



---

**DoD CAC Middleware Requirements Release 4.0**

---

Version 1.01  
26 November 2012

Prepared by: DoD Identity Protection and Senior Coordinating Group's  
(IPMSCG) Test and Evaluation Work Group (TEWG)

# TABLE OF CONTENTS

1	Introduction.....	6
2	Middleware Background .....	9
3	Middleware Requirements .....	11
4	Core DoD Requirements .....	12
4.1	Support for FIPS 201 and Associated NIST Special Publications.....	12
4.2	Card Interfaces .....	12
4.3	PKI Requirements.....	13
4.4	Common Access Card (CAC) and Alternate Tokens .....	15
4.5	Middleware Operating Environment.....	16
4.6	Card Readers .....	17
4.7	Application Support.....	17
4.8	Graphical User Interface .....	18
4.9	Middleware Resource Parameters.....	19
4.10	Middleware Installation .....	19
4.11	Middleware Configuration.....	19
4.12	PIN Management.....	20
4.13	Documentation .....	21
4.14	Process Descriptions.....	23
5	Optional .....	24
5.1	General.....	24
5.2	Middleware Operating Environment.....	25

5.3	PIN Services .....	25
5.4	Documentation.....	25
5.5	Support .....	26
6	Core DoD Requirements for CAC Microsoft Minidriver Only .....	28
6.1	General.....	28
6.2	Support for FIPS 201 and Associated NIST Special Publications.....	28
6.3	Card Interfaces .....	28
6.4	PKI Requirements.....	29
6.5	Common Access Card (CAC) and Alternate Token.....	30
6.6	Minidriver Operating Environment .....	31
6.7	Card Readers .....	32
6.8	Application Support.....	32
6.9	PIN Management.....	33
7	Core DoD Requirements for CAC PKCS11 Module Only .....	36
7.1	General.....	36
7.2	Support for FIPS 201 and Associated NIST Special Publications.....	36
7.3	Card Interfaces .....	36
7.4	PKI Requirements.....	37
7.5	Common Access Card (CAC) and Alternate Tokens .....	37
7.6	PKCS11 Operating Environment .....	39
7.7	Card Readers .....	39
7.8	Application Support.....	39
7.9	PIN Management.....	40
	Appendix A .....	42
	Appendix C- PKCS 11 Functions.....	48

Appendix D- BSI Functions .....	50
Appendix E- BSI Header Files .....	51
Appendix F- References .....	52
Appendix G- List of CAC Platform Configurations.....	55

## Document Revision History

Date	Version	Comments Provided By	Summary of Changes
16 February 2001	Release 1.0, Version 1.0	Approved by DoD Middleware Work Group	Final version
21 March 2006	Release 3.0, Version 1.0	Approved by DoD IPMSCG Test and Evaluation Work Group (TEWG)	Final version
12 May 2011	Release 4.0, Version 1.0	Approved by DoD IPMSCG Test and Evaluation Work Group (TEWG)	Final version
26 November 2012	Release 4.0, Version 1.01	Editorial changes to reflect migration to DISA Enterprise E-mail and CAC developer support website URL.	Final version

# **1 Introduction**

## **1.1 Background**

In May of 1999, the Deputy Secretary of Defense (DEPSECDEF) issued a policy memorandum mandating the implementation of a single, integrated Public Key Infrastructure (PKI) across the Department of Defense (DoD). This policy mandated that the DoD PKI be used to digitally sign all email, support mutual authentication to private web sites, cryptographically authenticate to computer networks, and be used in DoD applications when appropriate. In November of 1999, a Smart Card policy memo was issued by the DEPSECDEF which required that a Common Access Card (CAC), based on smart card technology, be used as the primary identification card for DoD personnel, support building access, and be the token for PKI credentials. More recently, Homeland Security Presidential Directive-12 [HSPD-12] mandates the implementation of a Federal Information Processing Standard 201 [FIPS 201] Personal Identity Verification (PIV) of Federal Employees and Contractors. The DoD CAC and DoD PKI programs are being aligned to meet this additional set of requirements.

The DoD established a Middleware Sub-Work Group (MSWG) under the Test and Evaluation Work Group (TEWG) of the Identity Protection and Management Senior Coordinating Group (IPMSCG) to consolidate and document the baseline middleware requirements across the DoD. This middleware requirements document represents the consensus of the participating members of the TEWG.

## **1.2 Purpose**

The Middleware Requirements defines the standard set of services, interfaces, and configuration options that must be implemented by all middleware for use on personal computer desktops, servers, laptops, and other fully functional Microsoft environments listed in Appendix A, figures 5 and 6. Additionally, this document identifies recommended and optional capabilities that middleware providers should consider implementing to differentiate their products and provide added value. The core requirements remain applicable in other operating environments, but Combatant Commands, Services and Agencies (CC/S/A) are free to tailor the requirements for these environments.

## **1.3 Audience**

This document is intended for middleware providers, acquirers, testers, and application developers.

## **1.4 Document Scope**

This document applies to middleware that operates on personal computer desktops, servers, laptops and other fully functional computing environments.

## 1.5 Document Objectives

The objective of this document is to provide unambiguous and testable requirements for middleware vendors to support requisite acquisition efforts by DoD organizations.

## 1.6 Assumptions and Constraints

Each CC/S/A in the DoD will execute middleware acquisitions using processes and procedures available to that organization. It is expected that this document will serve as the centerpiece of those acquisitions.

## 1.7 Abbreviations

ATR	Answer to Reset
BSI	Basic Services Interface
CAC	Common Access Card
CAM	Card Authentication Management
CC/S/A	Combatant Command, Service, Agency
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSP	Cryptographic Service Provider
DoD	Department of Defense
EDIPI	Electronic Data Interchange Personal Identifier
FIPS	Federal Information Processing Standard
GSC	Government Smart Card
GSC-IS	Government Smart Card – Interoperability Standard
IPMSCG	Identity Protection and Management Senior Coordinating Group
MS-CAPI	Microsoft Cryptographic API
MSI	Microsoft Windows Installer Package
MSW	Middleware Sub-working Group

PKCS11	Public Key Cryptography Standard #11
PKI	Public Key Infrastructure
PIN	Personal Identification Number
PIV	Personal Identity Verification

## **2 Middleware Background**

### **2.1 Middleware Definitions**

Middleware is defined as the software application that serves as the interface between host applications (such as email, cryptographic network logon, web browsers, and PK-enabled applications) and the CAC. Functionally, middleware provides access to cryptographic services, CAC data, and CAC management features.

### **2.2 Cryptographic Services**

Cryptographic services are the set of functions necessary for cryptographic operations, such as signing and encrypting email. Middleware provides cryptographic services through three standards-based interfaces: MS-CAPI, MS-CAPI Next Generation (CNG), PKCS11, and BSI.

### **2.3 CAC Data**

CAC data is defined as non-cryptographic data stored on the CAC such as name, rank and person identifier.

### **2.4 CAC Management**

CAC management is the set of functions necessary to manage the card and the middleware environment, such as PIN changes and PIN timeout.

### **2.5 New Card Type**

A new card type is a smart card that is functionally equivalent to the CAC that is currently being issued, which has been selected by the DoD to replace the CAC in the future. Functional equivalency means that new features and changes in the middleware are restricted to version updates within a software release and changes required to make the CAC operational.

### **2.6 New Applet**

A new applet is an applet, approved for use on the CAC by DoD, that provides unique functionality not available with current approved DoD applets. A new instantiation of an existing applet, for example a Generic Container Applet, is not a new applet.

### **2.7 Modified Applet**

A modified applet is an applet, previously approved for use on the CAC by DoD, where the functionality, data and/or layout is changed to accommodate new features, requirements, or capabilities. A new instantiation of a modified PKI Container Applet would be an example of a modified applet.

## Section A: Requirements for Bundled CAC Middleware

**This section outlines DoD requirements for bundled middleware products whose package includes Public Key Cryptographic Standard #11 module, Microsoft cryptographic service provider, Microsoft mini-driver, a user console, and application development and management features.**

### **3 Middleware Requirements**

#### **3.1 Requirements Structure**

##### **3.1.1 Core DoD**

Requirements listed in the Core DoD Requirements section of the document are mandatory, and middleware vendors must have 100% compliance in order to be considered for DoD purchase. Core requirements pertain to interoperability, core middleware functionality, and middleware architecture.

Core DoD requirements are listed in section 4.

##### **3.1.2 Optional**

Optional requirements are those which the DoD considers desirable but not mandatory. The majority of these requirements will be based on each individual purchaser's preference and/or unique circumstances. A good example of an optional requirement is support for other non-DoD card types.

Optional requirements are listed in this document because a) they are value added and differentiators among middleware vendors, and b) it is likely that some variation of these requirements will appear in individual CC/S/A acquisition documentation. Similarly, it is possible requirements listed in the "optional" section will appear as "required" in individual CC/S/A acquisitions.

Optional requirements are listed in section 5.

## **4 Core DoD Requirements**

### **4.1 Support for FIPS 201 and Associated NIST Special Publications**

- 4.1.1 Middleware shall conform to NIST Special Publication 800-85-1A.
- 4.1.2 Middleware shall be certified by an approved NIST laboratory to be FIPS 201 compliant.
- 4.1.3 Middleware vendors shall migrate product offerings, as part of routine maintenance, to support any updates or adjustments to FIPS 201 and any applicable NIST Special Publication.

