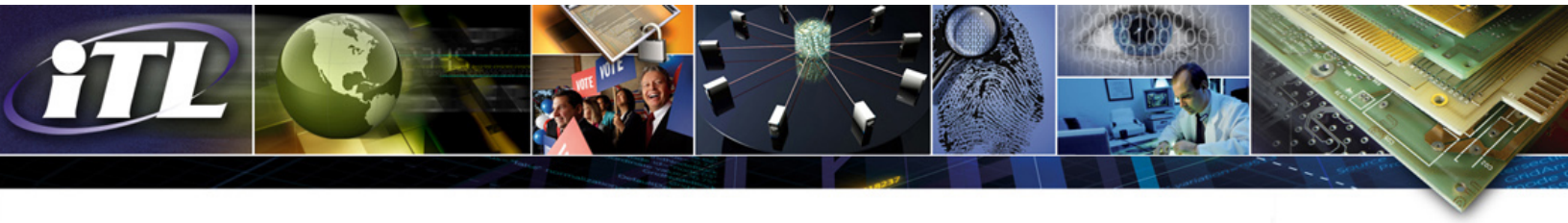


ITL BULLETIN FOR JULY 2015

IMPROVED SECURITY AND MOBILITY THROUGH UPDATED INTERFACES FOR PIV CARDS

Hildegard Ferraiolo, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

NIST has released Special Publication (SP) 800-73-4, *Interfaces for Personal Identity Verification*. This document has been updated to align with Federal Information Processing Standard 201-2 (FIPS 201-2). The new specifications add enhanced identity security features and encryption capabilities, including support for mobile devices such as smart phones.

Federal employees and contractors use Personal Identity Verification (PIV) Cards for secure access to government facilities and IT systems. The PIV Card features a microchip to store the digital representation of a cardholder's information, such as the employee's image, personal identification number (PIN), and fingerprint information, as well as digital certificates and keys. These multifactor credentials are used to authenticate the cardholder to access government facilities and IT systems.

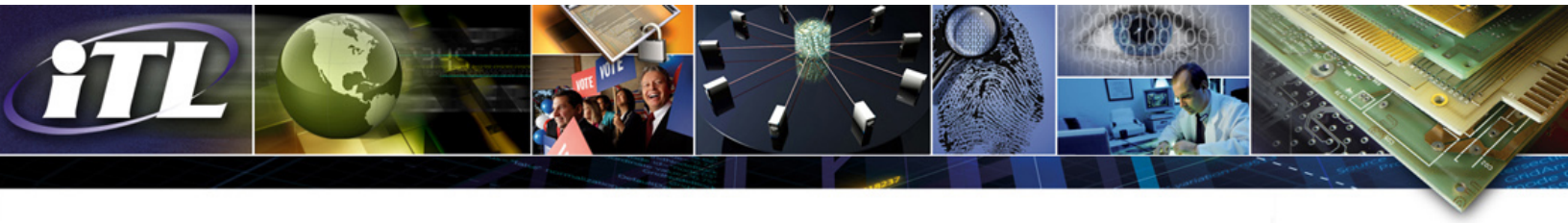
NIST has also released SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, which has been updated to support the PIV Card features in SP 800-73-4. More specifically, it contains the technical details of the mandatory and optional cryptographic keys and the supporting infrastructure specified in FIPS 201-2 and the SP 800-76-2, *Biometric Specifications for Personal Identity Verification*, that rely on cryptographic functions.

Introduction

SP 800-73-4 contains the technical specifications to interface with the smart card to retrieve and use the multifactor identity credentials for authentication. The specifications reflect the design goal of interagency interoperability of the PIV Card. The goal is addressed by specifying a PIV data model, card edge interface, and application programming interface (API). The document enumerates requirements where the international integrated circuit card (ICC) standards (ISO 7816) for smart cards include options and branches. The document also constrains implementers' interpretations of the normative ICC standards. These restrictions are designed to ease implementation, facilitate interagency interoperability, and ensure performance, in a manner tailored for PIV applications.

SP 800-73-4 is organized into the following three parts:

- Part 1 – *PIV Card Application Namespace, Data Model and Representation*, specifies the PIV Card Application Namespace, the PIV Data Model, and its logical representation on the PIV Card.



- Part 2 – *PIV Card Application Card Command Interface,* contains the technical specifications of the PIV Card interface. The specification defines the set of commands surfaced by the PIV Card Application at the card edge of the ICC.
- Part 3 – *PIV Client Application Programming Interface*, contains technical specifications of the PIV client API to the PIV Card.

