

PIV Card Computer Logon Considerations

PAPER HIGHLIGHTS

- Provides the benefits of smart card logon
- Steps to get started
- Critical errors that derail efforts

Goal of this document

The purpose of this document is to provide an understanding of how to use the PIV card for computer logon. It describes how the cryptographic technologies associated with PIV eliminate numerous security threats, provides steps to perform various system configurations and covers common errors typically experienced during the implementation phase.

The value of PIV card computer logon

The most secure authentication mechanism for windows computer logon is through the use of a cryptographic token. The reasons are based in technology and user behavior. In terms of a technology advantage, when configured for PIV card logon the workstation and domain controller must perform a series of cryptographic transactions that are resistant to any known cyber attack vector. From a user behavior perspective the nature of the PIV card requires they must insert it and provide a the PIV Card PIN which eliminates the practice of sharing or writing down passwords.

- ✓ Unbreakable authentication transaction
- ✓ No shared passwords between users
- ✓ Secured domain password database
- ✓ Auto logoff when leaving

Steps to configure PIV card logon

The following steps list the actions necessary to get started with implementing PIV card logon.

1 - Backup and Test

By design, PIV Card logon is a very sensitive feature to the Microsoft infrastructure. When implementing, take the proper precautions to ensure all changes are planned for and that a recovery plan is available to restore the domain in the case of a failure. Also, ensure any applications that use the domain for authentication services are properly tested to ensure the changes do not negatively impact their behavior.

2 - Gather the tools

The two following free tools provide significant assistance in configuring and troubleshooting settings related to PIV card logon:

Tool Name	Description
CERTUTIL	Helps display certificate information and can automate the installation of issuing certificates into active directory. LINK http://technet.microsoft.com/en-us/library/cc732443%28WS.10%29.aspx
OPENSLL	Provides the ability to manually inspect certificates, perform external path validation and convert certificates for troubleshooting purposes. LINK http://www.openssl.org/

3 - Ensure validation path connectivity

The domain and the workstation must be able to reach the network locations in each of the certificates in the chain. To perform the basic connectivity checks, open the certificates in the chain and telnet to port 80 or 389 (depending on the protocol) to the addresses listed within the Authority Information Access and CRL Distribution points in the certificates. If the client or domain cannot reach these addresses, the transaction will fail.

3 - Install the issuing CA certificate [Domain Controller]

Microsoft utilizes the PKINIT protocol to perform the smart card logon process. During this transaction, a mutual authentication between the workstation and domain are performed which entails certificate validation for both parties. For this reason, the issuing CA certificate of the PIV authentication certificate must be installed into the domain controller's NTAAuth store. For step by step directions, go to: <http://support.microsoft.com/kb/281245>

4 - Install software and hardware [Workstation]

To read the PIV card, the next step involves installing the hardware drivers and middleware software. To ensure both components were installed properly, run a quick test to export the public certificates from the card and also view the photo. This should ensure the card can interact with the operating system in a manner to provide the certificates and perform PIN authentication.

5 - Restart, Insert the card and perform logon

The next step involves having the user perform PIV card logon. If all of the steps have been performed properly, the user will be able to insert their card, enter their PIN and be logged into their desktop using their PIV card.

WARNING

Implementing PIV card logon requires appropriate planning, piloting, training and recovery capabilities. Since this change is effectively upgrading the entire domain authentication infrastructure, the changes must be thoroughly tested, carefully implemented and continuously monitored.

A setting that is tempting to make is to enforce smart card logon. However, this setting known as, "Smart card is required for interactive logon" must be adequately planned for and tested. This change transfers ownership of the password from the user to the operating system. Upon which, the operating system will erase the user's password and assign a randomly generated 255 character password. This blocks the user from ever using their password to log on again. If not properly planned for, the user and any applications that use that account will be blocked from authenticating resulting in system and application lockout.

Conclusion

PIV card logon provides unmatched security that can instantaneously fortify an infrastructure. Through proper planning, careful testing and a disciplined implementation methodology, PIV cards can replace one of the most vulnerable links in the security chain...the password.

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.