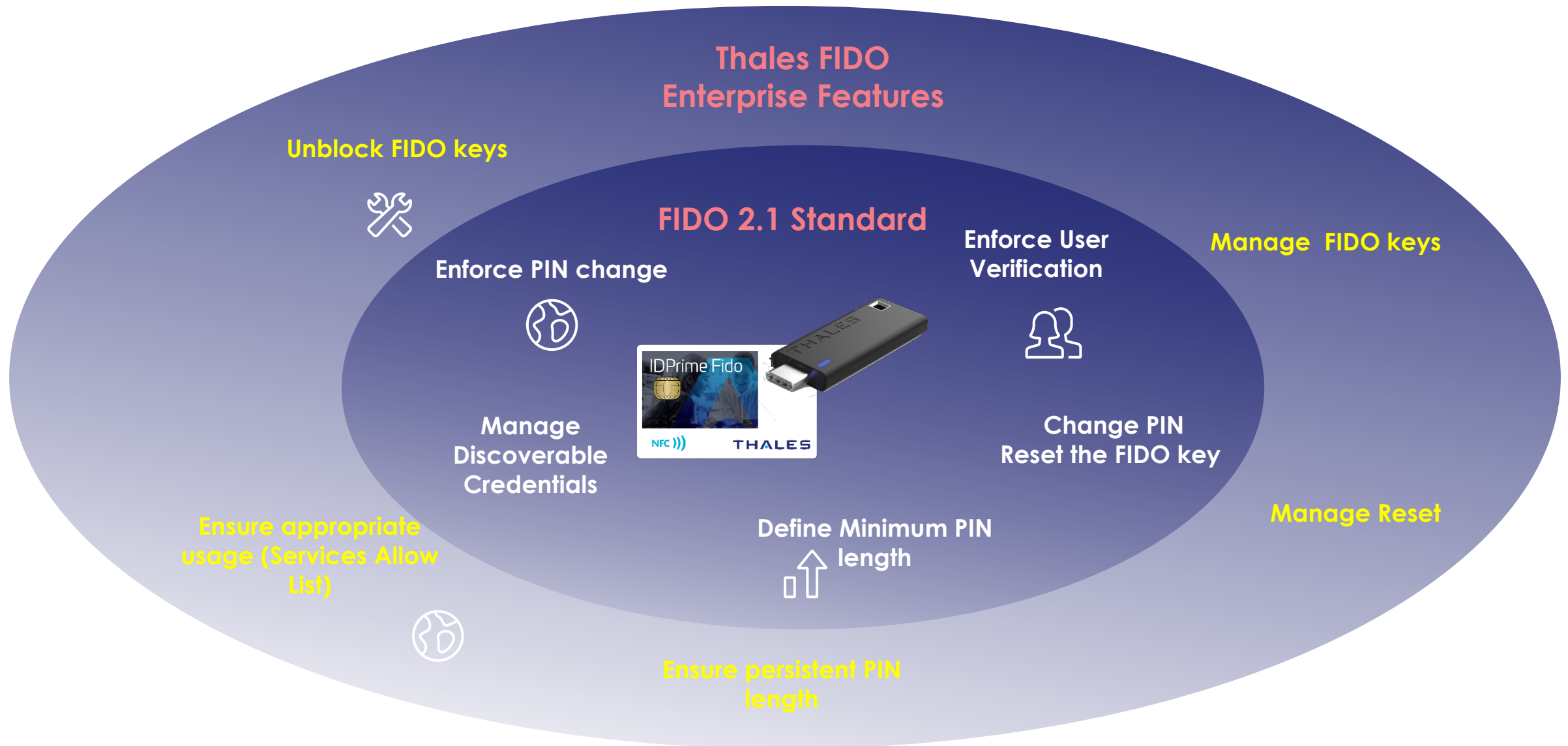
RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [PARTNERSHIPS AND COLLABORATION](#), [MULTIFACTOR AUTHENTICATION](#)



Central Management



FIDO2.1 and Thales FIDO Enterprise Features



Go Beyond the Standard: Benefits of Thales FIDO Enterprise Features



Managed Mode

- ✓ Allow the organization to manage FIDO key policies with additional administration layer



