CYBER ARMED

MFA

THE PIV WAY

A guide for using PIV to strengthen MFA security architectures.

Introduction

MFA Done Properly

Although implementing a Multi-Factor Authentication (MFA) system can drastically improve security, if not properly thought out, the MFA system itself can remain vulnerable to attacks as well as fail to deliver the long-term security benefits to justify the investment. Furthermore, the MFA system often introduces proprietary technologies that prevent organizations from scaling their MFA capabilities requiring different MFA solutions for different business and security needs.

This guidebook introduces the advanced security and compatibly benefits of the NIST Personal Identity Verification (PIV) security model. Our goal is to help IT and security managers understand how they can leverage PIV to implement an effective MFA solution capable of meeting both immediate and future compliance and business needs.

Contents

Chapter 1

MFA - The Basics

Multi-Factor Authentication (MFA) is a powerful security tool that can help eliminate many of the biggest vulnerabilities an organization can face. Given that some of the largest data breaches have occurred by either guessing or stealing passwords, implementing an MFA based access control system can drastically protect organizations by eliminating one of the weakest links in the chains...passwords.

The Reason MFA Is So Powerful

MFA systems force end users to use more than just a password to log in to the system. In addition to something they know, they also must possess a token (something they have) or have a physical trait such as fingerprints, iris or face that is unique to them. Employing these multiple factors during an authentication process drastically increases security because an attacker is very unlikely to steal the factors to impersonate the user.

Traditional MFA Issuance Models

Organizations that invest in MFA typically follow a two-step issuance model. 1) User's sponsor requests the credential, 2) IT operations will distribute the credential to the user. The user can then use their credential to successfully complete the authentication process for the MFA protected resource.

Sponsorship

An existing employee creates a request for the new user to receive the MFA credential.

Credential Activation

The MFA credential is initialized and made ready for use.

Traditional MFA Limitations

Although traditional MFA systems do a great job at eliminating passwords, there are many security controls that are often overlooked that could render an MFA system useless. Furthermore, many MFA systems lack full cryptographic functionalities to enable organizations to use MFA tokens for encryption or other access control scenarios.

Traditional MFA systems do not cover

• Traditional MFA systems do not cover

• Identity Verification: Applicants are only verified by easy to fake information.

• Collusion Prevention: The approval process typically requires only 1 person.

• Credential Distribution Integrity: The credential is distributed without ID verification.

• 2(+) Factor Authentication: The factors are limited to only 2.

• Limited: The credential cannot perform encryption or be used for physical access.

• Partner Interoperability: The credential cannot be used by business partners.

Think Long-Term

It is important to understand traditional MFA limitations to ensure investments can be utilized for a long-term, scalable solution.

Traditional MFA System Risks

Although MFA systems are designed to provide additional security, if not properly implemented, they can actually add additional risks to the environment if the wrong person ends up getting a valid MFA credential or if the token does not perform the security action required for compliance.

MFA Business and Security Risks

Impersonation: An unauthorized user posing as an authorized user receives a valid credential.

Collusion: An unauthorized user issues a credential to themselves.

Credential Theft: An unauthorized user gets a credential and registers themselves as the valid user.

Limited Functionality: The credential cannot perform encryption resulting in having to rely on a different encryption process.

Partner Interoperability: The credential cannot be used by business or government partners resulting in new credentials being issued.

Don't fail your audit (or waste money)

Traditional MFA systems are prone to well known attacks and may not even meet all of the organization's needs.

Getting more ROI from MFA

It is critical an organization carefully plan their MFA strategy to include the different security needs for their end user and corporate security policy. While many MFA systems are great at performing general logical access authentication, they lack the additional security features to perform encryption, digital signature or physical access which can cause an organization to have to purchase multiple access control system platforms.

Do More

Traditional MFA credentials that only do logical access lack encryption and physical access capabilities.

Common Reasons MFA Systems Fail To Meet Business Needs

Lack of Cryptography Services: The organization also needs to encrypt data however, the MFA credential only provides authentication services.

Cannot Open Doors: The MFA credential only works with logical systems and cannot be used for physical access.

Not Compatible with Business Partners: The MFA credential uses proprietary technology that is not compatible with business partners.

Weak Level of Assurance: The MFA credential cannot meet a high LOA required for sensitive transactions.

Chapter 2

Introducing PIV

The Personal Identity Verification (PIV) specification is a security model published by the National Institutes of Standards and Technology (NIST) designed to solve the security vulnerabilities impacting identity systems while also ensuring interoperability.

Why Use PIV?

