



ARMY CAC/PKI PROGRAM CARD READER SPECIFICATIONS

by
Cynetheia Brown

Information Assurance & Compliance
Research, Development, Test and Evaluation Cell

October 17, 2005
Rev. March 7, 2007

Table of Contents

EXECUTIVE SUMMARY 1

SCOPE 2

GUIDELINES 2

SPECIFICATIONS 3

– STANDARDS 3

 PC/SC 3

 ISO 8=7816 3

 WHQL 4

 M.U.S.C.L.E. 4

 OCF 4

– OPERATION SYSTEM SUPPORT 4

– LED 4

– TRANSMISSION PROTOCOL 4

– CLK FREQUENCY 5

– FLASH UPGRADEABLE 5

– CABLE or PCMCIA 5

– PROTOCOL MANAGEMENT COMMUNICATIONS 5

 DATA EXCHANGE RATE 5

– POWER 5

 SOURCE, VOLTAGE, and SPECIFICATION 5

– PHYSICAL 6

 INSERTION CYCLES, CHIP LOCATION, TYPE OF CARD CONTACT, OPERATING TEMPERATURE 6

 CASING AND SHORT CIRCUIT DETECTION 6

APPENDIX A: ARMY COMMON ACCESS CARD READER SPECIFICATIONS 7

Contact Readers

EXECUTIVE SUMMARY

The purpose of this document is to identify and specify the requirements for card readers for the Department of the Army’s (DA) Common Access Card (CAC) deployment as supported by Army’s Information Assurance CAC/PKI program office. The leveraging of industry standards and specifications for Commercial Off The Shelf (COTS) products is the foundation of the smart card technical specifications. This document outlines the core engineering standards used to define acceptable card readers for DA deployment and CAC/PKI use. Vendor independent Smart Card/Common Access Card Readers must comply with the following engineering specifications (see **Table 1** “Summary Army Common Access Card Reader Specifications”).

Table 1. Summary Army Common Access Card Reader Specifications

Summary Specifications	Army Common Access Card Reader Specifications			
	Workstation / Key-Board Embedded	9 pin RS-232 Serial Interface	USB 1.0/2.0 Port Interface	PCMCIA Interface
General Specifications				
Standards	ISO 7816, PC/SC, WHQL, M.U.S.C.L.E., OCF			
Reader Driver Operating System (OS) Support	W2K, WXP, W2K3 Svr, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	W2K, WXP, W2K3 Svr, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	W2K, WXP, W2K3 Svr, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	W2K, WXP, W2K3 Svr, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)
LED	Dual display “Power-On” and “Read/Write” LED Indicator(s).			
Transmission Protocol	T=1 and T=0	T=1 and T=0	T=1 and T=0	T=1 and T=0
CLK Frequency	1-5 MHz or greater			
Flash Upgradeable	YES	YES	YES	YES
Cable	N/A	Min. 1-3 meter	Min. 1-3 meter	N/A
PCMCIA	N/A	N/A	N/A	Type II Interface
Protocol Management/Communication				
Data Exchange Rate	9600 bps to 115,200 bps or greater			
Power				
Source	N/A	Via PS/2 or DIN5 Port	USB Port	PCMCIA Interface
Voltage	3V and 5V	3V and 5V	3V and 5V	3V and 5V
Specifications	ISO 7816 EMV (5V, 60mA)			
Physical				
Insertion Cycles	Up to 100,000	Min. 100,000	Min. 100,000	Up to 100,000
Chip Location	ISO 7816	ISO 7816	ISO 7816	ISO 7816
Type of Card Contact	Friction Contact (Landing Contact preferred where available)	Landing Contact	Landing Contact	Friction Contact (Landing Contact preferred where available)
Operating Temperature	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity
Additional Desirable but not Required Features				
Casing	N/A	Supports Vertical	Supports Vertical	N/A
Short Circuit Detection	YES	YES	YES	YES

See **Appendix A “Army Common Access Card Reader Specifications”** for detailed engineering standards for peripheral-type readers, readers embedded in workstations or keyboards, and PCMCIA-type readers.