### **4.2 Card Interfaces**

- 4.2.1 Middleware shall support all card-edge command sets for CAC, PIV, and alternate tokens that conform to:
  - 4.2.1.1 National Institute of Standards and Technology's Special Publication 800-73-3, "Interfaces for Personal Identity Verification," February 2010.
  - 4.2.1.2 National Institute of Standards and Technology's Interagency Report 6887 – 2003 Edition, Government Smart Card Interoperability Specification. Version 2.1, July 13, 2003.
  - 4.2.1.3 CAC Developer's Kit version 4.2 (March 2009) or higher located at <http://www.cac.mil/common-access-card/developer-resources/>
  - 4.2.1.4 DoD Implementation Guide for CAC Next Generation NG version 2.6 (November 2006) located at <http://www.cac.mil/common-access-card/developer-resources/>. This outlines DoD's CAC PIV transitional implementation.
  - 4.2.1.5 DoD Implementation Guide for CAC PIV Endpoint version 1.22 (April 2010) located at <http://www.cac.mil/common-access-card/developer-resources/>. This outlines DoD's CAC PIV endpoint implementation.
  - 4.2.1.6 National Institute of Standards and Technology – Technology Administration U.S. Department of Commerce, Government Smart Card Interoperability Specification. Version 2.1, July 12, 2003, <http://smartcard.nist.gov>

4.2.2 Middleware must be configurable to only support NISTR 6887 and NIST SP 800-73-3 or newer card-edges. The middleware should not request or allow entry of PIN (i.e., activation data) for other card-edges. When an unauthorized card-edge is detected, the middleware must respond with an error to the user interface. An example of the error message could be, "This card is not supported within the current configuration of middleware."

#### 4.2.3 BSI Requirements

4.2.3.1 BSI shall be implemented and compliant in accordance with NIST Government Smart Card Interoperability Specification v2.1, 16 July 2003.

4.2.3.2 Middleware shall provide a BSI implementation per specifications and requirements listed in Appendix D.

### 4.3 PKI Requirements

#### 4.3.1 Supported Cryptography

4.3.1.1 Middleware shall support the exchange of information between the card and workstation when those transactions use the following cryptographic algorithms.

4.3.1.1.1 RSA 2048 and higher

4.3.1.1.2 ECC<sup>1</sup>

4.3.1.1.3 TDES

4.3.1.1.4 SHA 1

4.3.1.1.5 SHA 256 or higher<sup>1</sup>

4.3.1.1.6 AES<sup>1</sup>

#### 4.3.2 Cryptographic Service Provider (CSP)

4.3.2.1 Middleware shall provide a compliant CSP interface as specified in the Microsoft Cryptography API Service Provider documentation.

4.3.2.2 Middleware shall provide a smart card compliant CSP, as documented in Smart Card CSP Notes, available from the <http://www.microsoft.com/downloads/details.aspx?familyid=0F436C75-2304-42BB-B81A-BA0C2C47BAC2&displaylang=en> Web site.

4.3.2.3 Microsoft shall sign the middleware CSP for Microsoft operating environments.

---

<sup>1</sup> Requirement is only applicable when connected to cryptographic engines that support this algorithm.

4.3.2.4 CSP shall be compliant with the CSP requirements listed in Appendix B, CSP Functions.

#### 4.3.3 PKCS 11

4.3.3.1 Middleware shall support PKCS11 functions listed in Appendix C, PKCS11 Functions.

4.3.3.2 Vendor shall provide a list of all unsupported PKCS11 functions.

#### 4.3.4 Minidrivers

4.3.4.1 Middleware shall provide a compliant minidriver as specified for various Microsoft operating systems based on Windows Smart Card Minidriver Specification Version 5. 6, and 7.06 (July 1, 2009) or higher.

4.3.4.2 Middleware's minidriver implementation shall be certified and logoed as part of Microsoft's Windows Logo Program.

4.3.4.3 Middleware's mini driver implementation shall be in such a way that only middleware vendor provided updates will be loaded from Microsoft's Windows update features. This will ensure other vendor's or card manufacturer's mini driver implementations do not overwrite or load in the place of the middleware vendor's implementation.

4.3.4.4 Vendor shall provide a list of all unsupported minidriver functions.

#### 4.3.5 Minimum Components to be Included in Bundled Package

4.3.5.1 Middleware shall minimally support the following by Microsoft operating systems

	<b>PKCS11</b>	<b>MS CSP</b>	<b>MS Minidriver</b>
Microsoft Windows 2000	X	X	
Windows XP Service Pack SP3	X	X	
Windows Vista SP1	X		X
Windows 7	X		X

## 4.4 Common Access Card (CAC) and Alternate Tokens

### 4.4.1 Minimum Supported CACs<sup>2</sup>:

4.4.1.1 Axalto Cyberflex Access 64k v1 soft mask 4 version 1

4.4.1.2 Gemplus GemXpresso (GXP) PRO 64 K

4.4.1.3 Axalto Cyberflex Access 64k v1 soft mask 4 version 2

4.4.1.4 Oberthur ID-One Cosmo v5.2D 64K

4.4.1.5 Oberthur ID-One Cosmo v5.2 72K

4.4.1.6 Schlumberber Cyberflex Access v2c 64K

4.4.1.7 Oberthur ID-One Cosmo v5.2D 72K

4.4.1.8 Gemalto GemCombiXpresso R4 dual interface

4.4.1.9 Gemalto TOP DL GX4 144K

4.4.1.10 Oberthur ID-One Cosmo 128 v5.5 for DoD CAC

### 4.4.2 Alternate Tokens

4.4.2.1 Gemalto Cyberflex Access 64k V2c

4.4.2.2 Oberthur ID-One Cosmo v5.2 64K

4.4.2.3 Specific Information on DoD alternate tokens to be included at a later date.

### 4.4.3 New Card Types

4.4.3.1 Middleware vendor shall provide support for the ability to utilize future card types (e.g. recognition of new Answer to Reset (ATR) codes) as issued by the CAC Program or other Federal PIV programs.

4.4.3.2 Middleware vendor shall provide documentation describing the middleware's software architecture for supporting new card types. Areas of interest to the DoD are modularity and methodology.

4.4.3.3 Middleware vendor shall provide documentation describing the process by which new card types shall be added to the middleware desktop configuration.

---

<sup>2</sup> Specific details on these CAC platforms are outlined in Appendix F. The most current listing of CAC platforms can be found at <http://www.cac.mil/common-access-card/developer-resources/>.

4.4.3.4 Middleware shall be able to utilize “new card types” without the need to restart the middleware services running on the computer or downloading of software patches, fixes, or updates.

#### 4.4.4 Card Applets

4.4.4.1 Middleware shall support all current and modified DoD CAC applets. (e.g., ID applet, Generic container applets, PKI applet, PIN management applet, Access Control Applet).

4.4.4.2 Support for new CAC applets shall be considered routine maintenance.

4.4.4.3 Support for applet changes shall be provided no later than 30 days after the vendor receives a request from the DoD.

#### 4.4.5 Certificates

4.4.5.1 Middleware shall support all DoD CACs and federally issued PIV cards using X.509 formatted PKI digital certificates.

4.4.5.2 Middleware shall support all certificate types issued under the DoD and Federal PKI certificate policies.

4.4.5.3 Middleware shall present certificates for PK services in accordance with key usage and extension key usage policies.

4.4.5.4 Certificates shall be displayed and described in human readable form.

4.4.5.4.1 Middleware shall display for user selection all applicable smart card-based certificates capable of performing/completing a particular transaction based on 4.4.5.3.

4.4.5.5 Middleware shall not depend on the presence of a specific certificate to support cryptographic functions of another certificate. For example, the identity certificate need not be present in order to use the email signing and encryption certificates.

### 4.5 Middleware Operating Environment

#### *Operating System Requirements*

Middleware shall operate with the following operating systems:

Operating Systems Supported by Middleware		
Windows Server 2003	Windows 2000 Service Pack 4	Windows XP SP3
Windows Server 2008		Windows VISTA SP1
		Windows 7

## 4.6 Card Readers

Middleware shall operate and comply with any reader that is ISO 7816 compatible, Personal Computer/Smart Card (PC/SC) Windows Hardware Quality Labs (WHQL/HCL) Logo certified. Middleware shall operate with reader drivers that are compatible with Windows 2000, Windows XP, Windows VISTA, and Windows 7 client as well as Windows Server 2003 and Windows Server 2008 operating systems.

## 4.7 Application Support

### 4.7.1 E-mail

The middleware shall provide cryptographic services to the email application and operating system combinations as listed in Appendix A, Figure 6, Primary Email and OS Combinations to: Sign, decrypt, and encrypt email messages with or without attachments. The middleware MUST NOT be dependent on the email address within any x.509 certificate in order to configure or utilize a certificate as part of a middleware feature/function.

### 4.7.2 Cryptographic Logon

4.7.2.1 The middleware shall provide the means to conduct cryptographic authentication to DoD applications and operating systems.

4.7.2.1.1 The middleware shall support Microsoft Smart Card Logon functionality inherent to the Microsoft Windows 2000, XP, VISTA, and 7 Client operating systems. The middleware shall have the ability to use any appropriate DoD certificate as indicated by the User Principal Name in the certificate's Subject Alternative name field and the following "Enhanced Key Usage" extensions:

- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Secure Email(1.3.6.1.5.5.7.3.4)
- Client Authentication(1.3.6.1.5.5.7.3.2)

4.7.2.1.2 The middleware shall have the capability to display all appropriate certificates on the CAC to allow the user to select the correct certificate

and key pair provided that Microsoft Smart Card Logon functionality permits this capability.

