FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

PIV CARDHOLDER AUTHENTICATION

Changes to PIV Authentication Mechanisms

- Mandatory Asymmetric Card Authentication Key (PKI-CAK)
- Mandatory signature verification for BIO, BIO-A, and CHUID and certificate validation for PKI-AUTH and PKI-CAK authentication mechanisms.

- Optional On-card Biometric Comparison
- Optional PIV Card Activation for privileged operations can be done with On-card Biometric Comparison in addition to required PIN.

Electronic Authentication – Logical Access Control Systems

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
SOME confidence	CHUID, PKI-CAK	PKI-CAK
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, PKI-AUTH	PKI-AUTH

Electronic Authentication – Physical Access Control Systems

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID, PKI-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI-AUTH

Electronic Authentication – Characteristics

Method	**Type**	**Use of PKI**	**Assurance Level**
CHUID	Data Token	Signature Verification	SOME (1 factor authentication)
PKI-CAK	Challenge/ Response	Certificate Validity	SOME (1 factor authentication)
BIO	Fingerprint Biometric	Signature Verification	HIGH (2 factor authentication)
BIO-A (Attended)	Fingerprint Biometric	Signature Verification	VERY HIGH (3 factor authentication)
PKI-AUTH	Challenge/ Response	Certificate Validity	VERY HIGH (2 factor authentication)

Questions (?)

- Should NIST consider other authentication mechanisms outside of PIV?
- What else needs to be Standardized? Should NIST consider standardizing interface between Identity and Access Management Systems and Physical Access Control Systems?