SCOPE

Although some card readers can read both contact and contactless smart cards, this document focuses on contact card readers and does not specifically address contactless card reader specifications. Such specifications will be defined as guidelines for the Army's deployment of contactless smart cards mature. This document does not address card readers for Personal Digital Assistants, Cell Phones, or other portable wireless devices. Card readers read data from and write data to the smart card. Card readers acceptable for DA use must comply with several governmental and departmental guidelines, and industry standards.

See **Appendix A "Army Common Access Card Reader Specifications"** for detailed engineering standards for peripheral-type readers, readers embedded in workstations or keyboards, and PCMCIA-type readers.

GUIDELINES

- Homeland Security Presidential Directive 12 (HSPD-12) requires all federal agencies to issue Identification cards that are interoperable across agencies and will also impact card reader requirements for DA.
- Federal Information Processing Standards Publication (FIPS) 201; Personal Identity Verification (PIV) of Federal Employees and Contractors, (February 25, 2005)

Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader to-host system interface in the general desktop and laptop computing environment.

- NIST Interagency Report 6887 – 2003 Edition; *Government Smart Card Interoperability Specification v 2.1(GSC-IS 2.1)* (July 16, 2003)

*The GSC-IS does not address interoperability between smart card readers and host computer system. Several specifications already exist in this area, e.g.,
PC/SC*

- Government Smart Card Handbook; U.S. Government Services Administration (GSA) (February 2004)

Refers to the GSC-IS 2.1

- Access Card Office (ACO); Common Access Card (CAC) Release 1.0 Reader Specifications, Version 1.0 (September 25, 2000)

Smart card readers will be needed to interact with the smart card in a Microsoft Windows 95, 98, NT 4.0 or higher; UNIX; LINUX; Macintosh, and JavaOS environments. All smart card readers shall minimally be PC/SC certified, and certified for the Microsoft Logo Program by the Windows Hardware Quality Labs (WHQL). Additionally, all smart card readers destined for UNIX, LINUX, Macintosh, and JavaOS environments shall be PC/SC certified, and be certified for Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.) and OpenCard Framework (OCF) complaint reader drivers and/or components.

There are several technologies combined into a smartcard such as magnetic stripe, bar codes, as well as an integrated circuit chip (ICC) or mini-processor. However, it is the ICC that defines the card as a smart card. There are contactless smart cards that require the smart card to be within a specified proximity of the card reader in order to read/write to the card and contact smart cards that require the smart card to be inserted into the card reader devices.

Smart Card Readers are also known as Smart Card Programmers, Smart Card Terminals, Smart Card Acceptance Device (CAD) and Interface Device (IFD). The smart card reader is an important component in building a secure network infrastructure. The smart card reader will soon be a typical and necessary component in a PC; much like the floppy drive, CD ROM drives, etc. External card readers are employed as peripheral devices, connected to the PC via USB port, serial port, or the PCMCIA.

SPECIFICATIONS

– STANDARDS

PC/SC

Personal Computer Smart Cards (PC/SC). The PC/SC Workgroup was formed to address limitations in existing standards, from a personal computer/smart card application perspective.

The PC/SC standard for the reader-to-host system interface builds upon existing industry smart card standards - ISO 7816 and Europay MasterCard and Visa (EMV) - and compliments them by defining low-level device interfaces and device-independent application APIs as well as resource management, to allow multiple applications to share smart card devices attached to a system. As with all previous versions, Specifications 2.01 is completely platform independent, and can be implemented on any operating system. PS/SC identifies card reader requirements based a 10 part requirements document. A card reader is recognized as PC/SC compliant once it has implemented the PC/SC specification steps.

The goals of the PC/SC Working Group are:

To promote a standard specification, to ensure that smart cards, smart card readers, and computers made by different manufacturers will work together; and

To facilitate the development of smart card applications for PC and other computing platforms. www.pcscworkgroup.com.

