AXIAD

Hardware-based Authentication at Enterprise Scale: A Streamlined Approach

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.

To provision and manage hardware-based authentication via certificates within an authentication management solution, several key steps can be taken:

- Certificate Issuance
- Device Registration
- Certificate Lifecycle Management
- Key Management
- Integration with Zero Trust Framework
- User Experience Optimization
- Phishing Resistant Multi-Factor Authentication (MFA) Integration

By provisioning and managing hardware-based authentication through authentication management solutions, organizations uphold strong Zero Trust principles while still delivering an optimized experience for users. Certificate-based authentication serves as a cornerstone of this approach, enabling secure and seamless access to resources while mitigating risks associated with unauthorized access and credential compromise.

OVERCOMING THE CHALLENGES IN SCALING

Cybersecurity leaders commonly acknowledge the effectiveness of existing authentication technologies, like FIDO and certificate-based methods, in safeguarding government users and systems. These tools have made strong authentication widely achievable. However, challenges arise in **deploying** these technologies at the **vast scale** and **diversity required by government IT**, including:

- Serving thousands of users with varying levels of skill and experience.
- Accommodating thousands of systems across different platforms and operating systems.
- Integrating on-premises, cloud-based, and hybrid systems, all while adhering to specific authenticator assurance levels and security protocols.

The main obstacle is not the availability of strong authentication technology, but rather the difficulty in automating the provisioning of authenticators and credentials on a large scale. This involves managing the entire identity lifecycle, including issuance, account recovery, renewal, and revocation processes.

Axiad Conductor addresses these challenges with comprehensive solutions designed for large government networks and organizations, offering:

- Lifecycle management.
- Support for a wide range of systems and platforms.
- A FedRAMP-ready framework.
- Seamless integration into existing authentication workflows.

Through automation and lifecycle management features, **Axiad Conductor enables** administrators to automate tasks, such as:

- Selecting authenticator options and credentials.
- Streamlining the rollout of MFA across the organization.
- Handling incidents efficiently.
- Facilitating credential renewal or resetting.

Meanwhile, **end-users benefit** from the ability to:

- Choose and enroll their preferred authenticators.
- Easily issue and manage credentials.
- Assist in account recovery without needing IT involvement.
- Renew credentials as needed, whether for account recovery or upon expiration.

Administrators set the list of permitted authenticators (e.g., YubiKeys, Smart Cards, Windows Hello for Business, Axiad ID mobile authenticator) and credentials (e.g., X.509 Certificates, OTP, FIDO2) for their organization and user groups. Users enjoy a self-service process where they can select an authenticator, enroll it with Axiad, and have the requested credentials automatically issued and stored on their device.

SUPPORT FOR HETEROGENEOUS ENVIRONMENTS

Enterprise networks are known for their complexity and diversity. **Axiad Conductor is designed to seamlessly operate within these multifaceted IT landscapes**, supporting a wide range of operating systems including Windows, Mac, and Linux. It is equally adept at managing environments with multiple Identity and Access Management (IAM) systems and can integrate with on-premises, cloud-based, and hybrid setups.

This broad compatibility empowers enterprise IT teams to standardize authentication practices, eliminating inconsistencies and vulnerabilities in user authentication across their complex infrastructures. As a result, the management of large and intricate authentication systems becomes simple: systematic and reliable, and enhancing overall cybersecurity measures.

Axiad Conductor's flexible framework ensures that as federal networks evolve, introducing new technologies and expanding capabilities, administrators have the tools needed to sustain consistent authentication practices across different platforms, technologies, and operational models. This adaptability ensures that security protocols remain robust and unified, regardless of the network's complexity or growth.

NO IMPACT TO YOUR AUTHENTICATION WORKFLOW

- Best of all, you and your teams determine what your authentication workflow and individual tools will be, based on organizational standards, risk levels, or best practices. **Axiad Clonductor acts as a mediator across your authentication and authorization technologies**, allowing the use of UserID/ Password authentication, Legacy MFA (Push Notifications), or MFA with options for certificate-based authentication, FIDO2, and more.

- With Axiad Conductor, enterprise IT teams can efficiently **roll out authentication to groups of end users** while optimizing individual workflows: some groups of end users can leverage strong authenticators (like YubiKeys or Smart Cards) while others use lower-friction methods when authenticating into daily systems. The status of the entire rollout is tracked, so IT teams can view progress and adjust workflows or requirements as needed.