PIV Credentials

SP 800-73-4 Part 1 describes seven mandatory, two conditionally mandatory, and twenty-eight optional interoperable data objects that are stored on the PIV Card. Some of these objects provide cardholder characteristics in digital form including facial information, iris images, and fingerprints. These are used for biometric authentication of the cardholder. Other objects refer to digital components such as certificates and keys that support logical authentication and digital signatures or encryption capabilities. The combination of these objects enables PIV card services for authentication, encryption, and signing.

PIV Card Application Card Command Interface

Part 2 of SP 800-73-4 specifies a set of card commands that may be used to interact with the PIV card and its services. These commands enable the user to perform services such as authentication, signing/encryption, and credential initialization/administration functions. Part 2 details the specific commands, interface, and conditions by which a system may communicate with the PIV card.

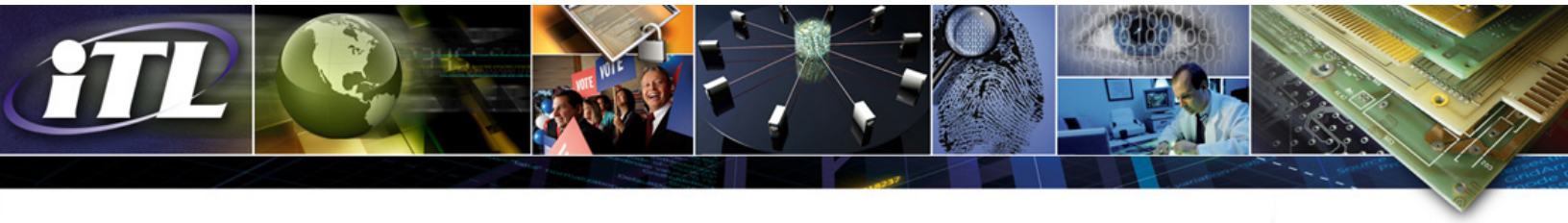
PIV Authentication Mechanisms and Secure Messaging

The authentication services are defined by protocols and enable cardholder authentication, regardless of which agency issued the card. These services are represented in authentication mechanism diagrams. SP 800-73-4 also added a requirement for signature verification and certification path validation in the Card Holder Unique Identifier (CHUID), Biometrics (BIO), and Biometrics Attended (BIO-A) authentication mechanisms.

One new authentication service, On-Card Biometric Comparison (OCC-AUTH), compares the biometric fingerprint details stored on the PIV card with those presented by the cardholder. Performing this comparison on the card, rather than exchanging the information with the application, improves cardholder privacy.

According to SP 800-73-4, a PIV Card may now also support secure messaging. When secure messaging is established, the PIV Card is authenticated to the relying system and a set of symmetric session keys are established. These secure messaging keys are used to provide confidentiality and integrity protection for the card commands that are sent to the card and the card's responses.

The publication also introduces specifications for an optional virtual contact interface (VCI). All non-card management operations that are allowed over a contact interface may be carried out over the contactless interface if the VCI security condition is satisfied.



Cryptographic Algorithms and Key Sizes for Personal Identity Verification

SP 800-78-4 describes recommended procedures for key size and algorithm discovery to facilitate cryptographic authentication. This, in turn, enables appropriate decisions for granting access to logical and physical systems. The discovery procedure is defined in terms of asymmetric and symmetric cryptographic authentication.

The document also defines the security requirements for the PIV Card, the infrastructure that supports issuance and management of the PIV Card, and applications that rely on the PIV Card credentials. It identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, key establishment schemes, and message digest algorithms. These algorithms have been selected for consistency with applicable federal standards and to ensure adequate cryptographic strength for PIV applications. All cryptographic algorithms employed in the specification provide at least 112 bits of security strength.

Conclusion

NIST SP 800-73-4 and NIST SP 800-78-4 provide a richer set of credentials for personal identification and authentication. In addition to stronger cryptographic algorithms, the specifications enable more flexibility, including the ability to use a PIV card with mobile devices. Security is strengthened by implementing the cryptographically strong credentials, rather than the deprecated, less secure one (CHUID). These publications provide specifications that are designed to help agencies to ease implementation, facilitate interoperability, and ensure performance for PIV applications.

Additional Resources

NIST SP 800-73-4, *Interfaces for Personal Identity Verification* - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf
NIST SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf
Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
ISO 7816 (various parts), Identification cards -- Integrated circuit cards - http://www.iso.org/iso/home/store/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=240&ICS3=15&

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov