AXIAD

fido ALLIANCE

Reinforcing FIDO: How Certificates and PKI Fill Critical Gaps in FIDO Authentication

SUMMARY

Who should read this? CISOs, IAM directors, authentication administrators, and identity architects in regulated or high-risk environments who hold responsibility for securing systems and networks.

What they'll learn: How hardware-based authentication, specifically using certificates, enhances the implementation of Zero Trust principles by bolstering security while maintaining an optimized user experience. Certificate-based authentication involves the issuance of digital certificates to devices, enabling them to securely authenticate with network resources.

Axiad is proud to be one of the 40-plus vote-endowed "Board Level" members of the FIDO Alliance. Not only is the group behind Fast Identity Online fulfilling a critical cross-industry mission but the group's latest specification, FIDO2, has become the standard for strong user authentication. Some of the reasons are clear:

- FIDO2 is a secure-by-design identity architecture
- FIDO2 moves the market away from its old reliance on passwords
- When using device-bound credentials, FIDO2 blocks external ATO attempts by requiring the presence of physical tokens
- FIDO2 device-bound tokens and passcode combinations have 1: many uses, with the ability to work across multiple web sites or accounts

This is why Gartner, Inc., a research and advisory firm, noted in 2023's Hype Cycle for Digital Identity[1] that FIDO2 technology was moving out of the "trough of disillusionment" and into a phase of "early mainstream" adoption. This is also why the number of Axiad customers who say they are "all-in on FIDO" increases every year.

But like all other cybersecurity technologies, FIDO2 isn't an all-purpose silver bullet. There will continue to be use cases and scenarios that challenge FIDO2 implementation. These will require IAM teams to practice "layered defense" and "defense in depth" approaches when designing their identity and access architectures. This solution brief lays out some of those challenges in the beginning and at the end proposes enterprise-ready authentication alternatives.

[1] Hype Cycle for Digital Identity, 2023

CHALLENGE #1: USABILITY AT ENTERPRISE SCALE

Just like it is for B2C internet activity, usability is also king for B2B uses, although for different reasons: poor usability in commercial usage leads to expensive service ticket backlogs and help desk calls that sap energy, operating costs, and motivation from a company and its employees.

Researchers at Australia's Macqaurie University performed an extensive usability study in 2023 of FIDO2's suitability for enterprise environments[2], and uncovered several interesting data points:

- "In particular, an adequate handling of processes such as account recovery or enrollment, and edge cases like lost authenticator were found challenging…"
- Their report noted that "even fundamental processes such as registration and authentication were also found to pose significant challenges."
- "Our respondents believe that even though their general knowledge of FIDO2 is satisfactory, the practical knowledge and integration paths are still missing and pose a major obstacle."
- "Solution costs and missing native integrations were spotted as a major adaptation blockers. In particular, integration with commonly used servers (e.g., Windows or Linux) poses a significant challenge for enterprise deployment."
- The respondents clearly articulated that "usability, more precisely, differences in the presentation (UI) and process (UX) pose a challenge for the integration into employees' daily routines."

The Macquarie University study summarized itself this way: "Our findings were confirmed by the user study, in which we managed to identify and order the most challenging aspects of FIDO2 adaptation (i.e., missing know-how, cost, and usability)… In particular, we hope our study will be used as a guide for usability researchers as well as the FIDO community including standardization bodies (e.g., FIDO Alliance), commercial vendors, and enterprises."

While these data come from just one recent academic report, FIDO is reported to be spending nearly a third of its development budget to improve usability. This indicates the organization is hearing – and acting upon – the same usability message.

LEGACY?
ADMINISTRATIVE?
2ND TIER?

Whether IT teams consider them to be "second tier systems," "administrative systems" or sometimes pejoratively dismiss them as "old legacy gear" there remain a lot of antiquated systems in the modern enterprise.