Configure Services Allow List

- ✓ Allow the organization to limit the device usage to the preferred web services



Unblock FIDO Key

- ✓ No need to delete all the information from the key if the PIN is blocked
- ✓ Perform online or offline



Manage Reset

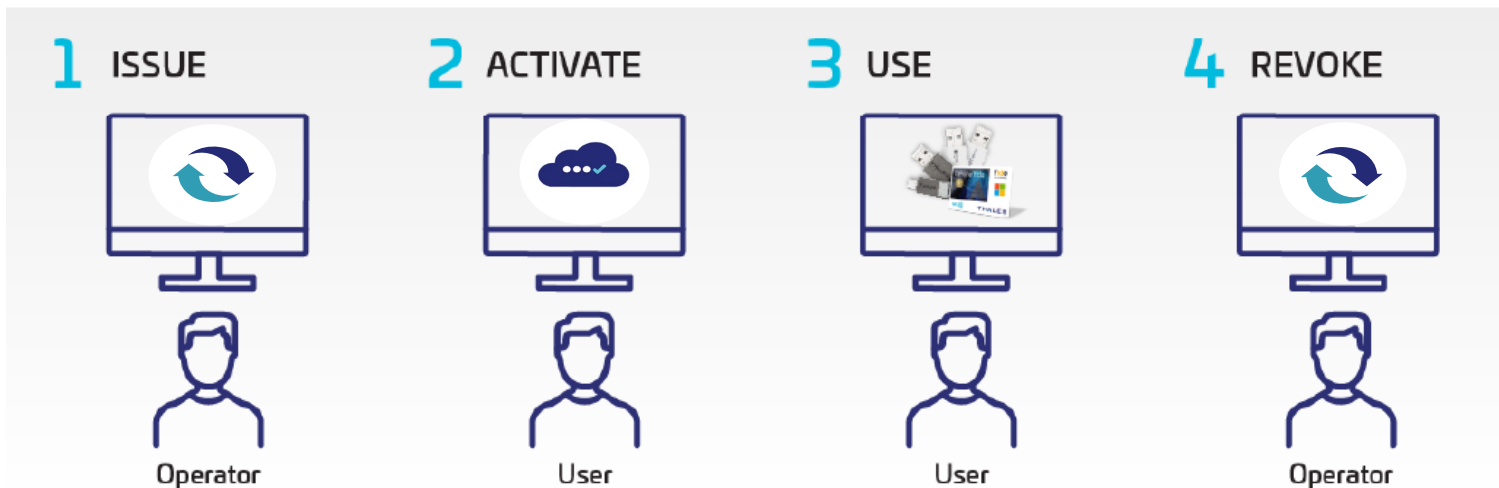
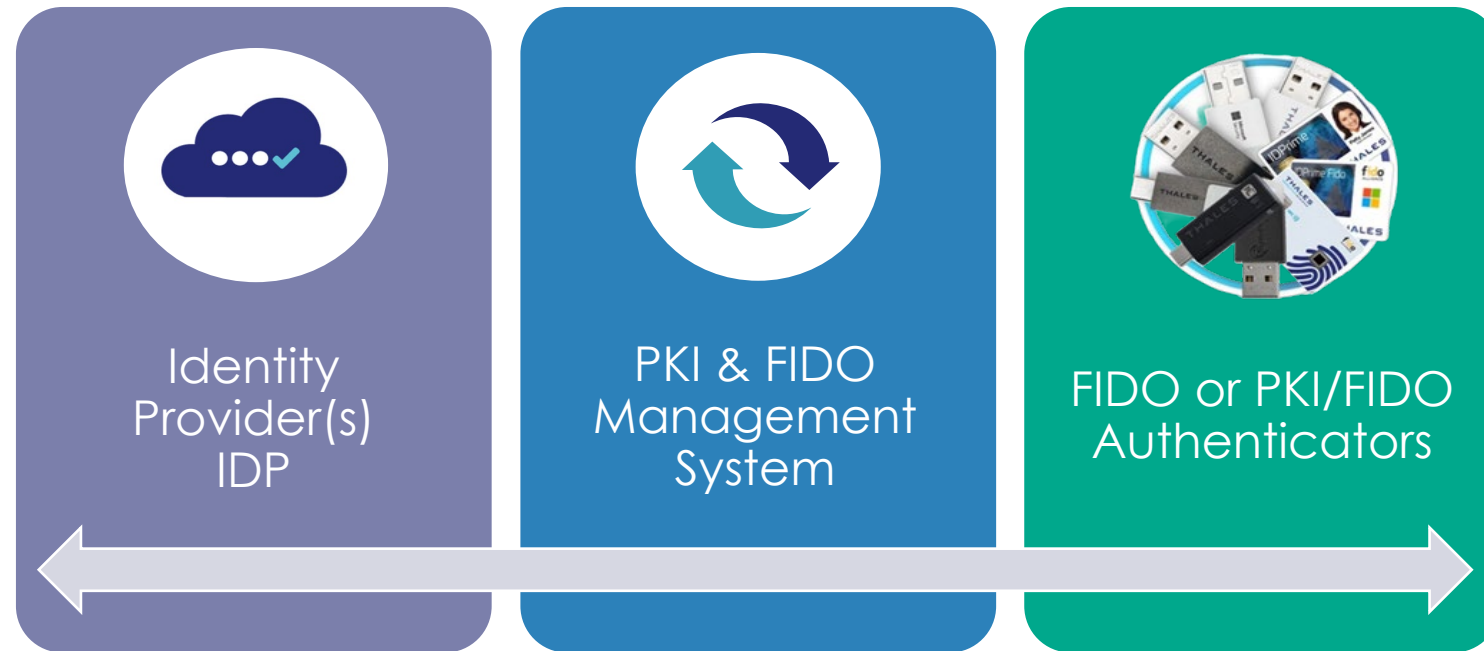
- ✓ FIDO keys containing valuable end-user information are protected against malicious or unintentional deletion