ISO 7816

The International Standard Organization (ISO) has established standards. ISO 7816 standard for the card-to-reader interface covers "Identification Cards - Integrated Circuit Cards with Contacts including Physical characteristics, Dimensions and location of the contacts, Electronic signals and transmission protocols, and Industry commands for interchange

WHQL

Windows Hardware Quality Labs (WHQL) supports the Microsoft® Windows® Logo Program for hardware with the Hardware Compatibility Test (HCT) kits, test information, and data for hardware testing and driver signing. These requirements are tested in Microsoft® Windows® Hardware Compatibility Tests (HCT) — Microsoft facility that tests and certifies third-party hardware and driver products for compatibility with Windows operating systems. Products that meet the compatibility requirements are then allowed to display Windows logos on product packaging, advertising and collateral and other marketing materials, indicating that the product has met the standards of Microsoft and that the product has been designed to work with the Windows operating systems. Once a product has received the WHQL logo it is listed on the Microsoft Hardware Compatibility List. www.microsoft.com/whdc/whql/device/smartcard.msp

M.U.S.C.L.E.

Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.). Muscle's goal is to provide crossplatform smart card and cryptographic support for Linux users. The purpose is to develop a set of compliant drivers, API's, and a resource manager for various smart cards and readers for the GNU environment. Source code is now distributed by this site that supports the Schlumberger Reflex 60 line of reader and all ISO-7816-4 compliant smart card readers. www.linuxnet.com

OCF

OpenCard Framework is a standard framework announced by an Industry consortium that provides for inter-operable smart cards solutions across many hardware and software platforms. The OpenCard Framework is an open standard providing an architecture and a set of APIs that enable application developers and service providers to build and deploy smart card-aware solutions in any OpenCard-compliant environment.

www.opencard.org/

– OPERATION SYSTEM SUPPORT

Compliant card readers support the following operating systems at minimum: Windows 2000, XP, Server 2003, Linux, Red Hat, Mac OS X.

– LED

Light Emitting Diode. A display technology that uses a semiconductor diode that emits light when charged. Compliant card readers provide LED dual displaying “Power-On” and “Read/Write”.

– TRANSMISSION PROTOCOL

T=1 and T=0. OSI (Open Systems Interconnect) Reference Model communications protocol between a smart card and a smart card reader. T=0 is a byte-oriented protocol. Byte-oriented means that a byte or individual character is the unit of information

transferred across a channel and that error handling is handled one byte at a time. T=1 is a block-oriented protocol. Block-oriented means that a well-defined collection of information or block is moved as a single unit between the reader and the card. T=0 and T=1 establish reliable channels for moving application protocol data units (APDUs) between application software elements on the smart card and on the reader-side of the communication. A card may support either but not both concurrently during a communication cycle.

– **CLK FREQUENCY**

A CLK (Clock) Frequency is clock signal used to coordinate the actions of two or more circuits. The clock frequency of a card reader determines the rate at which the signal travels through ICC Interface Device (IFD) I/O device. The Clock signal can be provided to the smart card's microprocessor chip to control the speed at which it operates and to provide a common framework for data communication between the reader and the smart card.

– **FLASH UPGRADEABLE**

Allows the engineer to keep up to date with the latest software enhancements by means of a downloadable link.

– **CABLE or PCMCIA**

Length of the cable connected to the card reader peripheral device or if the device has a PCMCIA (Personal Computer Memory Card International Association) connection which is a small credit card size device that fits into an expansion slot on a PC.

– **PROTOCOL MANAGEMENT COMMUNICATIONS**

DATA EXCHANGE RATE

A measurement of the number of bits of information that can be sent over a connection or ICC Interface Device I/O channel.

– **POWER**

SOURCE, VOLTAGE, and SPECIFICATION

The source in which the card reader device receives power (voltage and current), the standard voltage of the card reader device, and the specification that provides the implementation details.

– **PHYSICAL**

INSERTION CYCLES, CHIP LOCATION, TYPE OF CARD CONTACT,
OPERATING TEMPERATURE

The Insertion Cycles states expected life cycle of the insertion region of the card reader device. The Chip Location identifies the dimension and location of the ICC contacts according to ISO 7816; the international standard for integrated-circuit cards. The Card Contact specifies the method in which the ICC makes contact with the card reader device. There are two main types of contact s: landing contact and friction contact (also known as sliding or wiping). For card readers of friction contact, the contact part is fixed. The contact wipes on the card surface and the chip when a card is inserted. For card readers of the landing type, the contact part is movable. The contact “lands” on the chip after a card is wholly inserted. In general, card reader of landing type provides better protection to the card than that of the friction type. Landing contact type is desired in view of the protection it can provide to the smart ID card which is expected to last for at least 10 years. The Operating temperature describes the environmental performance in which the card reader will function properly.