According to research and advisory firm Gartner, these are "information systems that may be based on outdated technologies, but are critical to day-to-day operations." Gartner's 2024 research note "Use Continuous Modernization to Optimize Legacy Applications" cited survey data showing "47% of the respondents selected 'integrate, innovate and modernize enterprise applications' as a focus for the next 12 months, making it the third highest priority overall."

Axiad's experience with enterprise customers suggests that 1/3 of commercial applications or services do not yet support FIDO

Regardless of what we call them, most of these systems cannot use FIDO authentication processes or mechanisms. Axiad's experience with enterprise customers suggests that 1/3 of commercial applications or services do not support FIDO and need to rely on other mechanisms. Many of these default to password-based authentication methods, and therefore inherit the security and usability problems of password-only systems. An emerging best practice for these legacy solutions is to combine certificate-based authentication with knowledge-based systems, giving IT teams an additional, transparent authentication factor for greater security that doesn't impact or hinder users

[2] Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study

CHALLENGE #2: THE HETEROGENEOUS ENTERPRISE

As modern enterprises have evolved it's become more and more apparent there's no such thing as a "one-size-fits-all technology." Diversity has increased in modern networks rather than decreased:

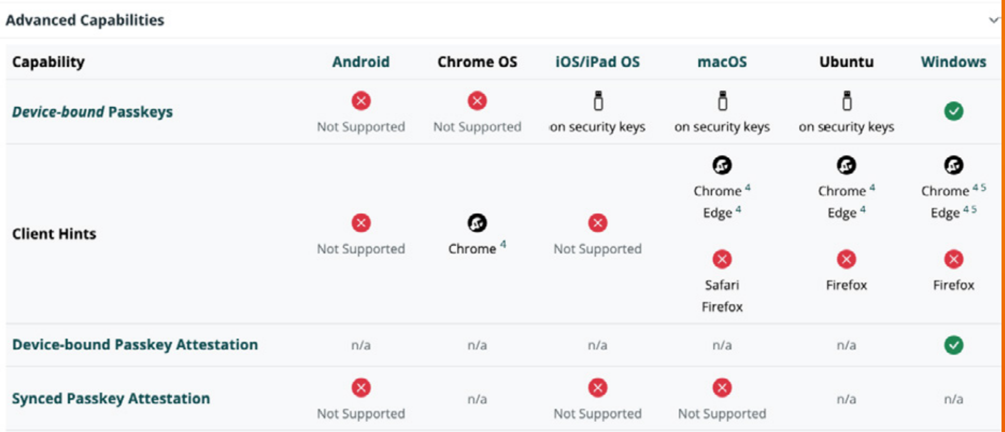
- The OS mixture continues to move towards a blend of platforms. Computerworld stated in 2023 that "Ten years ago, Windows held 85.6% of the US desktop share to macOS's 12.86%. Today, Windows is down to 53.43% and Apple has seized 31.34% share."[3]

- The same is true for Linux desktops as well, with Ars Technica reporting earlier this year that "Linux was on 6.34 percent of computers if you count ChromeOS."[4]

- Smartphones and tablets are distributed in enterprises at 70% or more using Android OS and 30% or more using Apple iOS.[5]

Why does this matter to an organization's FIDO strategy? It's possible FIDO support is not as heterogenous as your network is, or as deep as your plans are. While support for basic FIDO features is broad across platforms, support for advanced features – like startup from boot through user login, or the ability to use device-bound passkeys, or obtain device attestation – is rare on Windows machines, and shallower still on other platforms.

Organizations planning to replace their password-based authentication systems are best served by having a companion strategy that leverages another authentication method where FIDO is not yet a good fit.