4.7.2.1.3 The middleware shall support Microsoft Smart Card Logon functionality inherent to the Microsoft Windows 2000, XP, VISTA, and 7 Client operating systems. The middleware shall have the ability to use any appropriate Federal PIV or Federal bridge interoperable certificate on a smart card as indicated by the User Principal Name in the certificate's Subject Alternative name field and the following "Enhanced Key Usage" extensions:

- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Client Authentication(1.3.6.1.5.5.7.3.2)

4.7.2.1.4 If a single certificate on the CAC is configured for Microsoft Smart Card Log-on, the middleware shall be capable of making use of it without prior user or system action.

#### 4.7.3 Client Authentication

4.7.3.1 The middleware shall support authentication, digital signature, and encryption functions, to include SSL V3 and TLS 1.0, with browsers, operating systems and applications as specified in Appendix A, Figure 5, Web Servers.

4.7.3.2 The middleware shall support client authentication, which requires a 'PIN Always' access control rule. Middleware must be configurable at an application and/or capability level.

4.7.3.2.1 The middleware shall have the capability to display all appropriate certificates on the CAC or Federal PIV based on key usage to allow the user to select the correct certificate and key pair for a particular transaction.

#### 4.7.4 Additional Applications

4.7.4.1 See Appendix A, figure 5

### **4.8 Graphical User Interface**

#### 4.8.1 Requirements for a Graphical User Interface (GUI)

4.8.1.1 There shall be a single middleware graphical interface or utility to manipulate the middleware's features and configuration.

4.8.1.2 Middleware shall, by default, place an icon in the system tray for indicating middleware activity (e.g. card access indicator) and launching the middleware graphical interface.

4.8.1.3 Only items relative to the context of the user or administrator who is logged in should be displayed (e.g. administrative features that would otherwise not be configurable by the individual logged in should not be displayed to the user, etc.).

4.8.1.4 Middleware shall have the ability to display all fields from the x.509 certificate for each certificate type stored on CAC.

## **4.9 Middleware Resource Parameters**

### **4.9.1 Disk Space and Workstation Requirements**

4.9.1.1 The maximum disk space required for CAC middleware installation on a client workstation shall not exceed 30 Mbytes and, for a server, shall not exceed 100 Mbytes.

4.9.1.2 The CAC middleware shall comply with the minimum hardware characteristics of the operating systems in section 4.5. The middleware shall consume no appreciable (i.e. less than 1%) CPU time when in an idle state and shall not exceed 10% (ten percent) of the system's total resources at rest.

## **4.10 Middleware Installation**

### **4.10.1 Middleware Behavior**

4.10.1.1 Middleware shall support software push capability for installation such as Microsoft SMS.

4.10.1.2 Middleware shall not install card reader drivers.

4.10.1.3 Middleware shall alert the user if no card reader is connected to the workstation.

4.10.1.4 Middleware shall have the ability to uninstall completely in each supported operating system. Uninstall should include the removal of any registry entries added during installation as well as changing any registry settings that were modified at the time of install back to those settings prior to installation. This includes, but is not limited to, the required registry entries used for discovery purposes as specified in this document as well as any vendor-specific registry entries that may be added during installation. Vendors are recommended to use standardized installation tools such as Microsoft Installer.

## **4.11 Middleware Configuration**

### **4.11.1 Configurations**

4.11.1.1 Middleware shall support central and remote administration of all configuration settings. For Microsoft OS's, all configuration options must be

stored in the registry and maintainable via group policy for central administration.

- 4.11.1.2 Middleware shall have the ability to enable or disable any and all configurable settings for the end user at time of installation.
- 4.11.1.3 Middleware configuration settings shall be set and configured in accordance with Appendix A, Figures 1, 2, and 3.
- 4.11.1.4 Middleware shall provide an option to automatically register (or make available for use) all user certificates stored on the CAC for MS Internet Explorer based environments.
- 4.11.1.5 Middleware shall provide an option to automatically remove CAC certificates from the workstation on card removal events.

## **4.12 PIN Management**

### **4.12.1 PIN Services**

- 4.12.1.1 Middleware shall provide a single PIN service, which will have the ability to handle PIN management for MS-CAPI, MS-CAPI Next Generation (CNG), and PKCS11 interfaces. For example, if a user enters a PIN for use with MS-CAPI, and then uses the PKCS11 interface within the specified PIN timeout period, the user should not have to re-enter the PIN since the same PIN service would handle the PIN requirements for both PKCS11 and MS-CAPI modules.
- 4.12.1.2 Middleware shall have the ability to set the amount of inactivity time, which should elapse before the card requires a PIN entry. Inactivity time shall be defined as the amount of time elapsed since the last time a PIN-protected area on the CAC was accessed.
- 4.12.1.3 Middleware shall have the ability to disable all PIN timeout/caching features.
- 4.12.1.4 PIN caching must be accomplished using FIPS 140-2 level 1 or above approved cryptographic methods to protect the PIN. An outline of the implementation and the FIPS 140-2 approved methods shall be provided the vendor.
- 4.12.1.5 PIN caching methods must ensure that when PINs are cached, they are visible only to the middleware application, only stored in system memory (e.g. not on the hard disk drive), and all traces completely removed upon timeout or card removal.
- 4.12.1.6 PIN timeout configurations shall be configured and maintained in accordance with Appendix A, Figure 4.

#### 4.12.2 PIN Change

4.12.2.1 Middleware shall provide the ability for the user to change PINs after the end user has entered the correct PIN.

4.12.2.2 The middleware shall enforce PIN validation rules set out in 4.12.3.1.

4.12.2.3 Middleware shall require the end user to verify the new PIN before submitting the PIN change request to the CAC.

#### 4.12.3 PIN Validation

4.12.3.1 Middleware shall require all new PINs to be no less than 6 and no greater than 8 numeric characters in length.

4.12.3.2 As specified in GSC-IS 2.1, for PINs less than 8 characters, middleware shall pad the PIN with 0xFF to the least significant bytes.

4.12.3.3 In the event an invalid PIN is entered, the Middleware shall notify the user of the error.

4.12.3.4 Middleware shall indicate to the user how many remaining PIN attempts before locking.

#### 4.12.4 PIN Unblock

4.12.4.1 PIN unblock function is a privileged activity on the CAC that is only available from specialized DoD software and workstations. This is not a function that is expected to be available from normal CACholder client workstations.

### **4.13 Documentation**

#### 4.13.1 End-User Documentation

4.13.1.1 Online documentation shall be provided to the end user describing the features and functionality of the middleware application.

4.13.1.2 Access to the online help documentation shall be accessible from all error or stop work notifications to the end user.

4.13.1.3 Middleware shall provide context sensitive help for any utilities or configuration applications that are included with the middleware to aid the user in understanding the meaning of the various options or settings.

4.13.1.4 Help documentation shall be searchable.

4.13.1.5 Help documentation shall have a table of contents.

- 4.13.1.6 Help documentation shall be indexed.
- 4.13.1.7 Middleware shall provide a “Read Me” document that describes middleware key features, feature changes, any known bugs, product ID/codes, or compatibility issues.
- 4.13.1.8 Help topics shall not include features or functionality not included in the middleware or features which have not been enabled.

#### 4.13.2 Administrator Documentation

- 4.13.2.1 Vendor shall provide online documentation as to the setup, installation, and configuration of the middleware.
- 4.13.2.2 Middleware vendors shall provide online documentation as to the location, name, and values of all registry keys used in option configuration settings.
- 4.13.2.3 Middleware vendors shall provide a complete and detailed list of all changes, additions, updates, or deletions made to an end user workstation after installation.
- 4.13.2.4 Middleware vendors shall provide a complete list of any artifacts or upgrades left after an uninstall subject to uninstall rules set out in 4.10.1.4.
- 4.13.2.5 Vendor shall provide documentation as to setup, installation, and documentation for any application or utilities included in the middleware.
- 4.13.2.6 For supported third-party installation products, middleware shall provide administrator documentation for using such products.
- 4.13.2.7 Vendor shall provide documentation for any known issues and their associated resolution.

#### 4.13.3 BSI Documentation for Application Developers

- 4.13.3.1 Vendor shall provide documentation that would aid application developers in the use of their BSI library.
- 4.13.3.2 Vendor shall provide a sample application, with source code, which demonstrates the use of their BSI library.
- 4.13.3.3 The sample application shall include the use of at least one function from each of the three sections of the BSI (utility, storage, and cryptographic).
- 4.13.3.4 Java, Visual Basic, and C/C++ language versions of the sample application shall be provided.

## 4.14 Process Descriptions

### 4.14.1 Middleware Functions

- 4.14.1.1 The middleware vendor shall provide, in detail, a flow chart or other descriptive material describing their cryptographic logon implementation. This material shall describe, at a minimum, how the appropriate certificate is identified and used during the cryptographic login process.
- 4.14.1.2 The middleware vendor shall provide, in detail, a flow chart or other descriptive material describing their card authentication (PIN) time-out implementation.
- 4.14.1.3 For any feature or functionality of the middleware not specifically listed by this document as a Core DoD Requirement or an Optional Requirement, the vendor shall provide a detailed list of those features, how they are used, and their benefit or value added to the DoD.

### 4.14.2 Use of Scratch Pad Space

- 4.14.2.1 Middleware shall fulfill all core DoD middleware requirements without using the CAC for middleware-specific data storage.
- 4.14.2.2 Middleware shall not write or modify any middleware-specific data in any GCA container on the CAC to meet core middleware requirements.

### 4.14.3 Support

- 4.14.3.1 Middleware shall readily display workstation and middleware configuration information in a manner readily available to the end user. The information should, at a minimum, include browser version, operating system, patch level, crypto strength, and PKCS11/CSP/Minidriver library versions and .dll name when available.

