BLUEPRINT

AXIAD

# Future-Proofing Your MFA

**Who should read this?** CISOs and their identity architects; Multifactor authentication (MFA) product owners; IAM program leaders and IAM teams; solution architects for identity systems and MFA.

**What they'll learn:** How MFA increasingly comes under new and innovative attacks; how it's been compromised; and how existing MFA solutions can be augmented to make them phishing- resistant and future-proof.

Ten years ago, multifactor authentication (MFA) came along as something of a savior to the cybersecurity industry. Password-based authentication was the norm, but "harvesting" – aka stealing or copying – those credentials became a cottage industry. Password attacks, including password spraying, password stuffing, dictionary attacks, and phishing, obliterated authentication defenses and corporate confidence in equal measures. July 4 of 2024 may have been the final straw for password-based authentication, when a file with 10 billion individual passwords was posted in an online hacking forum in what "could be the largest such compilation of leaked passwords ever[2]."

MFA, the notion that an authentication experience should consist of two or more different factors, became the accepted standard for authentication. MFA requires three factors – defined as knowledge, possession, and inherence – to be present for an authentication event to succeed.

## EXECUTIVE SUMMARY

- As MFA solutions have matured, so have the attacks against them
- What was once the high bar for authentication has become "barely good enough," putting MFA practices under scrutiny
- Regulatory standards like NIST, PCI, HIPAA, FIEC, and GDPR are evolving to call for more robust MFA as defined in NIST 800-63B, Digital Identity Guidelines[1] – Authentication and Lifecycle Management
- NIST 800-63 blasts "good enough MFA" and uses the AAL-2 standard to define "strong, phishing-resistant MFA" with the use of FIDO or PKI credentials
- This brief explains how these credentials and the security they provide can be added to existing MFA implementations

[1] Hype Cycle for Digital Identity, 2023

[2] Nearly 10 billion passwords leaked in what may be biggest dataset of its kind ever

# FUTURE-PROOFING YOUR MFA

These factors are demonstrated by what we now consider to be commonplace terms:

- Knowledge factors: something you know like passwords, PINs, or security codes
- Possession factors: something you have, like a smart card, a mobile device, or security fobs or tokens
- Inherence factors: something you inherently and unchangeably are, like your fingerprint, facial scan, iris scan, or other biometric value

As these terms took hold in cybersecurity's lexicon, MFA became mandated in regulatory standards like NIST, PCI, HIPAA, FIEC, and GDPR. It was preached as a best practice by almost every auditor, analyst and cybersecurity strategist. From 2020 to 2022 the number of MFA authentication events went from 6.6 billion to 13 billion[3] and the MFA market was pegged by some at $14.8 billion USD with expectation it would grow at a CAGR of 14.2% for several years[4].

[3] Total number of multi-factor authentications (MFA) worldwide from 2020 to 2022

[4] Multi-factor Authentication Market Trends

# ADVERSARIES HONE THEIR MFA ATTACKS

The general optimism that NFA would cure cybersecurity's weaknesses only lasted a few years. Numerous successful attacks against MFA-defended targets showed there were many levels of robustness" in MFA implementations, and that not all were created equal.

- In 2017, attackers in Germany focused on MFA solutions that used SMS push as an authentication method. By exploiting a flaw in SS7 protocols to bypass the two-factor authentication deployed by banks they were able to drain customer bank accounts[5].
- In 2019, the FBI issued an urgent industry warning showing how tools and techniques were being used to defeat MFA, including web hacks, cyberattack tools like Muraen and NecroBrowser, and SIM swapping[6].
- In 2021, a new attack using OTP interception bots showed that not only was MFA hackable, but that the tools to do so could be easily acquired on the dark web and even more easily deployed by lower-skilled adversaries[7].
- In 2022, SaaS money-maker Uber was crippled by the hacking group Lasus$ despite having MFA in place because people are, after all is said and done, people. In what has been dubbed an "MFA fatigue" attack, a contractor received multiple authentication approval requests on a secondary device and after at first denying the request was spoofed through another social channel and eventually approved a request.
- In 2023, kits like Evilginx 3.2, an adversary-in-the-middle attack became widely available on dark web forums. Evilginx was shown to defeat Microsoft's standard MFA offering, Windows Hello for Business (WHfB) in a "downgrade attack" where it forced WHfB to "shift down" to lower-grade methods like passwords or OTPs[8].
- In May 2024, InfoSecurity magazine reported that phishing attacks – primarily aimed at the weaker MFA functions – had experienced a 341% increase[9].

With these attacks as a backdrop industry strategists and analysts were quick to realize two facts: First, MFA could be perceived as a panacea for the company that deployed it, leading to a false sense of security. As the Forbes article cited above stated,

"An issue with MFA, it seems, is that it is a misleading comfort for the institution itself."