- Axiad Conductor empowers you and your teams to **customize your authentication workflow** and select the tools that best align with your organization's standards, risk assessments, and best practices. It serves as a versatile intermediary for your authentication and authorization needs, supporting a range of methods from traditional UserID/Password and Legacy MFA (such as Push Notifications) to more advanced options including phishing resistant certificate-based authentication and FIDO2.

- This flexibility allows IT teams to **implement authentication solutions** that cater to the specific needs of different user groups within the organization. For instance, some users might benefit from stronger authentication methods like YubiKeys or Smart Cards, while others might prefer less intrusive options for daily access.

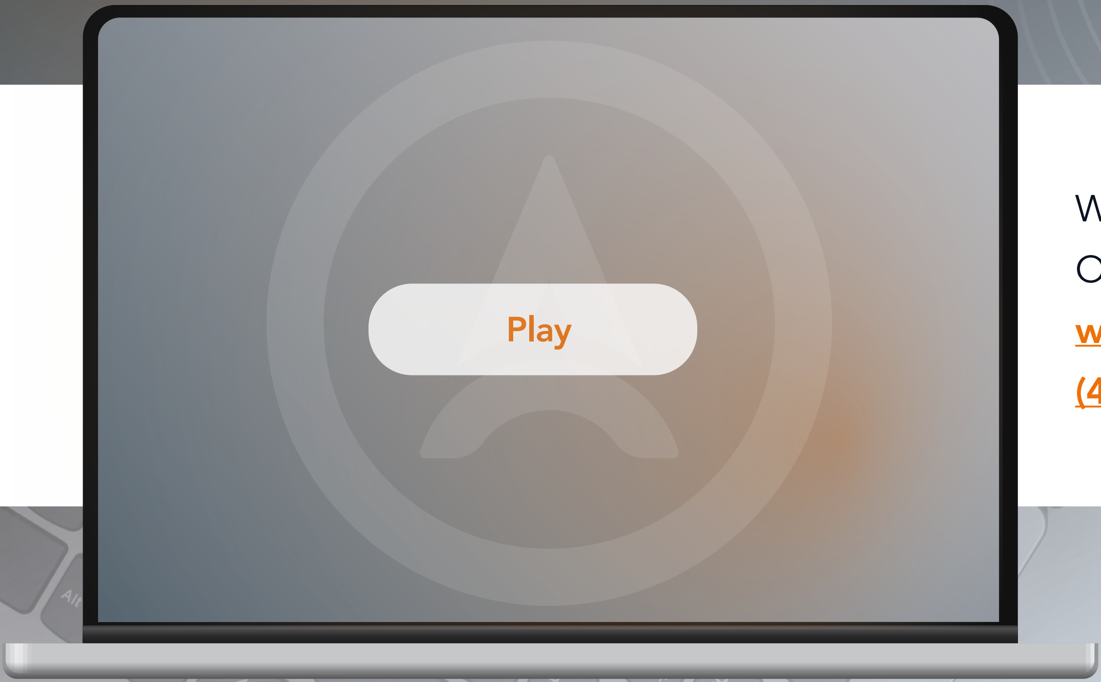
SCALE IS EVERYTHING:

An enterprise security architect at a retailer of over 10,000 employees said of Axiad Conductor:

"Our associates are very happy not to need their password for most situations anymore. It's very user-friendly – we're issuing YubiKeys for our corporate users and they just plug it in, go to the Axiad Conductor portal, and click the issue button. It's a couple of steps."

AXIAD CONDUCTOR SOLVES THE MANAGEABILITY PROBLEMS OF HARDWARE-BASED AUTHENTICATION

As the need for "phishing-resistant MFA" becomes a CISA battle cry, look for the hardware-based authentication deployments to mushroom in size while they're increasing in numbers. Organizations will be judged not on how many keys they bought and have in storage, but on how many are deployed and in use, protecting users and their machines. Axiad Conductor makes enterprise-scale deployments of strong authentication not only possible, but sustainable.



WATCH THE VIDEO
OR CONTACT AXIAD
www.axiad.com
(408) 841-4670.