### 4.14.3.2 Middleware Updates

4.14.3.2.1 Middleware updates shall be provided in either a Microsoft Patch (msp) or Microsoft Installer (msi) format.

4.14.3.2.2 Middleware shall be configurable to support an automated mechanism to update the middleware. The default configuration must be as off.

4.14.3.2.3 Vendor must provide, in detail, the mechanism(s) used to update the middleware for supporting new card types, bug fixes, and service releases. Attention should be paid to DoD cost reduction, technology requirements, ease of use, and security concerns.

#### 4.14.4 Event Logging

- 4.14.4.1 Middleware shall provide event logs for error reporting.
- 4.14.4.2 Middleware shall provide a method for turning on debug or detailed logging to help troubleshoot problems.

## 5 5.0 Optional

### 5.1 General

- 5.1.1 Middleware destined for workstations other than WINTEL should be interoperable with PC/SC Movement for the Use of Smart Cards in a Linux Environment (M.U.S.C.L.E) certified and Open Card Framework (OCF) compliant reader drivers.
- 5.1.2 Middleware vendor may provide a listing of other applications that can utilize the CAC PKI services. Areas of interest to the DoD are, but are not limited to, VPN, PKE (e.g. DTS), Data At Rest (DAR), and thin client environments.
- 5.1.3 Middleware vendor may provide a utility or other method for building custom installation images for the middleware for both initial installation and maintenance.
- 5.1.4 Middleware may provide advanced installation features that support COTS enterprise management products.
- 5.1.5 Middleware may operate with all other smart card types supported and/or manufactured by that vendor. Middleware may optionally support card types from other vendors. Non-CAC card types should be supported for read/write operations.
- 5.1.6 Middleware should have the capability to utilize one or more cards at the same time and any given time, provided readers are connected to the workstation.
- 5.1.7 Middleware should monitor smart card expiration date and warn user within 60 days of expiration.
- 5.1.8 Middleware should monitor PKI certificate expiration dates and warn user within 60 days of expiration.
- 5.1.9 Middleware should provide customizable help information on expiration reminder alerts. For example, information may be provided regarding proper procedures for decryption and retention of encrypted e-mails in the user's mailbox or personal folders.

5.1.10 Middleware should monitor smart card presence in reader and audibly and visibly warn user upon log off or screen lock if smart card is present.

5.1.11 Middleware should allow customization of help files for enterprise specific information.

5.1.12 Middleware may optionally provide a visual indication of CAC activity.

## **5.2 Middleware Operating Environment**

5.2.1 Middleware may optionally provide support for the following operating systems: Linux, Solaris, MAC OS 10.x, and/or Windows XP Professional x64 Edition.

5.2.2 Middleware may optionally provide cryptographic login capability using any DoD/Federal certificate to non-Microsoft Network operating systems.

5.2.3 The middleware may provide cryptographic services to the email application and operating system combinations as listed in Appendix A, Figure 7, Secondary Email and OS Combinations to sign, decrypt, and encrypt email messages and sign, decrypt, and encrypt email messages with attachments.

For the email applications listed in Appendix A, Figure 6, Primary Email and OS Combinations, and Appendix A, Figure 7, Secondary Email and OS Combinations, middleware may optionally configure the email client for use of PKI services.

## **5.3 PIN Services**

5.3.1 The middleware may implement a Card Authentication Management (CAM) which can differentiate PKI (sign and decrypt) from non-PK operations (such as access to a PIN-protected applet). In this example, the middleware may allow CAM to apply for all PIN-protected CAC operations except for those relating to PKI.

5.3.2 Middleware may provide the ability for applications to “opt out” of the CAM mechanism.

## **5.4 Documentation**

5.4.1 Middleware vendor may provide a detailed listing of third party or industry certifications.

5.4.2 Middleware vendor may provide detailed listing of partnerships with other technology companies which would provide a benefit to the DoD.

## **5.5 Support**

### 5.5.1 Technical Support

5.5.1.1 Middleware may optionally display installed card reader and reader driver version number.

5.5.1.2 Middleware vendor may provide a diagnostic utility to facilitate technical support.

5.5.1.3 Middleware may provide a hyperlink to a vendor middleware product support website. If provided, it must also have the option to be disabled.

### 5.5.2 Vendor Support

5.5.2.1 Vendor may optionally provide a shared bug tracking environment with the DoD.

5.5.2.2 Vendor may cooperate with the DoD on the timing and functionality of service releases.

### 5.5.3 Future Enhancements

5.5.3.1 Middleware vendors are encouraged to provide additional enhancements to include support for biometrics.

5.5.3.2 Biometric support should conform with NIST SP 800-76 and any updates to this document to address iris biometrics and fingerprint biometric match-on-card.

5.5.3.3 Middleware vendors are encouraged to provide additional enhancements to include support for certificate validation clients.

## Section B: Requirements for CAC Microsoft Minidriver Only

**This section outlines DoD requirements for a Microsoft mini-driver for the CAC.**

## **6 Core DoD Requirements for CAC Microsoft Minidriver Only**

### **6.1 General**

- 6.1.1 Minidriver implementation shall implement a singular generic minidriver that supports the CAC, PIV, and DoD alternate token interfaces that conform to NISTR 6887 and NIST SP 800-73-3.
- 6.1.2 Minidriver implementation shall provide a compliant minidriver for various Microsoft operating systems based on Windows Smart Card Minidriver Specification Version 5, 6, and 7.06 (July 1, 2009) or higher.
- 6.1.3 Minidriver implementation shall be certified and logoed as part of Microsoft's Windows Logo Program.
- 6.1.4 Middleware's mini driver implementation shall be in such a way that only middleware vendor provided updates will be loaded from Microsoft's Windows update features. This will ensure other vendor's or card manufacturer's mini driver implementations do not overwrite or load in the place of the middleware vendor's implementation.
- 6.1.5 Vendor shall provide a list of all unsupported minidriver functions.

### **6.2 Support for FIPS 201 and Associated NIST Special Publications**

- 6.2.1 Minidriver implementation shall support NIST Special Publication 800-85.
- 6.2.2 Minidriver implementation shall be certified by an approved NIST laboratory to be FIPS 201 compliant.
- 6.2.3 Vendors shall migrate product offerings, as part of routine maintenance, to support any updates or adjustments to FIPS 201 and any applicable NIST Special Publication.

### **6.3 Card Interfaces**

- 6.3.1 Minidriver implementation shall support all card-edge command sets for:
  - 6.3.1.1 National Institute of Standards and Technology's Special Publication 800-73-3, "Interfaces for Personal Identity Verification," February 2010.
  - 6.3.1.2 National Institute of Standards and Technology's Interagency Report 6887 – 2003 Edition, Government Smart Card Interoperability Specification. Version 2.1, July 13, 2003.

- 6.3.1.3 CAC Developer's Kit version 4.2 (March 2009) or higher 2006 located at <http://www.cac.mil/common-access-card/developer-resources/>.
  - 6.3.1.4 DoD Implementation Guide for CAC Next Generation NG version 2.6 (November 2006) located at <http://www.cac.mil/common-access-card/developer-resources/>.
  - 6.3.1.5 DoD Implementation Guide for CAC PIV Endpoint version 1.22 (April 2010) located at <http://www.cac.mil/common-access-card/developer-resources/>.
  - 6.3.1.6 National Institute of Standards and Technology – Technology Administration U.S. Department of Commerce, Government Smart Card Interoperability Specification. Version 2.1, July 12, 2003, <http://smartcard.nist.gov>.
- 6.3.2 Middleware must be configurable to only support NISTR 6887 and NIST SP 800-73-3 or newer card-edges. The middleware should not request or allow entry of PIN (i.e., activation data) for other card-edges. When an unauthorized card-edge is detected, the middleware must respond with an error to the user interface. An example of the error message could be, "This card is not supported within the current configuration of middleware."

## 6.4 PKI Requirements

### 6.4.1 Supported Cryptography

6.4.1.1 Minidriver implementation shall support the exchange of information between the card and workstation when those transactions use the following cryptographic algorithms.

6.4.1.1.1 RSA 2048 and higher

6.4.1.1.2 ECC<sup>3</sup>

6.4.1.1.3 TDES

6.4.1.1.4 SHA 1

6.4.1.1.5 SHA 256 or higher<sup>3</sup>

6.4.1.1.6 AES<sup>3</sup>

---

<sup>3</sup> Requirement is only applicable when connected to cryptographic engines that support this algorithm.

## 6.5 Common Access Card (CAC) and Alternate Token

6.5.1 Minidriver implementation shall minimally support the following CAC configurations<sup>4</sup>:

6.5.1.1 Axalto Cyberflex Access 64k v1 soft mask 4 version 1

6.5.1.2 Gemplus GemXpresso (GXP) PRO 64 K

6.5.1.3 Axalto Cyberflex Access 64k v1 soft mask 4 version 2

6.5.1.4 Oberthur ID-One Cosmo v5.2D 64K

6.5.1.5 Oberthur ID-One Cosmo v5.2 72K

6.5.1.6 Schlumberber Cyberflex Access v2c 64K

6.5.1.7 Oberthur ID-One Cosmo v5.2D 72K

6.5.1.8 Gemalto GemCombiXpresso R4 dual interface

6.5.1.9 Gemalto TOP DL GX4 144K

6.5.1.10 Oberthur ID-One Cosmo 128 v5.5 for DoD CAC

### 6.5.2 Alternate Tokens

6.5.2.1 Gemalto Cyberflex Access 64k V2c

6.5.2.2 Oberthur ID-One Cosmo v5.2 64K

6.5.2.3 Specific information on DoD alternate tokens to be included at a later date.

### 6.5.3 New Card Types

6.5.3.1 Minidriver implementation shall provide support for the ability to utilize future card types (e.g. recognition of new Answer to Reset (ATR) codes) as issued by the CAC Program or other Federal PIV programs.

