

A Practical Road Map for Implementing PIV

PAPER HIGHLIGHTS

- Synopsis of how PIV works in common security transactions
- Associates PIV transactions with complexities and infrastructure requirements
- Provides guidance to create a practical plan to carefully integrate PIV

Goal of This Document

This white paper provides a practical roadmap for implementing PIV in a manner that will produce the most effective results while minimizing the complexity and frustration for the end user. The goal is to be able to introduce PIV in a manner where the end user can safely get experience with the card while still be able to perform their job tasks. As they gain more confidence, and technical administrators work out configuration bugs, the organization will be able to introduce additional PIV uses to significantly improve security operations and glean a true return on investment on their efforts.

Introduction

When integrating PIV, an easy mistake to make is to start the implementation without an overall strategy to ensure the organization carefully introduces the technology in a manner that considers the end user's ability to learn how to use the card while also ensuring the technology staff and infrastructure can adequately support the associated requirements. This has led to various forms of technology pushback, unneeded implementation frustrations and overall dissatisfaction with PIV technologies. For example, scores of users, administrators and executives have grown frustrated because of problems relating to being locked out of their systems, encrypting data for which they cannot decrypt and waiting an excessive amount of time to perform basic operations.

Why is this? The answer is simple...too much, too soon. The fact is PIV bundles numerous sophisticated security technologies that have not been fully understood and adopted despite being in the market for years. For example, cryptography software once only usable by the mathematically elite is now a PIV standard feature that must be learned by all using the PIV card, regardless of their computing knowledge or sophistication.

This is a good thing! Although the PIV technologies are much more complex than the current systems people use today, they have arrived just in time. As our computing infrastructure reaches a level of complexity unfathomable only a few years ago so too have our security threats. Now, organized computer crime syndicates and terrorist organizations have established a scalable hacking infrastructure comprised of malware, psychological traps and binary attack vectors rendering today's current security solutions useless.

How PIV Works – Understanding the PIV Security Transaction (PST)

The features of the PIV card enable multifactor security transactions for numerous identification and authentication contexts including, identification, authentication and encryption. To understand how this works, the first thing is to define what a PIV Security Transaction (PST) is. A PST is defined as the physical or electronic usage of the PIV card and its contents to provide reasonable assurance that both the PIV card has been issued from a trusted source and that the holder of the card provides knowledge, possession and/or biometric data in order to prove that they are the proper bearer of the card.

