Certificate-Based Authentication (CBA) for IAM

Datasheet

Challenges

Increasingly, phishing attacks are taking a toll on organizations. In particular, attacks on remote workers are rising dramatically.

Implementing passwordless and phishing-resistant authentication with certificates is an effective way to master complex environments with high numbers of end users. However, most Identity Access Management (IAM) systems do not provide these capabilities and most organizations do not have the resources to create a custom approach.

Certificate-Based Authentication (CBA) delivered as an add-on to IAM is the optimum way for organizations to stop phishing attacks while getting more out of their IAM investments.

Authentication Challenges

70% Use 3 or more IAM systems

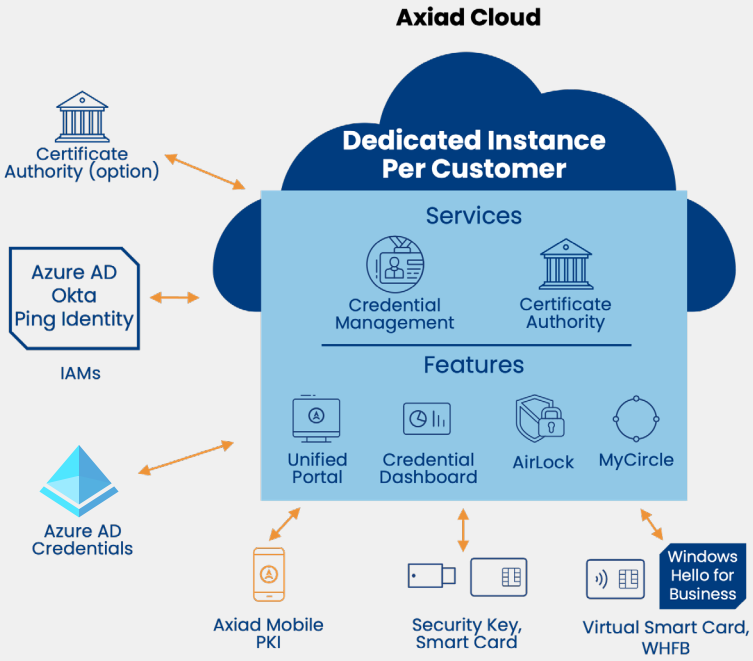
89% Use 3 or more authentication methods

83% Authenticate to 2 or more OSs

Product Overview

Leveraging the power of the Axiad Cloud and as an add-on to IAM products, Axiad Certificate-Based Authentication (CBA) for IAM provisions and manages Phishing-Resistant authenticators and credentials for end users everywhere. By creating a consolidated authentication experience across OSs, tokens, and location, the product both enhances security and reduces end user friction. Axiad CBA for IAM helps organizations go beyond the built-in functionality of their existing IAM solutions to address authentication in an integrated fashion across the organization.

Certificate-Based Authentication for IAM



How CBA for IAM is unique

- **Extends IAM:** Provisions and manages passwordless, phishing-resistant MFA authenticators seamlessly to existing IAM systems at scale
- **Enhanced Credential Management:** Credential Dashboard uniquely provides visibility into all end user authenticators, including Microsoft Authenticator, Windows Hello for Business, Security Keys, and more
- **Consolidated:** IT can get a consolidated view of all the users MFA authenticators and manage them from one place
- **Efficient:** Replaces use of multiple tools for rollout, management, and support of authenticators and credentials

Key Features

Consolidated: Serves all authentication needs, everywhere across the environment

- **Extends IAM:** Provisions and manages passwordless, phishing-resistant MFA authenticators seamlessly to existing IAM systems at scale
- **End-to-end Security:** All entities are secured without using passwords or shared secrets so the authentication process is secure from end-to-end
- **Standards-based Certificate:** Leverages an international standard X.509 certificate to interoperate across a broad range of vendor products
- **Passwordless Multi-Factor Authentication (MFA):** Utilizes multiple types of authentication methods without a password or push notification that can be intercepted or phished
- **Phishing-Resistant Authentication:** Delivers a broad range of phishing resistant authentication based on FIDO2 and WebAuthn with Authenticators ranging from enterprise-grade mobile-based to government-grade AAL3

Consistent: Ensures consistent authentication across OSs, applications, services, and more

- **Broad OS support:** Secures login to Microsoft Windows, Apple OSs, Linux, and more
- **Windows-friendly:** Provides authentication across Windows ecosystem including Azure, Windows OS, and more
- **Authenticators:** Enables organization to support any / all authenticators
- **Integrated:** Supports wide range of protocols, connectors, and standards for interoperation across the Identity ecosystem out of the box

Efficient: Increases IT and end user efficiencies at scale with automated, streamlined workflows

- **Unified view of all MFA credentials:** Manages all MFA credentials, including Azure AD's issued credentials such as Windows Hello for Business and Microsoft Authenticator
- **Unified Portal:** Streamlines work and automates tasks for both IT and End Users across the organization
  - » **Single Pane of Glass:** Delivers all functionality including custom workflows for both IT and End Users
  - » **Airlock:** Provides help desk automation by eliminating temporary passwords, automating administration, and enabling self-service credential management
  - » **MyCircle:** Empowers self-service by enabling the workforce to issue department-level credential resets, thereby avoiding temporary passwords and increasing efficiency for IT and end users
  - » **Certificate Workflows:** Supports a range of certificate request and delivery workflows

Platform Capabilities: Leverages Axiad Cloud Platform capabilities including secure design, convenient implementation, and more.

Benefits

Get More from Your IAM

Provide your IAM with a superior user experience, reduced admin, and greatly enhanced security, thereby getting more from your investment

Move Beyond Passwords

Deliver better enterprise-wide security controls that go beyond passwords that are relatively simple to compromise in multiple ways

Automate MFA Processes

Automate processes and checklists (e.g., enforcing initial smart card setup) before an employee can gain full access to company systems

About Axiad

Axiad delivers organization-wide passwordless orchestration to secure users, machines, assets, and interactions for enterprise and public sector organizations that must optimize their cybersecurity posture while navigating underlying IT complexity. The company's flagship offering, Axiad Cloud, is a comprehensive, secure, and integrated authentication platform that allows customers to move to a passwordless future without the friction and risk of fragmented solutions. Axiad supports the widest range of credentials in the industry including FIDO, mobile MFA, Windows Hello for Business, YubiKeys, smart cards, TPM and biometrics.