PIV drastically increases security by using advanced identity proofing techniques to verify the user, separation of duties to prevent collusion, and an enhanced credential distribution model to prevent an unauthorized user from using a stolen MFA credential. Finally, the PIV MFA credential can support physical access controls, encryption transactions, and other security features to allow the MFA token to be used for many different security needs.

MFA Security Features	PIV	Traditional
Identity proofing	✓	✗
Separation of duties	✓	✓
Secure credential distribution	✓	✗
Credential interoperability	✓	✗
Auditing	✓	✓
Physical access	✓	✗
Encryption	✓	✗

How PIV Strengthens Traditional MFA

As described previously, the traditional MFA issuance model is typically comprised of a two step issuance model where the credential is given to the user after a basic request. PIV significantly strengthens this model by incorporating three additional security processes to accurately identify the user, prevent collusion and ensure the token is distributed, and initialized for the proper user.

Sponsorship:
An existing employee creates a request for the new user to receive the MFA credential.

ID Proofing:

The user's identity attributes are collected and verified to ensure the person is who they claim to be.

Suitability:

A separate security officer reviews the documents and approves the user for a token to ensure no one person can override the process.

Secure Credential Distribution:

The user is verified via biometric or authorized official to prove the MFA credential is properly assigned to them.

Credential Activation:
The MFA credential is initialized and made ready for use.

Chapter 3
Identity Proofing

One of the biggest threats to an authentication system is an unauthorized user successfully impersonating an authorized user. Advanced cyber-attacks often exploit such identity verification vulnerabilities in order to obtain valid credentials allowing them complete access to an otherwise well-defended system. This attack is devastating because there are no signs of illegitimate activity because the attacker has successfully authenticated and appears to be a valid user.

The PIV issuance model uses identity proofing processes to help prove the person is who they claim to be. Extra steps are taken to capture the user's identity documents and attributes in a manner that can be used to verify the person's identity.

Identity Proofing Levels

NIST has developed a framework known as the Digital Identity Guidelines that provide a standard way of verifying a user's identity. In summary, they create 3 different categories of proofing level scored from 1 (being the least trustworthy) to 3 (being the most trustworthy).

NIST Information Assurance Level 1:

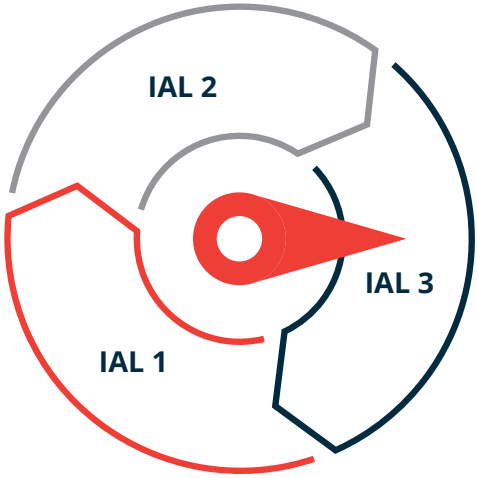
No verification - trust the user is who they claim to be.

Level 2:

Address confirmation, one form of government identification.

Level 3:

Address confirmation, two forms of government identification, biometric capture.



Proving Identity With Biometrics

Biometrics refers to physical characteristics a person has such as fingerprints, facial details, and eye (iris) information. A person can be uniquely identified using biometrics with a very high rate of accuracy making the identity proofing process much stronger and resilient to fraud or unauthorized access.

Facial Recognition

Iris Identification

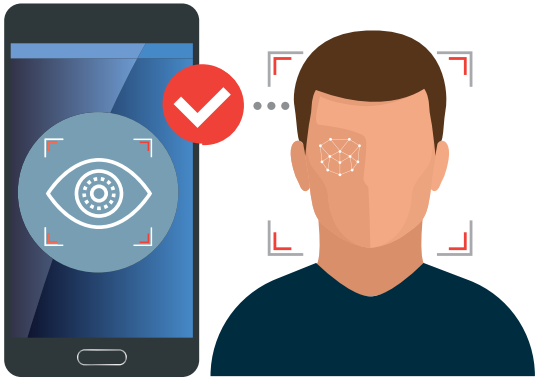
Fingerprint Identification

Popular Biometric Modalities

Face: The user's photograph is taken and is later manually and electronically verified to prove the person's identity.

Fingerprint: The user's fingerprints are captured and then later used to verify the individual, before issuing a credential.

Iris: The specialized camera will capture a detailed image of the user's iris for verification.