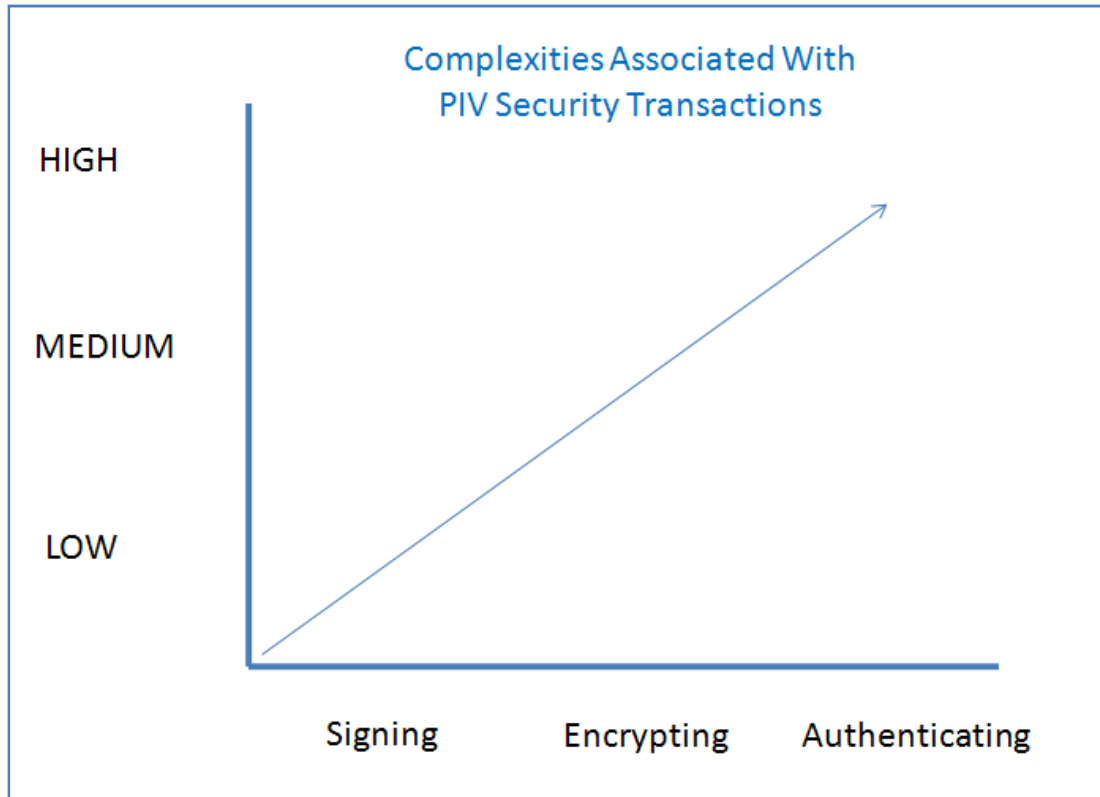
Differences in PST Complexities

PSTs can differ greatly in their complexity depending on the security and business context. For example, signing an email is much less complex than performing a computer based logon. At a very high level, the complexities can be attributed to the following:

- Length of validation path
- Number of cryptographic operations

Length of validation path: The process of making sure the PIV card is authentic, is trusted and has not been revoked is known as validation. During this process, various public key infrastructure (PKI) operations are performed to validate the digital certificates that are presented during the PST. What is important to understand is that depending on the PST, the validation path may be long or short. The longer the path, the longer the PST will take to complete. It is important to realize that the PIV card can utilize an entire system of authentication mechanism depending on how it is being used. Many of these systems are outside of the organization's control and may be a source of problems if not properly understood and managed.

Number of cryptographic operations: PIV is founded on sophisticated mathematical computations, known as cryptography, to provide security services on behalf of its cardholder. Cryptography, utilized in the context of a public key infrastructure (PKI), provides a scalable, robust mechanism to identify and authenticate and individual as well as make data tamperproof and unreadable except to authorized individuals. Although complex by its very nature, cryptography can grow drastically in complexity if the PST requires numerous cryptographic operations to be performed. For example, in the scenario of a computer based logon, cryptographic operations are performed in the digital certificates of the workstation, domain controller, certificate authority and all the systems defined in the certificate chain. If any of these fail, the entire transaction fails.

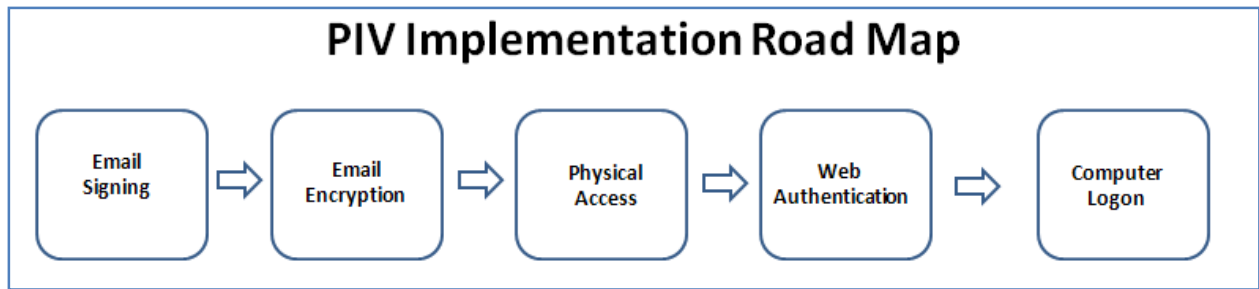


Creating a Practical Plan

The foundation of the plan should be focused on building the end user's experience and confidence with the PIV card through simple transactions that do not require extensive interaction from external systems. Thus, the goal should be, **start small and start local**. This is important for two reasons. First, it gets the user familiar with using the card and related software for a security transaction. Two, it allows the organization to begin to understand whether the hardware and software has been installed properly. It is critical to resolve all the installation problems with local PIV transactions before the more complicated uses begin.