6.5.3.2 Vendor shall provide documentation describing the software architecture for supporting new card types. Areas of interest to the DoD are modularity and methodology.

6.5.3.3 Vendor shall provide documentation describing the process by which new card types shall be added to the middleware desktop configuration.

---

<sup>4</sup> Specific details on these CAC platforms are outlined in Appendix F. The most current listing of CAC platforms can be found at <http://www.cac.mil/common-access-card/developer-resources/>.

6.5.3.4 Minidriver implementation shall be able to utilize “new card types” without the need to restart the middleware services running on the computer or downloading of software patches, fixes, or updates.

#### 6.5.4 Card Applets

6.5.4.1 Minidriver implementation shall support all current and modified DoD CAC applets. (e.g., ID applet, Generic container applets, PKI applet, PIN management applet, Access Control Applet).

6.5.4.2 Support for new CAC applets shall be considered routine maintenance.

6.5.4.3 Support for applet changes shall be provided no later than 30 days after the vendor receives a request from the DoD.

#### 6.5.5 Certificates

6.5.5.1 Minidriver implementation shall support all DoD CACs and federally issued PIV cards using X.509 formatted PKI digital certificates.

6.5.5.2 Minidriver implementation shall support all certificate types issued under the DoD and Federal PKI certificate policies.

6.5.5.3 Minidriver implementation shall present and use certificates for PK services in accordance with key usage and extension key usage policies.

6.5.5.3.1 Minidriver implementation shall display for user selection all applicable smart card-based certificates capable of performing/completing a particular transaction based on 4.4.5.3.

6.5.5.3.2 Minidriver implementation shall not depend on the presence of a specific certificate to support cryptographic functions of another certificate. For example, the identity certificate need not be present in order to use the email signing and encryption certificates.

### 6.6 Minidriver Operating Environment

#### ***Operating System Requirements***

Minidriver shall operate with the following operating systems:

<b>Operating Systems/applications Supported by mini drivers</b>		
Windows Server 2003 Windows Server 2008	Windows VISTA SP1 Windows 7	MS Internet Explorer 7.0, 8.0, and 9.0

## 6.7 Card Readers

Minidriver shall operate and comply with any reader that is ISO 7816 compatible, Personal Computer/Smart Card (PC/SC) Windows Hardware Quality Labs (WHQL/HCL) Logo certified. Minidriver shall operate with reader drivers that are compatible with Windows 2000, Windows XP, Windows VISTA, and Windows 7 client as well as Windows Server 2003 and Windows Server 2008 operating systems.

## 6.8 Application Support

### 6.8.1 E-mail

Minidriver shall provide cryptographic services to 2007, 2010 and higher running on the operating systems outlined in section 6.6.

### 6.8.2 Cryptographic Logon

6.8.2.1 Minidrivers shall provide the means to conduct cryptographic authentication to DoD applications and operating systems listed in section 6.6.

6.8.2.1.1 The minidriver shall have the ability to use any appropriate DoD certificate as indicated by the User Principal Name in the certificate's Subject Alternative name field and the following "Enhanced Key Usage" extensions:

- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Secure Email(1.3.6.1.5.5.7.3.4)
- Client Authentication(1.3.6.1.5.5.7.3.2)

6.8.2.1.2 Minidriver shall have the capability to display all appropriate certificates on the CAC to allow the user to select the correct certificate and key pair provided that Microsoft Smart Card Logon functionality permits this capability.

6.8.2.1.3 Minidriver shall have the ability to use any appropriate Federal PIV or Federal bridge interoperable certificate on a smart card as indicated by the User Principal Name in the certificate's Subject Alternative name field and the following "Enhanced Key Usage" extensions:

- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Client Authentication(1.3.6.1.5.5.7.3.2)

6.8.2.1.4 If a single certificate on the CAC is configured for Microsoft Smart Card Log-on, the middleware shall be capable of making use of it without prior user or system action.

### 6.8.3 Client Authentication

6.8.3.1 Minidriver shall support authentication, digital signature, and encryption functions, to include SSL V3 and TLS 1.0, with browsers, operating systems and applications in section 6.6 and 6.8.1.

6.8.3.2 Minidriver shall support client authentication, which requires a 'PIN Always' access control rule. This must be configurable through the PIN management service.

6.8.3.2.1 Minidriver shall have the capability to display all appropriate certificates on the CAC or Federal PIV based on key usage to allow the user to select the correct certificate and key pair for a particular transaction.

## 6.9 PIN Management

### 6.9.1 PIN Services

6.9.1.1 Minidriver shall have the ability to set the amount of inactivity time, which should elapse before the card requires a PIN entry. Inactivity time shall be defined as the amount of time elapsed since the last time a PIN-protected area on the CAC was accessed.

6.9.1.2 Minidriver shall have the ability to disable all PIN timeout/caching features.

6.9.1.3 PIN caching must be accomplished using FIPS 140-2 level 1 or above approved cryptographic methods to protect the PIN. An outline of the implementation and the FIPS 140-2 approved methods shall be provided by the vendor.

6.9.1.4 PIN caching methods must ensure that when PINs are cached, they are visible only to the minidriver module, only stored in system memory (e.g. not on the hard disk drive), and all traces completely removed upon timeout or card removal.

6.9.1.5 PIN timeout configurations shall be configured and maintained in accordance with Appendix A, Figure 4.

### 6.9.2 PIN Change

6.9.2.1 Minidriver shall provide the ability for the user to change PINs after the end user has entered the correct PIN.

6.9.2.2 Minidriver shall enforce PIN validation rules set out in 6.9.3.

6.9.2.3 Minidriver shall require the end user to verify the new PIN before submitting the PIN change request to the CAC.

### 6.9.3 PIN Validation

6.9.3.1 Minidriver shall require all new PINs to be no less than 6 and no greater than 8 numeric characters in length.

6.9.3.2 As specified in GSC-IS 2.1, for PINs less than 8 characters, minidriver shall pad the PIN with 0xFF to the least significant bytes.

6.9.3.3 In the event an invalid PIN is entered, the minidriver shall notify the user of the error.

6.9.4 Minidriver shall indicate to the user how many remaining PIN attempts before locking.

### 6.9.5 Specific PIN Management Requirements

#### 6.9.5.1 PIN Unblock

6.9.5.1.1 PIN unblock function is a privileged activity on the CAC that is only available from specialized DoD software and workstations. This is not a function that is expected to be available from normal CACholder client workstations.

## Section C: Requirements for CAC PKCS11 Module Only

**This section outlines DoD requirements for a PKCS11 module for the CAC.**

## **7 Core DoD Requirements for CAC PKCS11 Module Only**

### **7.1 General**

- 7.1.1 PKCS11 implementation shall implement a singular generic P11 module that supports the CAC, PIV, and DoD alternate token interfaces that conform to NISTR 6887 and NIST SP 800-73-3.
- 7.1.2 PKCS11 implementation shall support PKCS11 functions listed in Appendix C, PKCS11 Functions.
- 7.1.3 Vendor shall provide a list of all unsupported PKCS11 functions.

### **7.2 Support for FIPS 201 and Associated NIST Special Publications**

- 7.2.1 PKCS11 implementation shall support NIST Special Publication 800-85.
- 7.2.2 PKCS11 implementation shall be certified by an approved NIST laboratory to be FIPS 201 compliant.
- 7.2.3 Vendors shall migrate product offerings, as part of routine maintenance, to support any updates or adjustments to FIPS 201 and any applicable NIST Special Publication.

### **7.3 Card Interfaces**

- 7.3.1 PKCS11 implementation shall support all card-edge command sets for:
  - 7.3.1.1 National Institute of Standards and Technology's Special Publication 800-73-3, "Interfaces for Personal Identity Verification," February 2010.
  - 7.3.1.2 National Institute of Standards and Technology's Interagency Report 6887 – 2003 Edition, Government Smart Card Interoperability Specification. Version 2.1, July 13, 2003.
  - 7.3.1.3 CAC Developer's Kit version 4.2 (March 2009) or higher 2006 located at <http://www.cac.mil/common-access-card/developer-resources/>.
  - 7.3.1.4 DoD Implementation Guide for CAC Next Generation NG version 2.6 (November 2006) located at <http://www.cac.mil/common-access-card/developer-resources/>.
  - 7.3.1.5 DoD Implementation Guide for CAC PIV Endpoint version 1.22 (April 2010) located at <http://www.cac.mil/common-access-card/developer-resources/>.

7.3.1.6 National Institute of Standards and Technology – Technology Administration  
U.S. Department of Commerce, Government Smart Card Interoperability  
Specification. Version 2.1, July 12, 2003, <http://smartcard.nist.gov>.

7.3.2 Middleware must be configurable to only support NISTR 6887 and NIST SP 800-73-3 or newer card-edges. The middleware should not request or allow entry of PIN (i.e., activation data) for other card-edges. When an unauthorized card-edge is detected, the middleware must respond with an error to the user interface. An example of the error message could be, “This card is not supported within the current configuration of middleware.”

## **7.4 PKI Requirements**

### **7.4.1 Supported Cryptography**

7.4.1.1 PKCS11 implementation shall support the exchange of information between the card and workstation when those transactions use the following cryptographic algorithms.