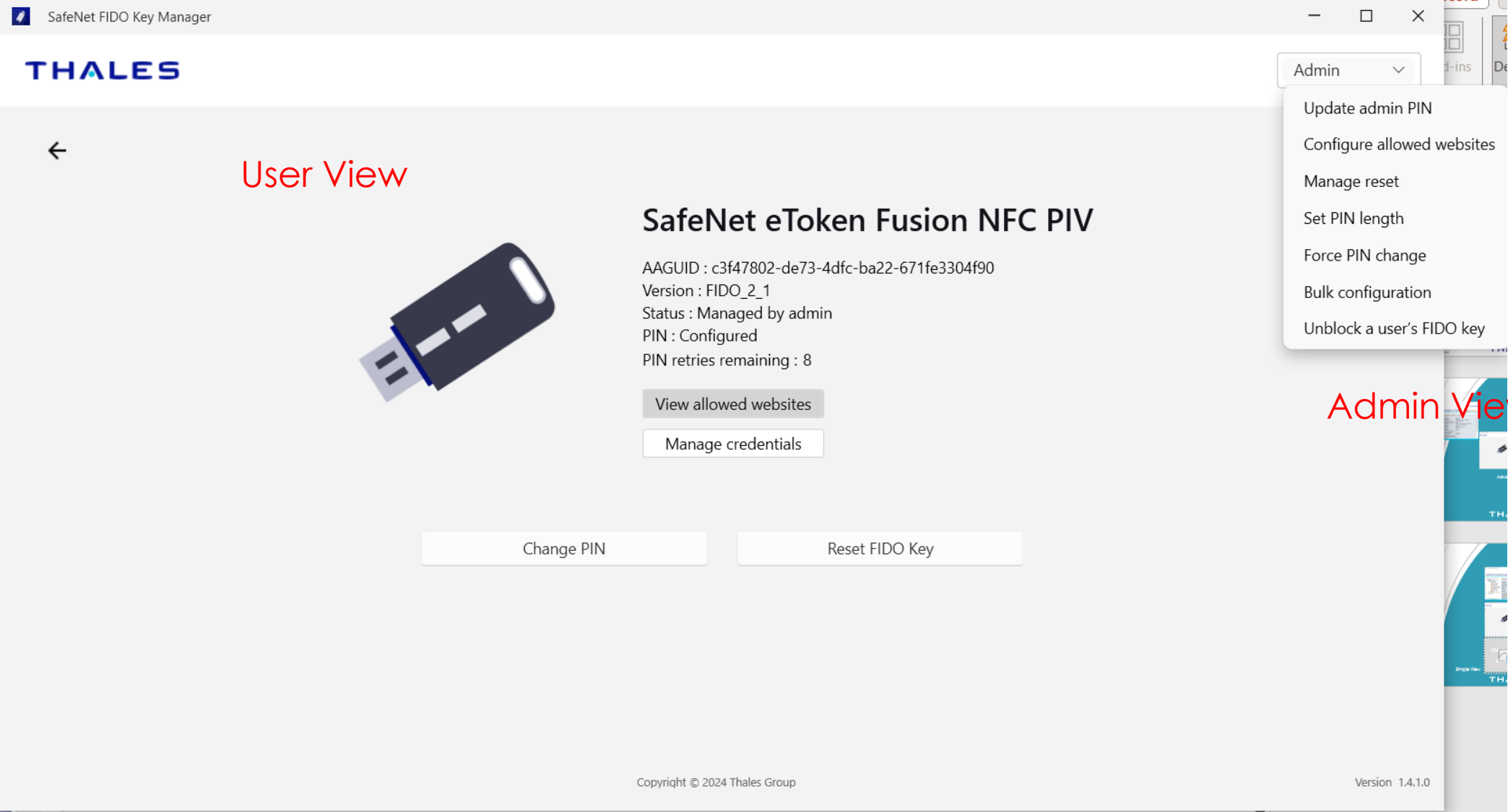
Ensure persistent PIN Length

- ✓ Allow PIN policy according to organization policy
- ✓ In managed mode, only allowed personnel can reconfigure the PIN length

Full PKI/FIDO Key life cycle Management



FIDO Key Manager- Client Utility



SYNERGY: Get the best of CBA and FIDO worlds



Thales TCT Offers Federally-Focused Solutions to Mitigate Risk



SECURITY

- FIPS140 certified
- Strong Cryptographic Libraries
- Secure Supply chain



COMPLIANCE

- FIPS201, PIV-D
- FIPS 140
- AAL3
- Zero Trust



ECOSYSTEM SUPPORT

- IdP Compatibility
- CMS Compatibility
- Both FIDO & PKI Support on all OS



STANDARDS & FEATURES

- JC / GP / Security
- FIDO
- CSP/PIV/FIDO
- Thales Enterprise Features



VENDOR TRUST

- Trusted U.S. Supplier
- SIPR and NIPR
- Long Product Lineage



Procurement Flexibility

- Extremely Competitive Pricing
- Flexible (perpetual, subscription)



Thales FIDO2 Authenticators Benefits

Best in Class Security By Design

- Phishing-resistant
- Thales Own FIDO crypto libraries
- Thales Controlled Manufacturing cycle

Same key for multiple tasks and devices

- Login to web apps and Windows session
- PKI Certificate-Based Authentication, digital signature, email encryption
- Login from multiple devices : mobile, laptops and desktops
- Physical access with smart card

Facilitate user adoption

- Fingerprint on smart card
- Sensitive presence detector on USB key

Simplify compliance

- U2F and FIDO2 certified
- FIPS and CC certified
- Comply with US Fed and EU cybesec regulations

Long life duration

- Robust, hard molded plastic, tamper resistant
- No usb ports damaged thanks to sensitive presence detector
- Support for firmware updates for better maintenance and upgradability

Additional SafeNet Offerings based on certified platform

> CAC

- ▶ FIPS 140-3, FIPS 201, GSA Certifications in process
- ▶ Available through DMDC

> SIPRNet SC650 & SC230



> PIV, Fusion, ID Prime 930

- ▶ FIPS 140-3, FIPS 201, GSA Certifications in process
- ▶ Samples available upon request
- ▶ Available through Standard channel



Combining PKI & FIDO = Thales Fusion Tokens & Cards



<https://www.thalestct.com/identity-access-management/fido-fusion-trial/>



Jim Dickens

Senior Product Manager

 **443-484-7046**

 **Jim.Dickens@ThalesTCT.com**