The start small and start local design goal promote the following implementation sequence.

- 1) Email Signing
- 2) Email Encryption
- 3) Physical Access
- 4) Web Authentication
- 5) Computer based logon



PST Execution – Planning Factors

The PSTs selected were based on the following factors.

Factor	Description
Security Context	The security service the PST is providing. For example, a digital signature provides authenticity and encryption provides digital protection.
Infrastructure Requirements	The infrastructure required to perform the PST.
User Education	The amount of knowledge the end user must possess in order to consistently perform the PST successfully.
Transaction Sensitivity (what happens if it fails)	The ability of the PST to be completed without failure due to external system influences.
Security ROI	The impact the PST has on the organization’s overall security posture.

Email Signing

The first place to start is where the user spends a lot of time and there a heavy infrastructure is not required...Email signing. This process can help get the user involved with the operations of the card including, entering their PIN, and inserting the card properly. Also, if it does not work properly, they have a failsafe mechanism because they can choose to send the email without the digital signature.

Email Signing	
Security Context	Message Authenticity
Infrastructure Requirements	Low
User Education	Low
Transaction Sensitivity	Medium
Security ROI	Medium

Email Encryption

Using today's standard email systems, all messages are sent in a clearly readable format across numerous network nodes until they reach their final destination where they are then stored in the same unprotected manner. The result is simple, all email is insecure. To combat this, the PIV card can scramble the email and attachments in a manner where only the sender and recipient can view the contents.

Email Signing	
Security Context	Data Protection
Infrastructure Requirements	Medium
User Education	Low
Transaction Sensitivity	Medium
Security ROI	High

Physical Access (FASC-N Read)

The PIV card can be leveraged to greatly streamline this process by utilizing the standardized data stored within the Card Holder Unique Identifier (CHUID) field. Using simplified PIV Card CHUID reader software, the cardholder can use their card to provide their information in a matter of seconds. The security guard can then review this information to make a determination whether to allow the person to be checked in.

Physical Access	
Security Context	Identification
Infrastructure Requirements	Medium
User Education	Low
Transaction Sensitivity	Low
Security ROI	High

Web Authentication

One of the most promising uses for PIV cards is to reduce the number of passwords end users must remember to authenticate to different web based applications. When properly implemented, PIV authentication can be utilized to replace outdated password systems enabling the end user to use one PIN for logging on to their web application.

Web Authentication	
Security Context	Identification and Authentication
Infrastructure Requirements	Medium
User Education	Medium

Transaction Sensitivity	Medium
Security ROI	High

Computer Based Logon

Due to the number of steps the user must perform begin the logon process, the systems required to validate the PIV card and the length of time required to provide the user feedback, using the PIV card to logon to a workstation may be the most technically challenging PIV security transactions the end user can perform. During this PST, numerous validation and authentication activities are taking place that are sensitive to network loss, end user error or data inconsistencies. If any of the activities are interrupted, the logon process will fail and the end user will not be able to logon to their computer. The main concern is to ensure the user can still perform logon even if they are unable to do so with the PIV card. In the first months of deployment, domain administrators should ensure the users have a fail back mechanism to enable them to logon. If the user is unable to logon, they will be unable to perform their daily tasks which could greatly impact the perception of the PIV card.

Web Authentication	
Security Context	Identification and Authentication
Infrastructure Requirements	High
User Education	High
Transaction Sensitivity	High
Security ROI	High

Next Steps

Utilizing the install sequence defined in this white paper will help to ensure users become familiar with the card in a manner that minimizes confusion and frustration. Additionally, the organizations technology staff will be able to utilize the lessons learned from the more simple PSTs to implement more complex uses for the PIV card.

NOTE:

This White Paper is for informational purposes only. CYBER ARMED SECURITY, LLC MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

© 2009 CYBER ARMED SECURITY, LLC. All rights reserved.