7.4.1.1.1 RSA 2048 and higher

7.4.1.1.2 ECC<sup>5</sup>

7.4.1.1.3 TDES

7.4.1.1.4 SHA 1

7.4.1.1.5 SHA 256 or higher<sup>5</sup>

7.4.1.1.6 AES<sup>5</sup>

## **7.5 Common Access Card (CAC) and Alternate Tokens**

7.5.1 PKCS11 implementation shall minimally support the following CAC configurations<sup>6</sup>:

7.5.1.1 Axalto Cyberflex Access 64k v1 soft mask 4 version 1

7.5.1.2 Gemplus GemXpresso (GXP) PRO 64 K

7.5.1.3 Axalto Cyberflex Access 64k v1 soft mask 4 version 2

---

<sup>5</sup> Requirement is only applicable when connected to cryptographic engines that support this algorithm.

<sup>6</sup> Specific details on these CAC platforms are outlined in Appendix F. The most current listing of CAC platforms can be found at <http://www.cac.mil/common-access-card/developer-resources/>.

- 7.5.1.4 Oberthur ID-One Cosmo v5.2D 64K
- 7.5.1.5 Oberthur ID-One Cosmo v5.2 72K
- 7.5.1.6 Schlumberber Cyberflex Access v2c 64K
- 7.5.1.7 Oberthur ID-One Cosmo v5.2D 72K
- 7.5.1.8 Gemalto GemCombiXpresso R4 dual interface
- 7.5.1.9 Gemalto TOP DL GX4 144K
- 7.5.1.10 Oberthur ID-One Cosmo 128 v5.5 for DoD CAC

#### 7.5.2 Alternate Tokens

- 7.5.2.1 Gemalto Cyberflex Access 64k V2c
- 7.5.2.2 Oberthur ID-One Cosmo v5.2 64K
- 7.5.2.3 Specific information on DoD alternate tokens to be included at a later date.

#### 7.5.3 New Card Types

- 7.5.3.1 PKCS11 implementation shall provide support for the ability to utilize future card types (e.g. recognition of new Answer to Reset (ATR) codes) as issued by the CAC Program or other Federal PIV programs.
- 7.5.3.2 Vendor shall provide documentation describing the software architecture for supporting new card types. Areas of interest to the DoD are modularity and methodology.
- 7.5.3.3 Vendor shall provide documentation describing the process by which new card types shall be added to the middleware desktop configuration.
- 7.5.3.4 PKCS11 implementation shall be able to utilize “new card types” without the need to restart the middleware services running on the computer or downloading of software patches, fixes, or updates.

#### 7.5.4 Card Applets

- 7.5.4.1 PKCS11 implementation shall support all current and modified DoD CAC applets. (e.g., ID applet, Generic container applets, PKI applet, PIN management applet, Access Control Applet).
- 7.5.4.2 Support for new CAC applets shall be considered routine maintenance.
- 7.5.4.3 Support for applet changes shall be provided no later than 30 days after the vendor receives a request from the DoD.

## 7.5.5 Certificates

7.5.5.1 PKCS11 implementation shall support all DoD CACs and federally issued PIV cards using X.509 formatted PKI digital certificates.

7.5.5.2 PKCS11 implementation shall support all certificate types issued under the DoD and Federal PKI certificate policies.

7.5.5.3 PKCS11 implementation shall present and use certificates for PK services in accordance with key usage and extension key usage policies.

7.5.5.3.1 PKCS11 implementation shall display for user selection all applicable smart card-based certificates capable of performing/completing a particular transaction based on 4.4.5.3.

7.5.5.3.2 PKCS11 shall not depend on the presence of a specific certificate to support cryptographic functions of another certificate. For example, the identity certificate need not be present in order to use the email signing and encryption certificates.

## 7.6 PKCS11 Operating Environment

7.6.1 Operating System Requirements. PKCS11 shall operate with the operating systems and applications listed in appendix A, figure 5.

## 7.7 Card Readers

PKCS11 shall operate and comply with any reader that is ISO 7816 compatible, Personal Computer/Smart Card (PC/SC) Windows Hardware Quality Labs (WHQL/HCL) Logo certified.

## 7.8 Application Support

### 7.8.1 E-mail

PKCS11 shall expose cryptographic services to e-mail packages that support PKCS11 interfaces.

### 7.8.2 Client Authentication

7.8.2.1 PKCS11 shall support authentication, digital signature, and encryption functions, to include SSL V3 and TLS 1.0, with browsers, operating systems and applications in section Appendix A, figure 5.

7.8.2.2 PKCS11 shall support client authentication, which requires a 'PIN Always' access control rule. This must be configurable through PIN management service.

7.8.2.2.1 PKCS11 shall have the capability to display all appropriate certificates on the CAC or Federal PIV based on key usage to allow the user to select the correct certificate and key pair for a particular transaction.

## **7.9 PIN Management**

### **7.9.1 PIN Services**

7.9.1.1 PKCS11 shall have the ability to set the amount of inactivity time, which should elapse before the card requires a PIN entry. Inactivity time shall be defined as the amount of time elapsed since the last time a PIN-protected area on the CAC was accessed.

7.9.1.2 PKCS11 shall have the ability to disable all PIN timeout/caching features.

7.9.1.3 PIN caching must be accomplished using FIPS 140-2 level 1 or above approved cryptographic methods to protect the PIN. An outline of the implementation and the FIPS 140-2 approved methods shall be provided by the vendor.

7.9.1.4 PIN caching methods must ensure that when PINs are cached, they are visible only to the PKCS11 module, only stored in system memory (e.g. not on the hard disk drive), and all traces completely removed upon timeout or card removal.

7.9.1.5 PIN timeout configurations shall be configured and maintained in accordance with Appendix A, Figure 4.

### **7.9.2 PIN Change**

7.9.2.1 PKCS11 shall provide the ability for the user to change PINs after the end user has entered the correct PIN.

7.9.2.2 The PKCS11 shall enforce PIN validation rules set out in 7.9.3.

7.9.2.3 PKCS11 shall require the end user to verify the new PIN before submitting the PIN change request to the CAC.

### **7.9.3 PIN Validation**

7.9.3.1 PKCS11 shall require all new PINs to be no less than 6 and no greater than 8 numeric characters in length.

7.9.3.2 As specified in GSC-IS 2.1, for PINs less than 8 characters, PKCS11 shall pad the PIN with 0xFF to the least significant bytes.

7.9.3.3 In the event an invalid PIN is entered, PKCS11 shall notify the user of the error.

7.9.3.4 PKCS11 shall indicate to the user how many remaining PIN attempts before locking.

#### 7.9.4 Specific PIN Management Requirements

##### 7.9.4.1 PIN Unblock

7.9.4.1.1 PIN unblock function is a privileged activity on the CAC that is only available from specialized DoD software and workstations. This is not a function that is expected to be available from normal CACholder client workstations.

## Appendix A

**Figure 1: Configurable Options**

Middleware Configurable Options Summary		
Option	Default Privilege Level	Default Settings
Certificate Auto Registration	Admin	On
Certificate Removal on Logoff	Admin	Off
Certificate Removal on Card Removal	Admin	Off
CAM Allow	Admin	On
CAM Time Out Setting	Admin	15
CAM Decrypt (optional)	Admin	On
CAM Sign (optional)	Admin	Off
CAM Other (optional)	Admin	On

**Figure 2: CSP Key**

CSP Key			
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider] \<CSP NAME> <<CSP NAME>> Should be replaced with the provider name			
Key Values	Type	Setting	Default Setting
Image Path	REG_SZ	<CSP DLL>	N/A
Type	REG_DWORD	<CSP Type>	N/A
Signature	REG_BINARY	<CSP Signature>	N/A
SigInFile*	REG_DWORD	0x00000000	0x00000000
Setting Description			
<CSP DLL>	The Image path value is a string value and is the name or fully qualified path of the CSP DLL		
<CSP Type>	3-digit CSP type as specified in the Security section of the Microsoft Platform SDK		
<CSP Signature>*	The digital signature of the CSP DLL		
SigInFile*	Optional replacement for <CSP Signature> on Windows 2000 and XP platforms. This value must be 0x00000000.		
* Only one of the "Signature" or "SigInFile" entries is required.			

Example
<pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ CAC Cryptographic Provider] "Image Path"="CAC_CSP.dll" "Type"=dword:00000001 "Signature"=hex:6c,32,98,03,c9,db,03,d9,dc,b9,a9,64,f8,a6,05,10,f5,dd,27,33,ae,\ 70,84,d5,20,1a,03,7b,3b,7d,d0,a8,b6,1c,47,0b,0e,5e,e5,94,94,36,f4,fc,c2,8b,\ 05,85,ac,e6,17,c8,27,3e,17,d6,64,56,94,82,e2,5a,18,bd,6d,15,7d,52,26,d6,98,\ 2b,e4,b6,fe,70,f3,ea,bc,aa,c1,c4,87,27,ac,3d,cf,ce,36,b9,59,57,f0,ad,3e,ba,\ 5a,ff,db,f6,ce,59,9e,a2,49,19,1f,5c,55,f5,20,b8,ef,7e,06,f7,b1,45,0f,9f,2b,\ 8e,0e,d9,31,50,c5,30,00,00,00,00,00,00,00,00,00</pre>

**Figure 3: Certificate Registration Key**

Certificate Registration Key			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration]			
Key Values	Type	Setting	Default Setting
AutoReg	REG_DWORD	0x00000000 (Feature is off) -OR- 0x00000001 (Feature is on)	0x00000001
AutoUnRegOnLogoff	REG_DWORD	0x00000000 (do not un-register on logoff) -OR- 0x00000001 (un-register on logoff)	0x00000000
AutoUnRegOnRemove	REG_DWORD	0x00000000 (do not un-register on card removal) -OR- 0x00000001 (un-register on card removal)	0x00000000
Setting Description			
AutoReg	If turned off, middleware will not register the CAC certificates. If on, the middleware will register the certificates.		
AutoUnRegOnLogoff	Middleware will/will not unregister certificates on the logoff event.		
AutoUnRegOnRemove	Middleware will/ will not unregister certificates on card removal event.		

