NIST Special Publication 800-96

PIV Card to Reader Interoperability Guidelines

James F. Dray
April Giles
Michael Kelley
Ramaswamy Chandramouli

I N F O R M A T I O N S E C U R I T Y

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8930

September 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-96, 10 pages

(September 2006)

Acknowledgements

The authors, Jim Dray and Ramaswamy Chandramouli of the National Institute of Standards and Technology (NIST), April Giles of General Services Administration (GSA), and Michael Kelley of Bearing Point wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors gratefully acknowledge and appreciate GSA's leadership in developing significant portions of this document.

Table of Contents

1. Introduction

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This recommendation has been prepared for use by Federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to present recommendations for Personal Identity Verification (PIV) card readers in the area of performance and communications characteristics to foster interoperability. This document is not intended to re-state or contradict requirements specifically identified in Federal Information Processing Standard 201 (FIPS 201) or its associated documents. It is intended to augment existing standards to enable agencies to achieve the interoperability goal of Homeland Security Presidential Directive 12 (HSPD-12).

The document provides requirements that facilitate interoperability between any card and any reader. Specifically, the recommendations are for end-point cards and readers designed to read end-point cards.

2. PIV Card Reader Requirements

2.1 PIV Contact Card Reader (Logical Access)

2.1.1 Application Programming Interface (API)

The reader shall be Personal Computer Smart Card (PC/SC) conformant when used with corresponding drivers for the host Operating System Platform.

The reader, in conjunction with its corresponding driver, should handle the Application Protocol Data Unit (APDU) exchange with T=0 for case 4 commands (e.g., GET DATA, GENERATE ASYMMETRIC KEY PAIR) by reading all data from the card. In other words, the reader in conjunction with its corresponding driver should process all APDUs from the card consisting of SW1 = '61' and SW2 = Number of bytes in the buffer, and should not transmit these APDUs through the PC/SC API to the software implementing the client-application programming interface (middleware).

2.1.2 Application Protocol Data Unit (APDU) Support

At a minimum, the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

2.1.3 Buffer Size

The reader must contain a buffer large enough to receive the maximum size frame permitted by International Organization for Standardization International Electrotechnical Commission (ISO/IEC) 7816-3:1997, Section 9.4.

2.1.4 Programming Voltage

PIV Readers shall not generate a Programming Voltage.

2.1.5 Support for Operating Class

PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

2.1.6 Retrieval Time

Retrieval time[1] for 12.5 kilobytes (KB) of data through the contact interface of the reader shall not exceed 2.0 seconds.

2.1.7 Transmission Protocol

The PIV Reader shall support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.

[1] The time to retrieve a specified amount of data does not include activation/deactivation time.

2.1.8 Support for PPS Procedure

The reader shall support Protocol and Parameters Selection (PPS) procedure by having the ability to read character TA1 of the Answer to Reset (ATR) sent by the card as defined in ISO/IEC 7816-3:1997.

2.2 PIV Contact Card Reader (Physical Access)

2.2.1 Common Requirements

The contact interface of the reader shall support all requirements in sections 2.1.2 to 2.1.8.

2.3 PIV Contactless Card Reader (Logical Access)

2.3.1 API

The reader shall be Personal Computer Smart Card (PC/SC) conformant when used with corresponding drivers for the host Operating System Platform.

The reader, in conjunction with its corresponding driver, should handle the APDU exchange with T=0 for case 4 commands (e.g., GET DATA, GENERATE ASYMMETRIC KEY PAIR) by reading all data from the card. In other words, the reader in conjunction with its corresponding driver should process all APDUs from the card consisting of SW1 = '61' and SW2 = Number of bytes in the buffer, and should not transmit these APDUs through the PC/SC API to the software implementing the client-application programming interface (middleware).

2.3.2 APDU Support

At a minimum, the contactless interface shall support all card commands for contactless based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1, Interfaces for Personal Identity Verification.

2.3.3 Buffer Size

The reader shall contain a buffer large enough to receive the maximum size frame permitted by ISO/IEC 7816-3, Section 9.4.

2.3.4 ISO 14443 Support

The PIV Reader shall support parts (1 through 4) of ISO/IEC 14443 as amended in the References of this publication.

2.3.5 Type A and B Communication Signal Interfaces

The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.

2.3.6 Type A and B Initialization and Anti-Collision

The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.

2.3.7 Type A and B Transmission Protocols

The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.

2.3.8 Retrieval Time

Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 2.0 seconds.

2.3.9 Transmission Speeds

The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s), and fc/32 (~424 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005. Bit rates fc/64 and fc/32 may be configurable to allow activation / deactivation.

2.3.10 Readability Range

The reader shall not be able to read a PIV card more than 10cm from the reader.

2.4 PIV Contactless Card Reader (Physical Access)

2.4.1 Common Requirements

The contactless interface of the reader shall support all requirements in sections 2.3.2 through 2.3.10.

3. References

ISO/IEC 7816-3:1997 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-3:1997/Amd. 1:2002 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1.8 V

ISO/IEC 14443-1:2000 Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 1: Physical Characteristics

ISO/IEC 14443-2:2001/Amd. 1:2005 Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface AMENDMENT 1:Bit rates of fc/64, fc/32 and fc/16.

ISO/IEC 14443-3:2001/Amd.1:2005/Amd.3:2006 Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 3: Initialization and anticollision. AMENDMENT 1: Bit rates of *fc* /64, *fc* /32 and *fc* /16, AMENDMENT 3: Handling of reserved field and values.

ISO/IEC 14443-4:2001/Amd.1:2006 Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 4: Transmission Protocol AMENDMENT 1: Handling of reserved fields and values

PC/SC - Interoperability Specification for ICCs and Personal Computer Systems Part 2. Interface Requirements for Compatible IC Cards and Readers, Revision 2.01.02, September 2005

SP 800-73-1 - NIST Special Publication 800-73 Revision 1, Interfaces for Personal Identity Verification. March 2006.

4. Abbreviations and Acronyms

APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer to Reset
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KB	Kilobyte
kbit/s	Kilobits / second
NIST	National Institute of Standards and Technology
PC/SC	Personal Computer / Smart Card
PIV	Personal Identification Verification
PPS	Protocol and Parameters Selection
TPDU	Transport Protocol Data Unit
Vcc	Voltage at the Common Collector