Advanced Capabilities

Capability	Android	Chrome OS	iOS/iPad OS	macOS	Ubuntu	Windows
Device-bound Passkeys	✗ Not Supported	✗ Not Supported	on security keys	on security keys	on security keys	✓
Client Hints	✗ Not Supported	Chrome[4]	✗ Not Supported	Chrome[4] Edge[4] ✗ Safari Firefox	Chrome[4] Edge[4] ✗ Firefox	Chrome[4,5] Edge[4,5] ✗ Firefox
Device-bound Passkey Attestation	n/a	n/a	n/a	n/a	n/a	✓
Synced Passkey Attestation	✗ Not Supported	n/a	✗ Not Supported	✗ Not Supported	n/a	n/a

FIDO advanced functions, like the ability to use device-bound keys, are available for Windows systems, but that function (as well as other capabilities like "client hints" and attestation) is still not supported for non-Windows systems. (Source: https://passkeys.dev/device-support/)

[3] StatCounter data confirms Apple's Mac renaissance

[4] Linux market share passes 4% for first time; macOS dominance declines

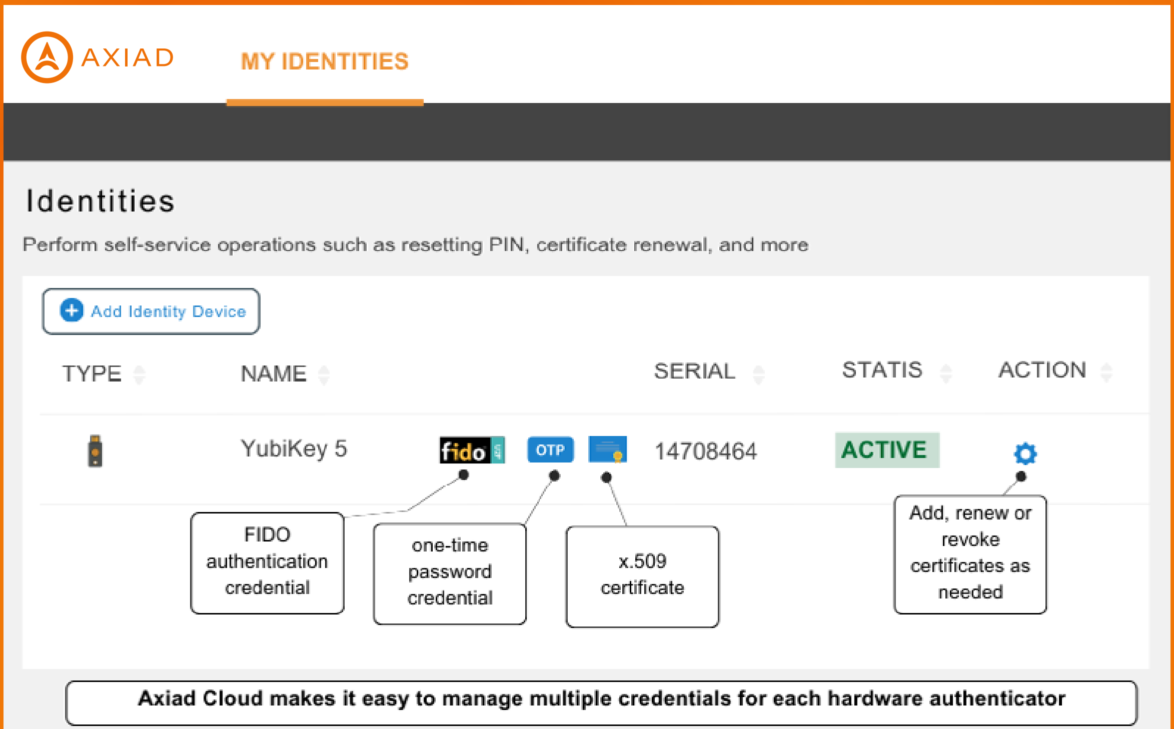
[5] Mobile Operating System Market Share

CHALLENGE #3: AIR-GAPPED AND ISOLATED ENVIRONMENTS

We're in an internet-connected world, so the "online" part of the FIDO name (Fast Identity "Online") seems self-evident. After all, the original purpose of FIDO was to streamline authentication to a subset of the 1.09 billion websites active on the internet today[6].