Example
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration] "AutoReg"=dword:00000001 "AutoUnRegOnLogoff"=dword:00000001 "AutoUnRegOnRemove"=dword:00000000

**Figure 4: Pin Configuration Key**

PIN Configuration Key			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication]			
Key Values	Type	Setting	Default Setting
Allow	REG_DWORD	0x00000000 (Feature is off) -OR- 0x00000001 (Feature is on)	0x00000001
Minutes	REG_DWORD	< 0x80000000 = number of minutes to allow automatic authentication  0x80000000 = no timeout value for automatic authentication during a session  > 0x80000000 = reserved values	0x0000000F
Setting Description			
Allow	If turned off, middleware will not provide any CAM services.		
Minutes	Number of minutes (hex) the CAM will keep PIN presentations from occurring.		
Example			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication] "Allow"=dword:00000001 "Minutes"=dword:00000000			

**Figure 5: Web Servers, Browsers, and Applications**

Web Servers, Browsers, and Applications	
OS	<ul style="list-style-type: none"> <li>▪ Windows 2000 (all SPs)</li> <li>▪ Windows XP SP-3</li> <li>▪ Windows VISTA</li> <li>▪ Windows 7</li> </ul>
Web browsers	<ul style="list-style-type: none"> <li>▪ MS Internet Explorer 7.0, 8.0, and 9.0</li> <li>▪ Firefox Mozilla</li> </ul>
Web Servers	<ul style="list-style-type: none"> <li>▪ Windows 2003</li> <li>▪ Windows 2008</li> <li>▪ Apache</li> </ul>
Other Applications	<ul style="list-style-type: none"> <li>▪ Citrix Client 10.100.55.836 or higher</li> <li>▪ Citrix Presentation Server (or XenApps) 4.5 or higher</li> <li>▪ Citrix server version 11.2 or higher</li> </ul>

**Figure 6: Primary Email and OS Combinations**

Primary Email OS Combinations				
Operating System	Email Clients			
	Outlook 2K SP2	Outlook 2002	Outlook 2003	Outlook 2007
Windows 2000	X	X	X	X
Windows XP	X	X	X	X
Windows VISTA	X	X	X	X
Windows 7	X	X	X	X

**Figure 7: Bug Classifications**

Middleware Bug Classifications	
The DoD shall be the sole determinant of middleware bug classifications.	
Category	Definition

1- Critical	The failure causes a system crash or unrecoverable data loss or jeopardizes personnel.
2- High	The failure causes impairment of critical system functions and no work around solution exists.
3- Medium	The failure causes impairment of critical system functions, though a work around solution does exist.
4- Low Required	The failure causes inconvenience or annoyance.
5- Low Desired	None of the above, or the anomaly concerns an enhancement rather than a failure.

## Appendix B- CSP Functions

All CSPs should support the following entry points as documented in the Security section of the Microsoft Windows Platform SDK at:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/entry\\_points.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/entry_points.asp)

All custom CSPs must support all of the following DLL entry points:

CPAcquireContext  
CPCreateHash  
CPDecrypt  
CPDeriveKey  
CPDestroyHash  
CPDestroyKey  
CPEncrypt  
CPExportKey  
CPGenKey  
CPGenRandom  
CPGetHashParam  
CPGetKeyParam  
CPGetProvParam  
CPGetUserKey  
CPHashData  
CPHashSessionKey  
CPImportKey  
CPReleaseContext  
CPSetHashParam  
CPSetKeyParam  
CPSetProvParam  
CPSignHash  
CPVerifySignature

All PROV\_RSA\_SCHANNEL and PROV\_DH\_SCHANNEL CSPs must also support the following DLL entry points: (These entry points are optional for other custom CSPs)

CPDuplicateHash  
CPDuplicateKey

Note: All of these functions must be declared with the WINAPI keyword.

## Appendix C- PKCS 11 Functions

The P11 module should be compatible with at least Version 2.11 of the cryptoki header files available at: <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html>.

**Note: DoD understands during the development of this document, a newer version was released, but version 2.11 is still widely used; therefore, it is a minimum requirement.**

The PKCS#11 registry setting shall identify the vendor and the fully qualified path of the DLL that supports the PKCS#11 interface.

Key			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\<<Vendor Name>>			
Key Values	Type	Setting	Default Setting
"PKCS#11DLL"	String	<PKCS#11 DLL>	N/A
"Vendor"	String	<Name of Vendor>	N/A
Setting Description			
<PKCS#11 DLL>	Fully qualified path to the PKCS11 DLL		
<Name of Vendor>	Vendor's full name.		
Example			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\PKCS#11\Vendor1] "PKCS#11DLL"="c:\windows\system32\pkcs11.dll" "Vendor"="Middleware Vendor 1"			

**Figure 9**

PKCS#11 Test Inputs	
CK_ATTRIBUTE one[7], two[7], three[7];	two[3].type = CKA_MODIFIABLE;
CK_OBJECT_CLASS cko_data = CKO_DATA;	two[3].pValue = &__true;
CK_BBOOL __false = CK_FALSE, __true = CK_TRUE;	two[3].ulValueLen = sizeof(CK_BBOOL);
char *key = "TEST PROGRAM";	two[4].type = CKA_LABEL;
CK_ULONG key_len = strlen(key);	two[4].pValue = "Test data object two";
one[0].type = CKA_CLASS;	two[4].ulValueLen = strlen((const

	char*)two[4].pValue);
one[0].pValue = &cko_data;	two[5].type = CKA_APPLICATION;
one[0].ulValueLen = sizeof(CK_OBJECT_CLASS);	two[5].pValue = key;
one[1].type = CKA_TOKEN;	two[5].ulValueLen = key_len;
one[1].pValue = &__false;	two[6].type = CKA_VALUE;
one[1].ulValueLen = sizeof(CK_BBOOL);	two[6].pValue = "Object two";
one[2].type = CKA_PRIVATE;	two[6].ulValueLen = strlen((const char*)two[6].pValue);
one[2].pValue = &__false;	three[0].type = CKA_CLASS;
one[2].ulValueLen = sizeof(CK_BBOOL);	three[0].pValue = &cko_data;
one[3].type = CKA_MODIFIABLE;	three[0].ulValueLen = sizeof(CK_OBJECT_CLASS);
one[3].pValue = &__true;	three[1].type = CKA_TOKEN;
one[3].ulValueLen = sizeof(CK_BBOOL);	three[1].pValue = &__false;
one[4].type = CKA_LABEL;	three[1].ulValueLen = sizeof(CK_BBOOL);
one[4].pValue = "Test data object one";	three[2].type = CKA_PRIVATE;
one[4].ulValueLen = strlen((const char*)one[4].pValue);	three[2].pValue = &__false;
one[5].type = CKA_APPLICATION;	three[2].ulValueLen = sizeof(CK_BBOOL);
one[5].pValue = key;	three[3].type = CKA_MODIFIABLE;
one[5].ulValueLen = key_len;	three[3].pValue = &__true;
one[6].type = CKA_VALUE;	three[3].ulValueLen = sizeof(CK_BBOOL);
one[6].pValue = "Object one";	three[4].type = CKA_LABEL;
one[6].ulValueLen = strlen((const char*)one[6].pValue);	three[4].pValue = "Test data object three";
two[0].type = CKA_CLASS;	three[4].ulValueLen = strlen((const char*)three[4].pValue);
two[0].pValue = &cko_data;	three[5].type = CKA_APPLICATION;
two[0].ulValueLen = sizeof(CK_OBJECT_CLASS);	three[5].pValue = key;
two[1].type = CKA_TOKEN;	three[5].ulValueLen = key_len;
two[1].pValue = &__false;	three[6].type = CKA_VALUE;
two[1].ulValueLen = sizeof(CK_BBOOL);	three[6].pValue = "Object three";
two[2].type = CKA_PRIVATE;	three[6].ulValueLen = strlen((const char*)three[6].pValue);
two[2].pValue = &__false;	C_OpenSession(pSlots[i], CKF_SERIAL_SESSION, (CK_VOID_PTR)NULL, (CK_NOTIFY)NULL, &h);
two[2].ulValueLen = sizeof(CK_BBOOL);	

Figure 10

## Appendix D- BSI Functions

The BSI module(s) should comply with the most current version of GSC-IS found at:  
<http://smartcard.nist.gov>.

All BSI functions listed in the GSC-IS document must be supported and must include at least the following:

- gscBsiUtilAcquireContext
- gscBsiUtilConnect
- gscBsiUtilDisconnect
- gscBsiUtilBeginTransaction
- gscBsiUtilEndTransaction
- gscBsiUtilGetVersion
- gscBsiUtilGetCardProperties
- gscBsiUtilGetCardStatus
- gscBsiUtilGetExtendedErrorText
- gscBsiUtilGetReaderList
- gscBsiUtilPassthru
- gscBsiUtilReleaseContext
- gscBsiGcDataCreate
- gscBsiGcDataDelete
- gscBsiGcGetContainerProperties
- gscBsiGcReadTagList
- gscBsiGcReadValue
- gscBsiGcUpdateValue
- gscBsiGetChallenge
- gscBsiSkiInternalAuthenticate
- gscBsiPkiCompute
- gscBsiPkiGetCertificate
- gscBsiGetCryptoProperties

## **Appendix E- BSI Header Files**

The latest version of the BSI headers which will work with either GSC-IS 2.0 or GSC-IS 2.1 are tagged as version 2.1.1.1. Link to be provided at a later time.