Capturing Biometrics

Through standardization, PIV has evolved the way biometrics are taken which make biometric capture solutions much more accessible to commercial organizations, and much more practical to implement. For example, the standardization has eliminated many once proprietary barriers which have created a marketplace of biometric products that are simple to install and easy to use.

Biometric Capture - Easier Than Ever

Organizations have much more flexibility in the biometrics they choose to collect. For example, they have the options to capture a photograph, iris biometric, or set of fingerprints. They can also capture all three to significantly strengthen their security process. Finally, the software performs all the necessary cropping, segmentation, and scoring automatically to make the capture process significantly easier on both the organization and applicant.

State Of The Art Hardware

Thanks to PIV, the biometric hardware market has drastically evolved in the last decade resulting in many different options for capturing fingerprints, iris, and facial features. Organizations now have a wide spectrum of practical options to implement strong identity proofing security controls into their security processes.

Suprema RS-D

IRIS ID - Iris Capture

Suprema G10

Ziggy HD - Photo Capture

Mobile Capture Station

Chapter 4

Suitability Check

One of the biggest threats to a credentialing system is the ability for one person to override the entire process and issue a credential for themselves. When this occurs, the person's actions are extremely hard to trace and detect because they appear to be legitimate users of the system.

Multi-Person Verification

PIV implements a suitability check process whereby a separate security officer will review the request and identity proofing documents of the applicant and then make a decision whether to move forward with the credential issuance process. This additional step makes collusion and system override nearly impossible.

Chapter 5

Secure Credential Distribution

Another vulnerable area of an MFA system is the way in which the person actually receives their MFA credential. If this process is not well controlled, an unauthorized user could impersonate a valid user to receive and activate their credential.

To secure the credential distribution process, PIV uses a two-phase security model to first link the credential to the user and second, to authenticate the user through biometrics or via an authorized officer. These security steps ensure the credential is sent to the correct person and that person has been verified before the credential is activated.

PIV Credential Distribution Process	
Link	The credential is linked to a user and a unique one-time pass-code is generated and sent to the user.
Distribute	The credential is securely distributed to the user.
Verify	The user is verified via pass-code, in person, and/ or biometric.
Activate	The credential is activated and loaded with user specific information.

Chapter 6

Creating a PIV based MFA Capability

Implementing a PIV based MFA system is more realistic than most people expect. For example, the HID™ PIV Express bundle contains all of the necessary hardware and software to implement all of the PIV security and interoperability features. There are also professional service packages that are designed for rapid installation.

Step 1: Plan

Determine the security services required from the MFA credential. For example, encryption, physical access, visitor management, mobile security, business, and government partner access.

Step 2: Install

Install the PIV Express server, biometric station, and activation kiosks. Connect to existing HR directories and begin the PIV based MFA processes to issue secure credentials.

Step 3: Train

Train security officers, auditors and end users on the functions of the PIV credential issuance and usage process.

Step 4: Expand Use

Consolidate different MFA systems to reduce overall security costs. Begin to issue mobile derived credentials and use the credentials streamline and secure business transactions.

The Real-World Value of PIV

The PIV specification, tools, and mythologies have been tested and evolved over the past decade. In this time, many customers have realized the true value of PIV once they harness its power. Below are real-world examples of how customers have used PIV to simultaneously improve security and create efficiencies in their business operations.

Replaced different proprietary MFA solutions with the single PIV credential to save licensing and hardware fees.

Eliminated third party encryption services and software licenses in favor of using the PIV credential for full disk encryption.

Passed a compliance audit when the regulation specified a strong form of authentication because the PIV credential is already compliant at the highest security (FIPS) level.

Eliminated expensive MDM software and digital certificates by leveraging the PIV derived credential model.

Streamlined on-boarding processes by providing 1 Smart ID Badge (PIV Credential) for both physical and logical access.control.

Conclusion

(PIV Based) MFA Is The Future

As the cyber threats multiply and the security regulations continue to require stronger security controls, MFA will continue to become one of the most important measures organizations can take to protect their resources and achieve compliance. Whether implementing a new MFA capability or expanding an existing one, consider the security and interoperability principles of PIV to ensure your MFA is both protected and scalable for the long term.

If you are interested in learning more about PIV, visit us at www.cyberarmed.com or send an email to info@cyberarmed.com. We have videos, blogs, and tutorials to help you learn quickly. If you want to get started implementing immediately we also have turnkey PIV systems, professional service packages and a wide selection of hardware and software to meet your PIV needs.

CYBER ARMED

Identity & Credentialing Experts[tm]

3100 Wilson Blvd, Suite 200, Clarendon, Virginia 22201
www.cyberarmed.com | info@cyberarmed.com