Interim and Non-PIV Authentication

USE CASE

Overview of Use Case

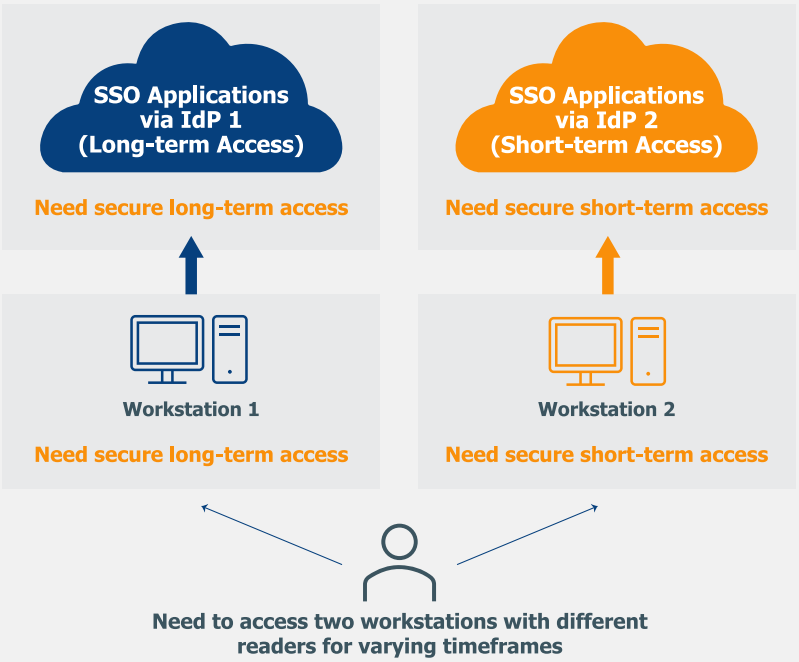
Federal Agencies must adhere to standards for phishing-resistant authentication. Existing systems are set up to utilize PIV cards. Yet, it can take six months to obtain a PIV card for a new employee and weeks to replace a lost card. Many consultants are ineligible to receive a PIV card yet must be provided secure access over long timeframes. Further, employees and contractors often need short term access only for a given project or for a set timeframe. Lastly, PIV cards are not read by all devices. For these needs, agencies today rely on weak authentication methods. So, how can interim authentication be made phishing resistant?

The answer is that flexible management of authenticators (e.g., Smart Cards and USB Keys) is needed to provide interim yet phishing-resistant authentication. This authentication must be able to handle diverse uses such as workstation logon and short-term (with a fixed end date) application access.

Challenges for Federal Agencies

Federal agencies require interim phishing-resistant authentication for a range of scenarios:

- **Complex Environment:** Multiple operating systems, workstations, Identity Providers (IdPs), and more.
- **Mix of Authenticator Readers:** Lacking a PIV reader, workstations may drive the use of a particular authenticator.
- **Mix of Ongoing and Temporary Access:** Even long-term employees and contractors are likely to require temporary access for a given project.
- **Multilayered Secure Access:** Authentication is needed at each layer.
- **Multiple Authenticators:** Individuals may need to authenticate to multiple workstations at the same time and so need multiple authenticators to be activated and maintained, each with discrete authentication credentials.



Federal Agencies need interim phishing-resistant authentication that spans all the scenarios where a PIV card approach isn't feasible

Introducing Axiad Cloud

Overview

Axiad Cloud is a comprehensive, efficient, and secure authentication SaaS platform that eliminates silos across the environment. Architected for best-practices security, it enables "mix-and-match" use of the Axiad Cloud product line. It can be applied in heterogeneous IT environments – e.g., organizations operating Windows, Mac, and Linux operating systems or with multiple existing IAM systems in place – allowing organizations to remove gaps and inconsistencies in how they authenticate across complex ecosystems, and ultimately to become more programmatic in their overall cybersecurity practices.

Capabilities

- **Comprehensive:** Supports all authentication methods across users, machines, and more while interoperating with the entire Identity ecosystem
- **Efficient:** Streamlines and automates help desk workload, enables end user self- service, and minimizes overall IT overhead
- **Secure-by-Design:** Architecture designed with best-practices security including a private instance for each customer, key storage in specialized hardware, and encrypted communications.