## Appendix F- References

In developing this document, the following documents have been used to develop a smart card middleware body of knowledge. Some of these documents are formal specifications or standards; others are maybe memos, drafts, or web documents. This listing is provided for reader reference and convenience. Unless otherwise specified in this document, these documents should be used for information only.

### Government References

- Department of Defense Access Card Office (ACO), "Common Access Card (CAC) Release 1.0 Reader Specifications" Version 1.01, August 17, 2007.
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
- National Institute of Standards and Technology – Inter-Agency Report 6887 – 2003 Edition, Government Smart Card Interoperability Specification. Version 2.1, July 13, 2003, <http://smartcard.nist.gov>
- NIST Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, February 2005, <http://csrc.nist.gov/piv-project>
- NIST Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, May 2001, <http://csrc.nist.gov/publications/fips/>
- NIST Special Publication 73, Interfaces for Personal Identity Verification, April 2005, <http://csrc.nist.gov/piv-project>
- NIST Special Publication 78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, April 2005, <http://csrc.nist.gov/piv-project>
- NIST Special Publication 800-85, PIV middleware and PIV Card Application Conformance Test Guidelines, October 2005, <http://csrc.nist.gov/piv-project>
- U.S. General Services Administration (GSA), Government Smart Card Handbook, February 2004.

## Industry References

- GlobalPlatform, Global Platform – The Standard for Smart Card Infrastructure: Overview, June 2004,
- International Organization for Standardization (ISO), ISO/IEC 7816-1 Identification Cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics, 1998.
- International Organization for Standardization (ISO), ISO/IEC 7816-1 Identification Cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics. Amendment 1: Maximum height of the IC contact surface, 2003.
- International Organization for Standardization (ISO), ISO/IEC 7816-2 Identification Cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and locations of the contacts, 2007.
- International Organization for Standardization (ISO), ISO/IEC 7816-3 Identification Cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols, 2006.
- International Organization for Standardization (ISO), ISO/IEC 7816-4 Identification Cards – Integrated circuit(s) cards with contacts – Part 4: Organization, security and commands for interchange, 2005.
- International Organization for Standardization (ISO), ISO/IEC 7816-5 Identification Cards – Integrated circuit(s) cards with contacts – Part 5: Registration of application providers, 2004.
- International Organization for Standardization (ISO), ISO/IEC 7816-6 Identification Cards – Integrated circuit(s) cards with contacts – Part 6: Inter-industry data elements for interchange, 2004.
- Microsoft Corporation, Cryptography API Service Provider, <http://download.microsoft.com/download/win2000pro/utility/v2.0/w98NT42KMe/EN-US/cspdk.exe>
- Microsoft Corporation, Windows Marketplace Tested Products List Webpage, Results from site search on ‘Smart Card Reader’ is located at <http://testedproducts.windowsmarketplace.com/results.aspx?text=smart+card+reader>
- Microsoft Corporation, Windows Smart Card Minidriver Specification Version 7.06 (July 1, 2009)

- Microsoft Corporation, Windows 2000 Hardware Compatibility List Webpage, Results from site search on 'Smart Card Reader' is located at <http://www.microsoft.com/whdc/hcl/search.mspix>
- Microsoft Corporation, "How to Get in the Windows Catalog?" Web page, <http://www.microsoft.com/winlogo/windowscatalog.mspix>
- OpenCard Consortium, OpenCard Framework – General Information Web Document." Second Edition, October 1998.
- PC/SC Workgroup Specifications Revision 2.01.00, Interoperability Specification for ICCs and Personal Computer Systems, June 2005
- Public Key Cryptographic Standard #11 version 2.11, [www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html](http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html)
- Smart Card in the Linux Environment (M.U.S.C.L.E), [www.linuxnet.com](http://www.linuxnet.com)

## Appendix G- List of CAC Platform Configurations

Attributes	Obsolete Platforms		
Card Manufacturer	Oberthur Card Systems (OCS) - Original Pilot CAC	Schlumberger (Axalto)	Oberthur Card System (OCS)
Product Name	Galactic v1 32K	Cyberflex 32k v2 card with Softmask 7 Version 2	CosmopolIC v4 32K
Laser Engraving on back of card	OCS Gal 2.1	Schlumberger Access 32K V2	Oberthur CosmopolIC v4
Chip Size (EEPROM)	32K	32K	32K
Answer to Reset (ATR)	3B 7D 11 0000 00 31 80 71 8E 64 86D60200 82 9000	3b6500009c020207 02	3B 7F 11 0000 00 31 C0 53 CAC401 64 52D90400 82 9000
CAC Applet Package	V1 Applets	V1 Applets	V1 Applets
Other features*	Contact only RSA EE 1024	Contact only RSA EE 1024	Contact only RSA EE 1024
Operational Intro Date	Fall 2000	N/A	N/A
Operational Sunset Date	Spring 2004	End of Spring 2005	End of Spring 2005
Expiration of last card issued	End of Spring 2008	End of Spring 2008	End of Spring 2008

Attributes	Obsolete Platforms			
Card Manufacturer	Axalto	Gemplus	Axalto	Oberthur Card Systems (contactless pilot)
Product Name	Axalto Cyberflex Access 64k v1 soft mask 4 version 1	GemXpresso (GXP) PRO 64 K	Axalto Cyberflex Access 64k v1 soft mask 4 version 2	ID-One Cosmo v5.2D 64K
Laser Engraving on back of card	Axalto Access 64KV2	Gemplus GXP3 64V2N	Axalto Access 64KV2	Oberthur C.S. Cosmo64 V5.2D
Chip Size (EEPROM)	64K	64K	64K	64K
Answer to Reset (ATR)	3B7512000029 05010401	3B6B00008065B 0830104748300 9000	3B75120000290 5010401	3B DB 96 00 80 1F 03 00 31 C0 64 77E30300 82 9000 C1
CAC Applet Package	V2.3	V2.3 and V2.3.0c Applets	V2.3.0c Applets	V2.6.1 Applets
Other features*	Contact Only RSA EE 1024	Contact only RSA EE 1024	Contact only RSA EE 1024	Dual interface RSA EE 1024
Operational Intro Date	April 2005	N/A	N/A	May 2006
Operational Sunset Date	Q1 CY 2007	Q1 CY 2007	Q1 CY 2007	Q2 CY 2007
Expiration of last card issued	Q1 CY 2010	Q1 CY 2010	Q1 CY 2010	Q2 CY 2010

Attributes	Current Platforms			
Card Manufacturer	Oberthur Card Systems	Gemalto	Oberthur Card Systems (PIV Transitional)	Gemalto (PIV Transitional)
Product Name	ID-One Cosmo v5.2 72K	Cyberflex Access v2c 64K	ID-One Cosmo v5.2D 72K	Gemalto GemCombiXpresso R4 dual interface
Laser Engraving on back of card	Oberthur ID One V5.2	Gemalto Access 64KV2	Oberthur ID One V5.2 Dual	Gemalto GCX4 72K DI
Chip Size (EEPROM)	72K	64K	72K	72K
Answer to Reset (ATR)	3B DB 96 00 80 1F 03 00 31 C0 64 77E30300 82 9000 C1	3B959540FFAE 01030000	3B DB 96 00 80 1F 03 00 31 C0 64 77E30300 82 9000 C1	3B 7D 96 00 00 80 31 80 65 B0 83 11 13 AC 83 00 90 00
CAC Applet Package	V2.6.1 Applets	V2.6.1 Applets	V2.6.2 Applets	V2.6.2 Applets
Other features*	Contact only  RSA EE 1024	Contact only  RSA EE 1024	Dual interface  RSA EE 1024	Dual interface  RSA EE 1024
Operational Intro Date	January 2007	February 2007	October 2006/ March 2007	June 2008
Operational Sunset Date	July 2010	September 2010	September 2008	September 2008
Expiration of last card issued	July 2013	September 2013	September 2011	September 2011

Attributes				
Card Manufacturer	Oberthur Card Systems (PIV Endpoint) with PIV endpoint applet and PIV auth cert	Gemalto (PIV Endpoint) with PIV endpoint applet and PIV auth cert	Gemalto (PIV Endpoint)	Oberthur Card System (PIV Endpoint)
Product Name	ID-One Cosmo v5.2D 72K	Gemalto GemCombiXpresso R4 dual interface	Gemalto TOP DL GX4 144K	Oberthur ID-One Cosmo 128 v5.5 for DoD CAC
Laser Engraving on back of card	Oberthur ID One V5.2 Dual	Gemalto GCX4 72K DI	Gemalto TOP DL GX4 144K	Oberthur ID One 128 v5.5 Dual
Chip Size (EEPROM)	72K	72K	144K	128K
Answer to Reset (ATR)	3B DB 96 00 80 1F 03 00 31 C0 64 77E30300 82 9000 C1	3B 7D 96 00 00 80 31 80 65 B0 83 11 13 AC 83 00 90 00	3B 7D 96 00 00 80 31 80 65 B0 83 11 17 D6 83 00 90 00  (Updated March 2009)	3B DB 96 00 80 1F 03 00 31 C0 64 B0 F3 10 00 07 9000 80
CAC Applet Package	V2.6.2 Applets	V2.6.2 Applets	V2.6.2b Applets	V2.6.2b Applets
Other features*	Dual interface  RSA EE 1024	Dual interface  RSA EE 1024	Dual interface  RSA EE 2048	Dual interface  RSA EE 2048
Operational Intro Date	June 2008	June 2008	July/August 2009	August/September 2010
Operational Sunset Date	February 2011	Ongoing	Ongoing	Ongoing
Expiration of last card issued	February 2014	Ongoing	Ongoing	Ongoing