CRYPTOGRAPHIC CAPABILITIES

New Requirement: Digital Signature and Key Management Key

Status Quo (FIPS 201-1):

- The digital signature key and key management key are optionally implemented on-card to support signature and encryption schemes.

New Requirement:

- Digital signature key and key management key are proposed to be mandatory* in support of the FICAM Roadmap.

  * if the cardholder has a government-issued email account at the time of credential issuance

Clarification: PIN caching

Comment: The PIN needs to be provided to the PIV Card before each use of the digital signature private key. What are the rules for caching of the PIN?

NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*, is under development and will address PIN caching.

New Requirement: UUID

Comment: The Universally Unique Identifier (UUID) must be mandatory for interoperability between PIV and PIV–Interoperable (PIV–I) ecosystems.

Revised Draft requires UUID to appear in PIV Authentication and Card Authentication certificates.

Clarification: Algorithm Testing

- Clarifies that scope of cryptographic module validation shall include all cryptographic operations performed by or in support of PIV Card Application.
- Specific cryptographic algorithm testing requirements for operations performed by PIV Card Application will be specified in SP 800-78.

Repository Requirements

Comment: FIPS 201-2 shouldn't require CA certificates and CRLs to be distributed via LDAP.

- Revised draft removed mention of LDAP.
- [PROF] can be updated to remove LDAP when it is deemed safe to remove requirement.

Revocation: How Quickly to Revoke

Comment: Multiple comments were submitted with varying opinions on CRL issuance frequency requirement

Revised draft defers to [COMMON] for CRL issuance frequency requirements.

- [COMMON] still requires CRLs to be issued every 18 hours

PIV Content Signer Certificate

Comment: Require use of an OID that is specific to content signer certificate, and require use of FIPS 140 level 2 validated hardware.

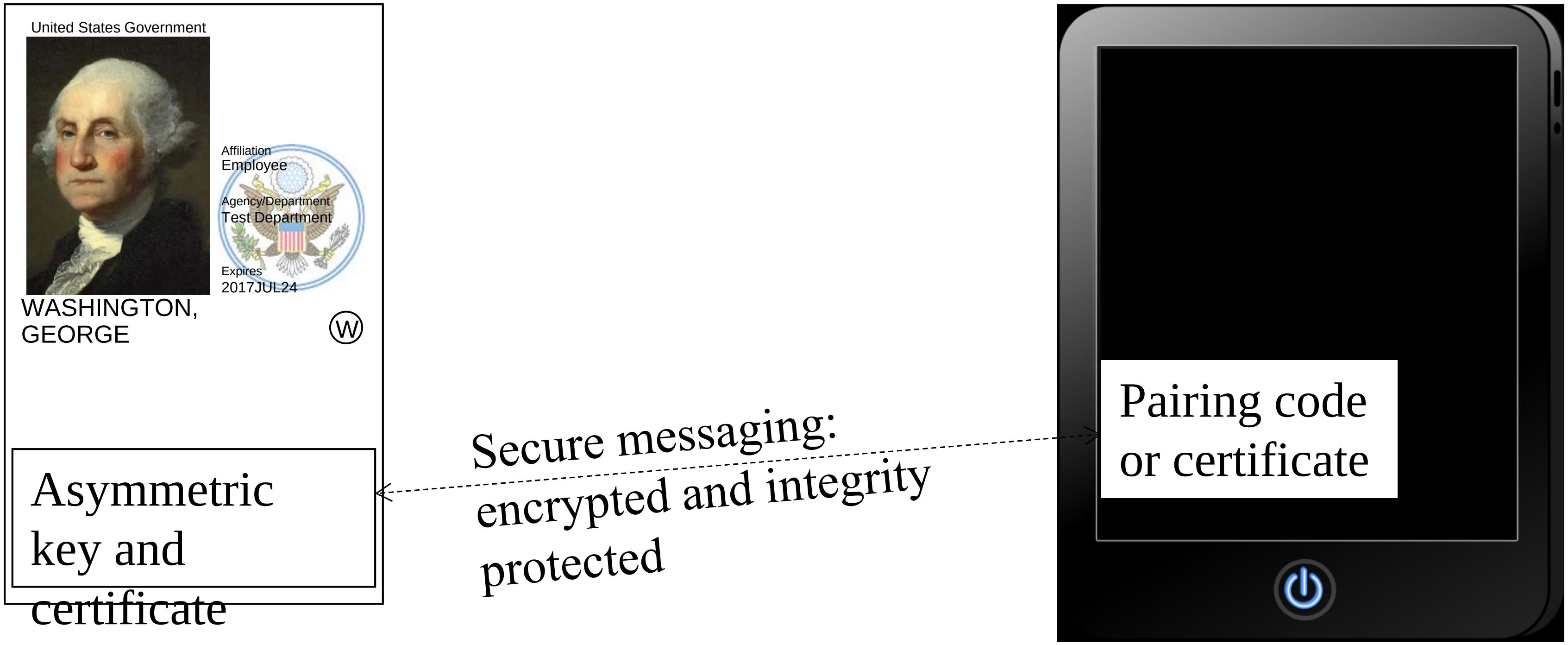
- FIPS 201-1 (Appendix B.4) already requires use of FIPS 140 level 2 cryptographic module.
- Revised draft requires use of id-fpki-common-devicesHardware.

