

Preparing the End User for PIV

PAPER HIGHLIGHTS

- Why PIV usage is challenging
- How to help the end user
- Free tools and training

Goal of this document

The purpose of this document is to help prevent common end user problems with PIV integration. This material has been generated from numerous PIV and smart card deployments and should assist agencies in helping their end users begin to leverage PIV technologies.

Why PIV usage is challenging

As with the introduction of any new technology, the end user needs to be adequately prepared to understand how the change will impact their current routines and what will happen as the transition occurs. Without this understanding, technology adoption will be greatly hindered and the end user will ultimately find ways to work around problems they experience, thus defeating the purpose of integrating the technology.

PIV represents a revolutionary change for end users that combines numerous advanced security technologies that lack intuitive usability features and are extremely sensitive to failure. Compounding the challenge is that the user must use these new technologies (security token (PIV card), peripheral (card reader) and security software (middleware/PKI)) at the same time and if any one fails, they all fail with little or no explanation as to why. To achieve successful adoption of PIV, agencies must equip their users with the necessary knowledge to use their PIV card.

Understanding the end user experience

In the numerous deployments performed, certain patterns have emerged that tend to consistently provide challenges for end users which dramatically hinder the agency's ability to successfully integrate PIV.

- Not understanding the value of the card: In numerous instances, the end user receives their PIV card without any high level explanation of what the card is and its expected usage. The result is the end user perceives the card as just a "badge replacement" and does not understand the card is part of a security infrastructure upgrade that will drastically help to improve national security as well as streamline their identification and authentication efforts. Without a fundamental understanding that the card will be used to protect the end user's identity and their agency, they will be less likely to use the card as intended.
- New hardware: The end user must now interact with new hardware including the PIV card and a card reader. In many instances, readers lack visual or audio cues for correct card placement

and insertion thus resulting in numerous cases where the card is either inserted incorrectly (upside down/reversed) or not correctly pushed in all the way. This has led to numerous expensive help desk calls be initiated to troubleshoot a problem that is easily prevented.







- New actions: Low security transactions such as sending an email without a signature or authenticating with a username and password rely on a set of tasks end users are familiar with. The advanced security features of PIV require the end user to take additional steps such as inserting the card, obtaining recipient certificates, explicitly requiring message security options and other new actions they are not currently familiar with and may not fully understand.
- Poor visual cues and feedback: The software responsible for binding the card to the computer during a security transaction (smart card logon, digital signature, encryption, SSL, etc) provides very little feedback and requires a greater transaction time the end user must participate in. The increased duration combined with the lack of proper feedback mechanisms creates confusion and provokes the end user to terminate the action before it has been completed.

Helping the end user

Gleaned from PIV deployments, the following low cost techniques can be used to dramatically help the end user effectively use PIV in their daily job tasks to strengthen security. They help to provide; a clear understanding of what the PIV card is, specific training for users to perform common security functions and potential methods agency's can use to continuously improve the user experience.

1 - Clarity

A clearly understandable high level explanation of the PIV card security features greatly helps users understand what their card does and how to use it. The example cue card provides a simplistic mechanism to explain to the end user what is in the card and how it can help them. It is critical they grasp high level concepts before trying to delve into the low level technical features of the PIV card.

What's Inside	How it Helps You
 User Information	Rapid Identification
 Photo	Visual Identification
 Fingerprints	Prove your identity with fingerprints
 Identification Keys	Prove your identity
 E-Signature Keys	Prevent forgery
 Data Security Keys	Protect information

2 - Training

Once the user has a high level understanding of what the card contains and its purpose, they should next receive basic training on how to perform the tasks. We recommend starting with email signature (see our practical PIV implementation paper for details).

3 - Proactive log monitoring and trending

System administrators should be proactively monitoring their logs to detect any errors related to smart card logon, path validation problems or areas related to PIV card usage. By understanding the problems,

architecture changes (such as path validation optimization, OS CRL tuning) can be performed to ensure the infrastructure can support PIV cards. A free tool from Microsoft is known as the Log Parser 2.2. This tool provides the logs in a manner that is easy to format and build trending reports.

4 - Involved Improvement

One of the best indicators of PIV performance is the end user. For this reason, their user experience should be leveraged to help continuously improve the PIV infrastructure. This can be done for free using a Microsoft outlook survey. In this, questions related to response time, error types and user feedback can be automatically captured with a simple email where engineers can use the information to optimize their infrastructure.

Conclusion

By helping the end user understand the fundamentals of PIV cards and how to use them, organizations can introduce more sophisticated uses to begin to [maximize the value of PIV](#) for both improved business operations and strengthen their security posture.

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.