And second, MFA (in and of itself) is only as good as it's configured to be. Some factors are inherently stronger than others.

[5] Attackers exploited SS7 flaws to empty Germans' bank accounts

[6] FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Authentication Is Being Defeated

[7] Cybercriminals going after one-time passwords with Telegram-powered bots

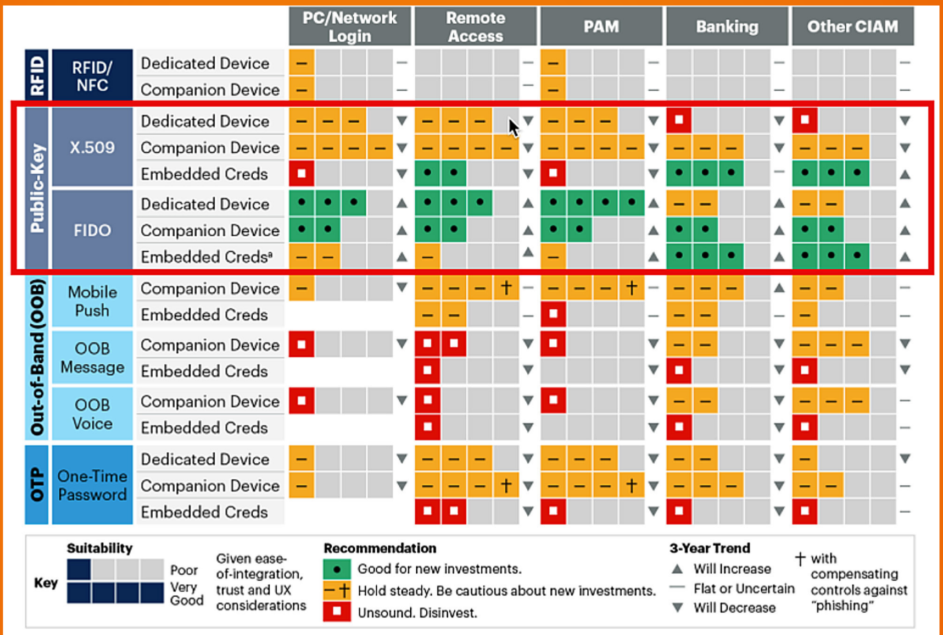
[8] Goodbye? Attackers Can Bypass 'Windows Hello' Strong Authentication

[9] Report Reveals 341% Rise in Advanced Phishing Attacks

# NOT ALL MFA IS CREATED EQUAL

A Gartner research report published in 2023, “Innovation Insight for Many Flavors of Authentication Token”[10] , showed how different authentication mechanisms (or “tokens”) differed in their suitability for different use cases. In this note, authentication tokens based on one-time passwords, out-of-band voice, SMS messages, and mobile push notification were all suspect, and considered “unsound” for most use cases.

## Suitability of Authentication Tokens in Different Use Cases and Recommendations



| | | | PC/Network Login | | Remote Access | | PAM | | Banking | | Other CIAM | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RFID | RFID/ NFC | Dedicated Device | – | — | | — | – | — | | — | | — |
| | | Companion Device | – | — | | — | – | — | | — | | — |
| Public-Key | X.509 | Dedicated Device | – – – | ▼ | – – – | ▼ | – – – | ▼ | ■ | ▼ | ■ | ▼ |
| | | Companion Device | – – – – | ▼ | – – – – | ▼ | – – – – | ▼ | – – – | ▼ | – – – | ▼ |
| | | Embedded Creds | ■ | ▼ | ● ● | ▼ | ■ | ▼ | ● ● ● | — | ● ● ● | ▲ |
| | FIDO | Dedicated Device | ● ● ● | ▲ | ● ● ● | ▲ | ● ● ● ● | ▲ | – – | ▲ | – – | ▲ |
| | | Companion Device | ● ● | ▲ | ● ● | ▲ | ● ● | ▲ | ● ● | ▲ | ● ● | ▲ |
| | | Embedded Creds[a] | – – | ▲ | – | ▲ | – | ▲ | ● ● ● | ▲ | ● ● ● | ▲ |
| Out-of-Band (OOB) | Mobile Push | Companion Device | – | ▼ | – – – † | — | – – – † | — | – – – | ▲ | – – | — |
| | | Embedded Creds | | | – – | — | ■ | — | – – | — | – | — |
| | OOB Message | Companion Device | ■ | ▼ | ■ ■ | ▼ | ■ | ▼ | – – | ▼ | – – – | ▼ |
| | | Embedded Creds | | | ■ | ▼ | | ▼ | ■ | ▼ | ■ | ▼ |
| | OOB Voice | Companion Device | ■ | ▼ | ■ | ▼ | ■ | ▼ | – – | ▼ | – – – | — |
| | | Embedded Creds | | | ■ | ▼ | | ▼ | ■ | ▼ | ■ | — |
| OTP | One-Time Password | Dedicated Device | – | ▼ | – – – | ▼ | – – – | ▼ | – – | ▼ | – | ▼ |
| | | Companion Device | – | ▼ | – – – † | ▼ | – – – † | ▼ | – – – | ▼ | – – | — |
| | | Embedded Creds | | | ■ ■ | ▼ | ■ | ▼ | ■ | ▼ | ■ | — |