New Option: Secure Messaging

Comments: Secure messaging capability should allow all functionality of the PIV Card to be accessible over the contactless interface of the card.

Revised Draft FIPS 201-2 introduced “virtual contact interface” over which all functionality of the PIV Card is accessible.

Virtual Contact Interface

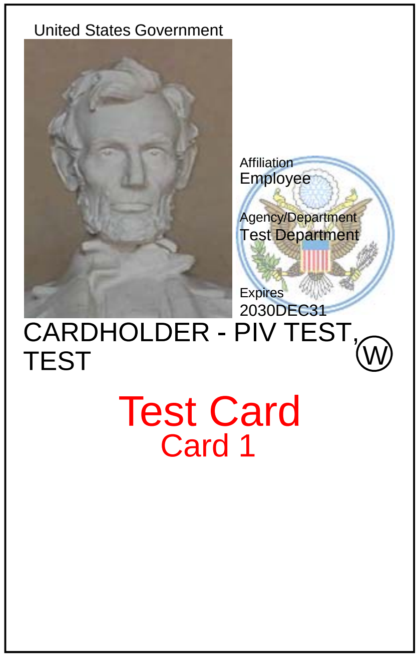


Asymmetric key and certificate

Secure messaging: encrypted and integrity protected

Pairing code or certificate

NIST Special Database 33: NIST Test PIV Cards



United States Government

Affiliation
Employee

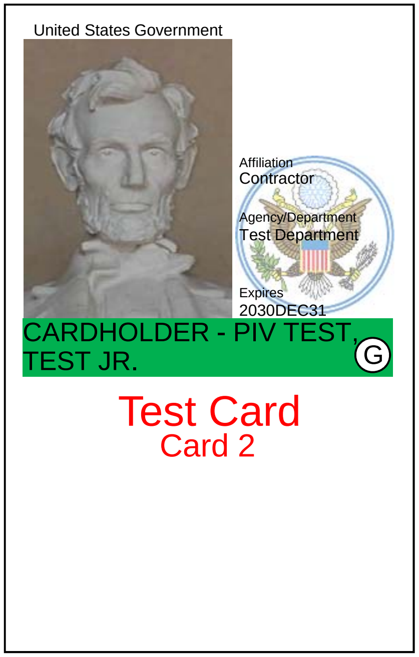
Agency/Department
Test Department

Expires
2030DEC31

CARDHOLDER - PIV TEST,
TEST

Ⓦ

Test Card
Card 1



United States Government

Affiliation
Contractor

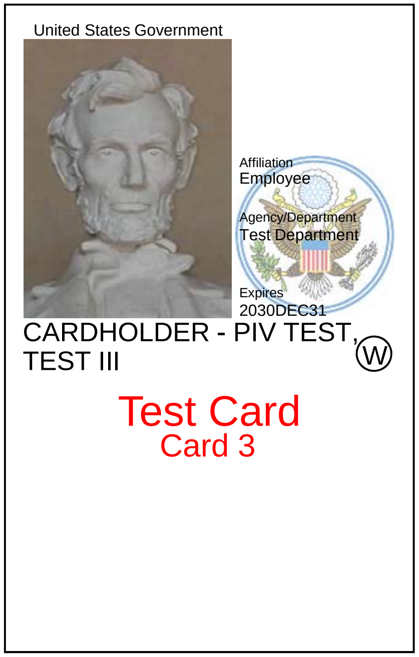
Agency/Department
Test Department

Expires
2030DEC31

CARDHOLDER - PIV TEST,
TEST JR.

Ⓖ

Test Card
Card 2



United States Government

Affiliation
Employee

Agency/Department
Test Department

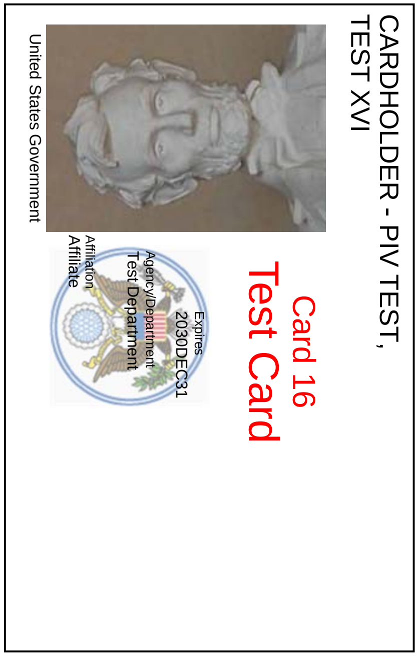
Expires
2030DEC31

CARDHOLDER - PIV TEST,
TEST III

Ⓦ

Test Card
Card 3

…



CARDHOLDER - PIV TEST,
TEST XVI

United States Government

Affiliation
Affiliate

Agency/Department
Test Department

Expires
2030DEC31

Test Card
Card 16

http://www.nist.gov/srd/nistsd33.cfm

Questions (?)