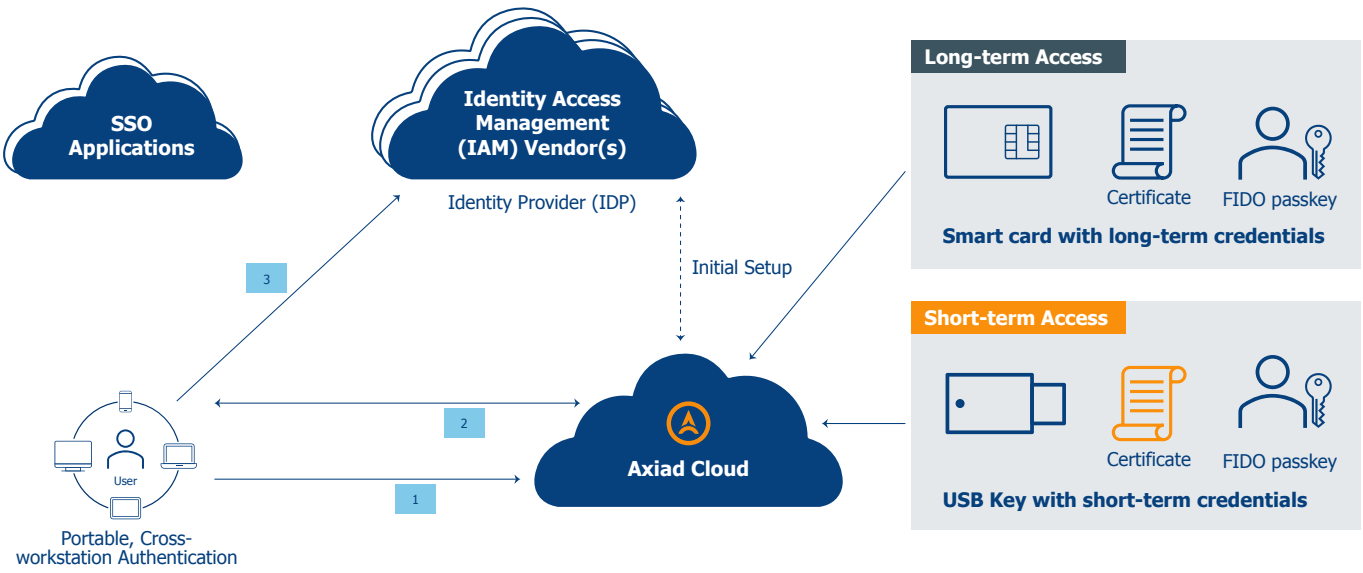
Interim and Non-PIV Authentication Management Lifecycle – One Example

Leveraging the Axiad Cloud platform, Axiad provides flexible and consistent Authentication Management focused on the authenticators and credentials required for each authentication operation (such as accessing a workstation versus an application). Key functionality:

- Broad Authenticator and Credential support: Axiad supports a broad range of phishing-resistant authenticators including PIV cards, Smart Cards, and USB Keys as well as credentials including FIDO passkey and certificates.
- Multiple Authenticators and Credential Management: Multiple physical authenticators, each with a unique set of credentials, can be assigned to and managed for each end user.
- High Security Practices: To maximize security, Axiad ensures that the appropriate authenticators and credentials are enrolled prior to workstation authentication. Further, Axiad supports workstation authentication as a prerequisite to application access.
- Broad environment support: Authentication across Windows, Mac, and Linux, across devices, and across IAM vendors – who provide the Identity Provider (IdP) functionality – are all supported.
- Unchanged authentication: While it leverages the appropriate authenticator and credentials, Identity Provider (IdP) authentication processes are unchanged. As an option, Axiad can also act as an IdP.