Key

Suitability: ■ □ □ □ Poor; ■ ■ ■ ■ Very Good. Given ease-of-integration, trust and UX considerations

Recommendation: ● Good for new investments. – † Hold steady. Be cautious about new investments. ■ Unsound. Disinvest.

3-Year Trend: ▲ Will Increase; — Flat or Uncertain; ▼ Will Decrease

† with compensating controls against "phishing"

In the research note, “Innovation Insight for Many Flavors of Authentication Token”, analysts for research firm Gartner show how different authentication factor or tokens are suitable for different uses, and where security investments should be made. (Red highlight added by Axiad.)

While these older methods were considered unsound investments, and not resistant to the aggressive phishing attacks being experienced in the wild, the research did recommend another path.

A set of methods designed around “public key” concepts was shown to be both strong enough for uses like PC and network login, remote access of systems, privileged user access, banking and customer access.

[10] Summary Translation: Innovation Insight for Many Flavors of Authentication Token

# PKI STRENGTHENS AND EXTENDS THE LIFE OF MFA

The concept of "public key" cryptography has been around almost as long as computers have been around. In simple terms, public-key cryptography is a system that uses pairs of related keys: a public key and a corresponding private key. Used together, the two keys turn encoded messages into understandable messages. Key pairs are generated digitally with cryptographic algorithms based on mathematical problems. When combined with other technologies like X.509 certificates, Transport Layer Security (TLS), Secure Shell (SSH), S/MIME or PGP, public-key concepts allow browsers to interact with web sites privately, machine-to-machine connections to be made, messages to be encoded and files to be secured.

In the Gartner table above, the class of capabilities recommended for authentication uses cases falls under the "public-key" label, but includes two different technologies, PKI and FIDO.

**PKI** is shorthand for "public key infrastructure". If the public key concept refers to the cryptography being used, PKI refers to all the infrastructure than enables it. This includes certificate authorities (CAs) who certify ownership of key pairs, registration authorities who verify user requests for digital certificate, certificate revocation list (CRLs) and policies, and the protocols and standards that allow these to communicate. PKI generally relies on digital credentials and not passwords.

**FIDO** is shorthand for "fast identity online". FIDO is another "public-key" concept like PKI and designed to replace passwords with passkeys. Instead of relying on certificates, FIDO generates unique key pairs for each website, with the website storing the public keys. Private keys are stored on the user's own devices.

As similar as these approaches are in philosophy and concept, they differ markedly in architecture, workflow, and overall coverage.

| PKI (Public Key Infrastructure) | FIDO (Fast Identity Online) |
|---|---|
| Relies on digital TLS certificates for public key distribution | Each website generates distinct key pairs and acts as the "relying party" |
| Certificates, signed by trusted authorities (CAs), ensure authenticity of keys | Websites retain public keys, reducing risks of cross-site attacks |
| Establishes secure, transparent authentication through built-in cryptographic connections | Private keys decode connection and remain securely stored on individual devices, usually laptop or desktop machines |
| Native support by operating systems, browsers, and applications streamlines integration | Support comes from the website being visited, may incorporate biometric authentication for user simplicity |

A table showing a few of the commonalities and differences between the two most popular public-key concepts, PKI and FIDO

# PKI STRENGTHENS AND EXTENDS THE LIFE OF MFA

CONTINUED

It's important, when thinking about public-key technologies in the context of MFA, to think of the tokens they generate as the "something you have" part of the MFA trifecta. They are a "possession factor," generally conveyed by some device we possess. This can be a smart card, a mobile device, or a hardware-based security token like the keys made by Yubico, IDEMIA, or Feitian.

Because we're embedding data (knowledge, of a sort) on the "thing in our possession" (the key or device) we're often tempted to think of passkeys and credentials as "knowledge factors" just like passwords. But in the strictest "multi-factor" sense they are not. Typically, when we store X.509-based or FIDO-based tokens on a key or device, the digital credential is "bound" it to the device: this assures the device's identity as well as its role as a "possession factor" in the authentication process[11].