Yet air-gapped environments – those that use discrete infrastructure and methods and forego standard internet connectivity – are still "common in military, government, banking, utilities, and manufacturing" according to Gartner[7].

Despite claims that "the airgap is dead"[8] because of the ongoing convergence of IT, OT and IoT, many cybersecurity teams still use air gapped architectures to defend their most critical data. A 2023 report from ESG and KeepIt[9] showed that more than 1 in 4 organizations (27%) used air gap designs in their networks as a critical defensive measure. These environments cannot leverage cloud-based Identity products like Microsoft Entra ID, or cloud-based Identity and Access Management (IAM) products that provide a platform for FIDO-based authentication functionality. Instead, they need to leverage new or existing on-premises authentication solutions.



Identities

Perform self-service operations such as resetting PIN, certificate renewal, and more

TYPE	NAME	SERIAL	STATIS	ACTION
	YubiKey 5 fido OTP	14708464	ACTIVE	⚙

FIDO authentication credential

one-time password credential

x.509 certificate

Add, renew or revoke certificates as needed

Axiad Cloud makes it easy to manage multiple credentials for each hardware authenticator

[6] The Website Statistics for 2024

[7] Market Guide for User Authentication

[8] The Air Gap Is Dead. It's Time for Industrial Organisations to Embrace the Cloud

[9] Ransomware resilience: Why air gapping is your best defense

ADDRESSING THE CHALLENGES: FILLING FIDO GAPS WITH CERTIFICATES AND PKI

A powerful way to address these challenges is by layering in another authentication method to work hand-in-hand with enterprise-scale FIDO implementations. For this to work, the alternative must not only integrate well with FIDO, but it must also be cost-effective, understandable to architects and end users, and extensible.

Axiad's Certificate-Based Authentication (CBA) for IAM uses digital X.509 certificates to provision and manage authenticators and credentials for end users leveraging FIDO. By integrating with FIDO technologies as well as X.509 functions, the product creates a consolidated authentication experience across OSs, tokens, and location. The product enhances security and further reduces end user friction.

How does Certificate Based Authentication stack up to the 3 Challenges described in this brief?

- **Usability at Enterprise Scale:** It's not uncommon to find large, Global-2000 organizations managing hundreds of thousands of keys and certificates on a daily basis. For FIDO2 to be adopted at enterprise scales it needs the same sort of automation that solutions based on X.509 certificates leverage, but for the deployment, management and auditing of FIDO-based credentials.

  Axiad solutions provide this degree of enterprise-wide manageability. While no one should claim that certificate configuration and management is "easy," Axiad Conductor's Certificate-Based Authentication for IAM and PKI as a Service solutions dramatically and demonstrably reduce the overhead and IT burden of using certificates as transparent, strong authenticators at enterprise-wide scales.

ADDRESSING THE CHALLENGES:
FILLING FIDO GAPS WITH CERTIFICATES AND PKI

CONTINUED

- **The Heterogeneous Enterprise:** Certificate-based Authentication is ubiquitous. It's a key part of the ecosystem mentioned earlier that supports over 1 billion web sites in the world. Applying certificates to enterprise endpoints as an additional layer of authentication covers gaps in MacOS, Linux and Ubuntu systems cited earlier, as well as legacy systems still prevalent in many enterprise networks. If an organization wants phishing-resistant across the board for all device types, and wants to retire as many passwords as possible, it needs a blended authentication strategy that leverages both FIDO and Certificate-based functions.