CASING AND SHORT CIRCUIT DETECTION

The Casing determines if the card reader device will support vertical mounting for top entry of the smart card into the card reader device. The Short Circuit detection provides a shut off function when a short circuit occurs to protect the smart card and the reader.

APPENDIX A
PAGE 1 OF 2

READER TYPES

The following are the reader specifications for the accepted hardware interfaces (embedded in workstation or keyboard, RS232 interface, USB 1.0/2.0 interface, and PCMCIA interface) to client workstations. CINCs/Services/Agencies may desire additional features or functions, but ALL CAC readers used by Army installations must minimally comply with the below specifications.

Specifications	Army Common Access Card Reader Specifications			
	Workstation / Key-Board Embedded	9 pin RS-232 Serial Interface	USB 1.0/2.0 Port Interface	PCMCIA Interface
General Specifications				
Standards	All shall be ISO 7816, PC/SC, and Windows Hardware Quality Labs (WHQL Logo) certified. Additionally, those readers destined for workstations other than WINTEL shall provide Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.) certified and OpenCard Framework (OCF) compliant reader drivers.	All shall be ISO 7816, PC/SC, and Windows Hardware Quality Labs (WHQL Logo) certified. Additionally, those readers destined for workstations other than WINTEL shall provide Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.) certified and OpenCard Framework (OCF) compliant reader drivers.	All shall be ISO 7816, PC/SC, and Windows Hardware Quality Labs (WHQL Logo) certified. Additionally, those readers destined for workstations other than WINTEL shall provide Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.) certified and OpenCard Framework (OCF) compliant reader drivers.	All shall be ISO 7816, PC/SC, and Windows Hardware Quality Labs (WHQL Logo) certified. Additionally, those readers destined for workstations other than WINTEL shall provide Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E.) certified and OpenCard Framework (OCF) compliant reader drivers.
Reader Driver Operating System (OS) Support	Windows 2000, XP, Server 2003, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	Windows 2000, XP, Server 2003, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	Windows 2000, XP, Server 2003, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)	Windows 2000, XP, Server 2003, Linux, Red Hat, Mac OS X, Windows OS 64-Bit Edition (Optional)
LED	1. Provide dual displaying "Power-On" and "Read/Write".	1. Provide dual displaying "Power-On" and "Read/Write".	1. Provide dual displaying "Power-On" and "Read/Write".	N/A
Transmission Protocol	T=1 and T=0	T=1 and T=0	T=1 and T=0	T=1 and T=0
CLK Frequency	1-5 MHz or greater			
Support Flash Upgradeable Software Updates (Drivers and Protocols)	YES	YES	YES	YES
Cable	N/A	Min. 1-3 meter	Min. 1-3 meter	N/A
PCMCIA	N/A	N/A	N/A	Type II Interface
Protocol Management/Communication				
Data Exchange Rate (smart card to reader)	9600 bps to 115,200 bps or greater			
Power				
Source	N/A	Via PS/2 or DIN5 Port	USB Port	PCMCIA Interface
Voltage	3V and 5V	3V and 5V	3V and 5V	3V and 5V
Specifications	ISO 7816 EMV (5V, 60mA)			
Physical				
Insertion Cycles	Up to 100,000	Min. 100,000	Min. 100,000	Up to 100,000
Chip Location	ISO 7816	ISO 7816	ISO 7816	ISO 7816

APPENDIX A
PAGE 2 OF 2

Type of Card Contact	Friction Contact (Landing Contact preferred where available)	Landing Contact	Landing Contact	Friction Contact (Landing Contact preferred where available)
Operating Temperature	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity	0 to 50 Degrees Celsius / 40-80% Humidity
<i>Additional Desirable but not Required Features</i>				
Casing	N/A	Supports Vertical	Supports Vertical	N/A
Short Circuit Detection	YES	YES	YES	YES