X.509-based solution and FIDO solutions are similar, but not the same. FIDO passkeys were designed for end user access to web sites and retain a very "consumer centric" flavor for that reason. They are not, however, well suited to all the other activities that take place daily in the commercial or business environment, like securing machine-to-machine connections, digitally signing and encrypting emails or signing documents[12].

For this reason, the ideal MFA solution would support both PKI-based and FIDO-based credentials.

[11] The alternative to "bound" keys is "synced passkeys,"also known as multi-device passkeys, which are designed to be stored and synchronized across a user's various devices via cloud services.

[12] For more on the differences X.509 and FIDO, see this Axiad blog post

## ADDING PKI AND FIDO TO EXISTING MFA

Mobile devices like the iPhone shown below running Axiad's MFA solution, or like the IDEMIA Smart Credential options shown next to it, are the backbone of MFA. Most MFA solutions use one of these methods to deliver up the possession or inherence factors of MFA. Non-password knowledge factors, like PINs and passphrases, are used less and less. The "strength" of modern MFA comes from the credentials we insert into the process.

Account
corp.cloud

Application
Microsoft Office 365...

User
mthelander

Location
Oregon, US

IP Address
12.345.568.999

# ADDING PKI AND FIDO TO EXISTING MFA

## CONTINUED

Because these credentials are software-based and made up of encryption methods and code, they are inherently extensible and upgradeable. The real trick to future-proofing MFA becomes: "How to manage these credentials, at scale, and how do we use them effectively within our MFA workflows?" How do we treat MFA as an ecosystem with several parts and options?

Or put another way, can we future-proof our MFA if we provide a management plane across our MFA systems, applications, and devices that allows us to apply multiple types of credentials (PKI-based or FIDO) across different types of authenticators (hardware tokens or mobile devices)? Do we future-proof it if we can we manage enrollment, renewal and revocation of these credentials as needed?

The answer is Yes. We future-proof MFA when we deploy a management system that supports three principles: consolidation; consistency; and cryptographically-sound design.

**Consolidation:** Serves all MFA needs, everywhere across the environment.

- End-to-end Security: All entities are secured without using passwords or shared secrets, so the authentication process is secure from end-to-end
- Passwordless consolidation: Utilize multiple types of authentication methods without a password or push notification that can be intercepted or phished
- Phishing-Resistant Authentication: Deliver phishing resistant authentication based on FIDO2 and WebAuthn with Authenticators ranging from enterprise-grade mobile based to government-grade AAL3
- Certificate-Based Authentication: Leverage an international standard X.509 certificate to interoperate across a broad range of vendor products
- Customization of Certificates: Support custom certificates and workflows
- Customizable Workflows: APIs should enable full integration with vendor products or custom software
- Interaction Certification: Certifies email senders and attachments

# ADDING PKI AND FIDO TO EXISTING MFA

CONTINUED

**Consistency:** Enable consistent authentication experiences across OSs, applications, and services.

- Broad OS support: Be able to secure Microsoft Windows, Apple OSs, Linux, and more
- Windows-friendly: Provides authentication across Windows ecosystem including Azure, Windows OS, and more
- Token Side-by-Side support: Leverages a wide array of physical and virtual tokens working in the same environment
- Integrated: Support a wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

**Cryptographically-sound:** System must be architected for best-practices security including isolation by customer, encrypted communications, and key storage in specialized hardware.

- Hardened Approach: Leverage a private cloud instance for each customer, private certificate store, and secure, encrypted network communications
- End-to-end Security: All entities are secured on the front-end with MFA or greater and on the back end without using shared secrets
- Asymmetric Cryptographic Authentication (ACA): Eliminates shared secrets with ACA so credentials cannot be intercepted in transit
- Hardware Root of Trust: Each customer's cryptographic information is stored in a dedicated Hardware Security Module (HSM) partition
- Customer Interface: All customer data is under customer control and edited via Unified Portal
- Continuous Compliance: There is an annual SOC2 Type II audit of the solution's security, based on NIST controls

Nothing in cybersecurity is a silver bullet. This is as true for MFA as any other control, principle, or design. But MFA can be future proofed against upcoming threats and unforeseen technology shifts if we view it through the lens of these Three Cs: Consolidation, Consistency, and Cryptographically sound thinking. If we do that while we leverage existing technologies to their fullest – like PKI and FIDO – we can have enterprise-class MFA solutions that will grow with us.

To read more about how Axiad products can help your MFA evolve without ripping and replacing existing systems, visit us at www.axiad.com.

101 Metro Drive, Suite 560 San Jose, CA 95110 United States

AXIAD