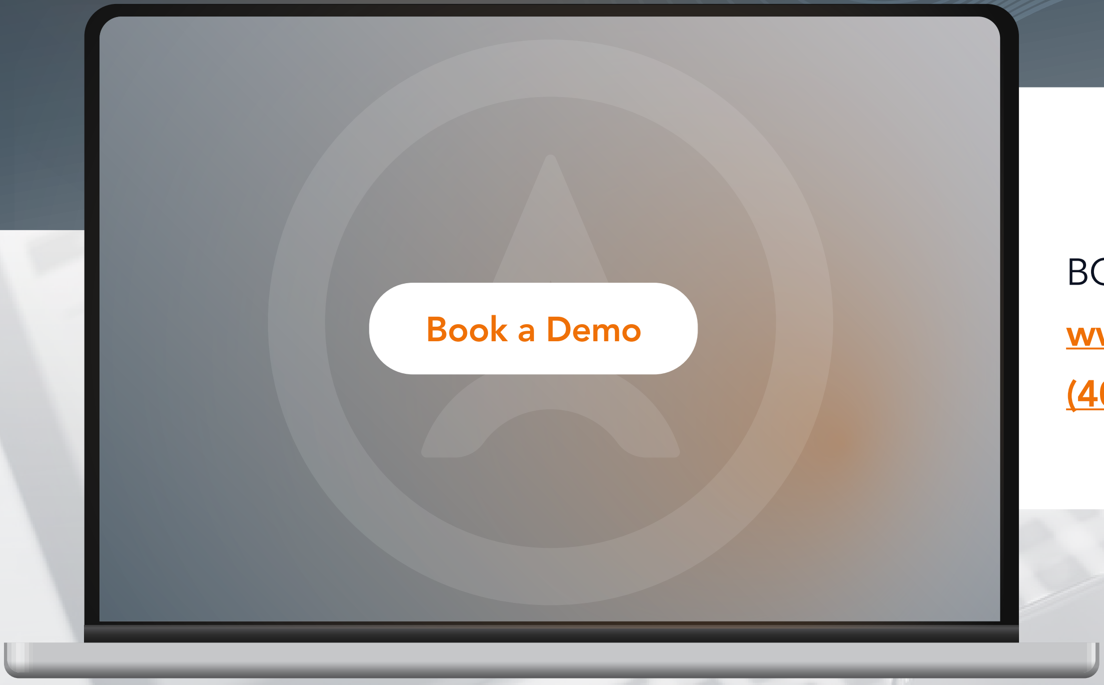
  In reality, FIDO2 was never designed for enterprise use: it was designed to protect the privacy of the end-users, a goal that often runs counter to an enterprise's need for centralized management. Because of this, the current standard makes it all but impossible to create a controlled rollout of passwordless implementations in the enterprise. The FIDO Alliance is working on addressing this gap, but certificate-based authentication methods are available today. These systems address the challenge of enforcing, controlling and reporting on the deployment of authentication at scale because the overarching schema was designed with many operational safeguards in mind. In fact, solutions like Axiad Conductor are now available that leverage manageability mechanisms built for certificate-based systems and can apply those6 capabilities to FIDO2 credentials. This solution achieves true phishing-resistant MFA across the largest of distributed modern enterprises.

- **Air-gapped and Isolated Environments:** Certificate-based Authentication can provide local machine-to-machine, client-to-server, internal hosts, or machine-to-intranet authentication even in internet-disconnected environments like air-gapped networks. Effectively, those environments where users need to access legacy or web applications hosted on-premises or in data-center servers, over the LAN/WAN or VPN, connected by Fiber, MPLS, or leased lines.

  Axiad's Certificate-based authentication supports a full range of authenticators, and even enables multiple authenticators, each with different credentials that can be assigned and managed per end user. In this manner, any mix of ongoing and temporary (project-based) authentications can be managed by a centralized system.

TAKE THE NEXT STEP

Axiad is proud to be a Board-level member of the FIDO Alliance. We're also proud to deliver solutions that work seamlessly with FIDO technologies to create end-to-end strong authentication solutions that are flexible, cover security gaps, and provide an unparalleled user experience.



BOOK A DEMO

www.axiad.com

(408) 841-4670.