Interim and Non-PIV Authentication Use Case

Authentication Management – One Example



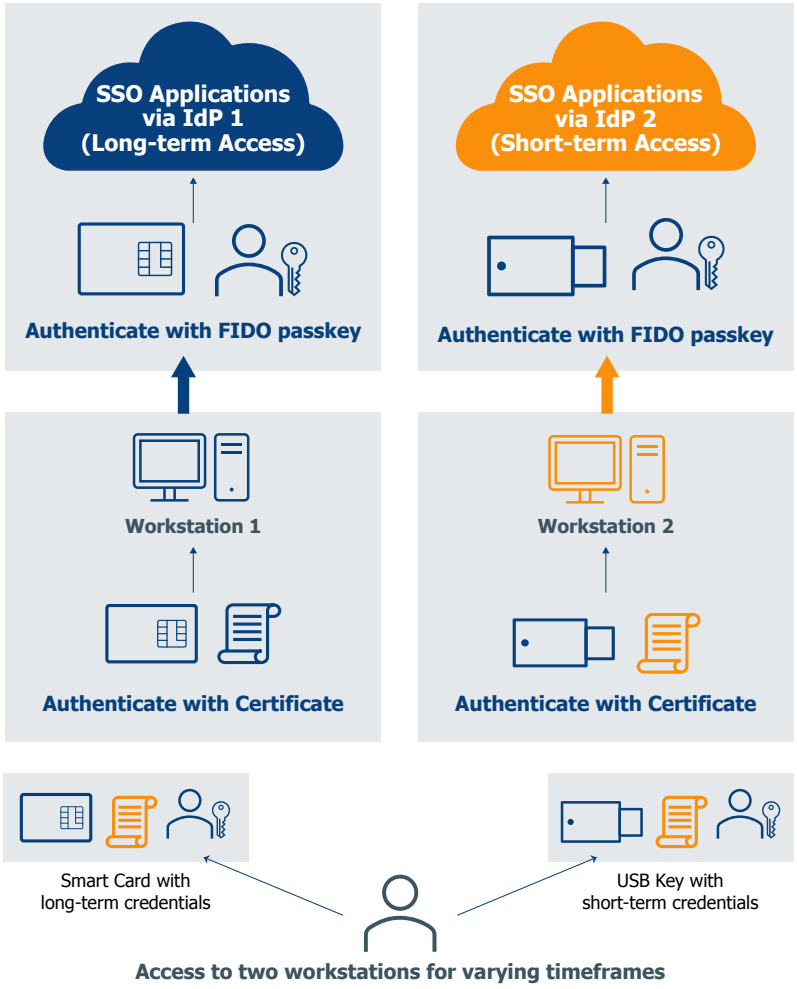
1 **End User registers Authenticator** 2 **Authenticator is enrolled with assigned credentials** 3 **IdP authentication processes are unchanged**

Axiad centralizes Authentication Management – including phishing-resistant authenticators and custom credentials – across diverse environments including Windows, Mac, and Linux

Interim and Non-PIV Authentication In Use – One Example

With the appropriate set of authenticators, credentials, and expiration dates defined, interim authentication is precisely controlled and phishing resistant to maximize security and minimize end user friction. In this example, Smart Cards and USB Keys are chosen by the Agency due to their ability to be read by the appropriate workstation. Key functionality:

- **Multilayered Secure Authentication:** By supporting the issuance and maintenance of multiple credentials, each authentication process such as initial authentication to the workstation and each subsequent application access can be controlled by a custom credential.
- **Custom Durations:** By being able to create customized certificates, each set of interim needs can be precisely addressed with pre-set expiration dates.
- **Choice of Authenticator Form Factors:** A wide range of authenticator options enable matching to the workstation reader.
- **Mix of Ongoing and Temporary Access:** By setting the expiration date of factors and whether they are renewable or expire on a fixed date, a mix of ongoing and temporary access can be flexibly defined for each end user and each project.
- **Multiple Devices:** Individuals may need to authenticate to multiple devices at the same time and so need multiple authenticators to be activated and maintained, each with discrete credentials.



Federal Agencies can leverage centralized Authentication Management that provides flexible phishing-resistant authentication for the gamut of interim needs

Unique Authentication Management Capabilities

As of this writing, Axiad's approach provides capabilities that cannot be matched elsewhere:

- Consistent phishing-resistant authentication: All authentication steps can be made phishing-resistant even for interim needs.
- Multiple device use: Multiple authenticators can be issued and efficiently manage to enable the use of multiple secured devices at the same time.
- IT efficiencies: IT efficiencies are maximized via leveraging Axiad's utilities for authentication lifecycle management.

Benefits for this Use Case

Rock Solid Security

Government-grade phishing-resistant authentication can be enforced for each interim authentication need

Productivity Improvement

By eliminating the wait for authenticators, productivity can be improved by weeks to months

Match "Need to Know"

With precise yet flexible controls, authentication for each project can match the "need to know"

axiad

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.