
COMMON ACCESS CARD RELEASE 1.0
ICC REQUIREMENTS

FINAL Version 1.1
February 8, 2001

Prepared by: Chip Allocation Technical Workgroup

Prepared for: Smart Card Senior Coordinating Group

--FOR OFFICIAL USE ONLY--

I. Changes

Each version of the ***Common Access Card Release 1.0 ICC Requirements*** document will be recorded in this section. As changes are recommended and approved, they will be reflected in this section.

Baseline: Draft Version 1.0, 24 May 2000.

Version 1.1 FINAL as of 8 February 2001:

At the 9 January 2001 Meeting of the Smart Card Senior Coordinating Group, further clarification and guidance was approved regarding Backward Compatibility. The changes made to the Baseline version are reflective of the direction of the SCSCG.

Changes include:

1. *Page vi and vii, Executive Summary, Key Area #2: Backward Compatibility* Recommendation B expanded to acknowledge policy clarification.
2. *Page 6, 3.1.1 Existing Smart Card Initiatives to CAC Release 1.0.* Added specific clarifications and guidance regarding Backward Compatibility policy change.
3. *Page 7, 3.1.2 Beyond CAC Release 1.0.* Updated the reference to the latest version of the Configuration Management Plan

TABLE OF CONTENTS

| | |
|---|-----------|
| EXECUTIVE SUMMARY | V |
| 1 INTRODUCTION..... | 1 |
| 1.1 REFERENCE DOCUMENTATION..... | 2 |
| 2 DOD FUNCTIONALITY..... | 2 |
| 2.1 DEFINITION | 2 |
| 2.1.1 <i>Data Element Requirements</i> | 2 |
| 2.1.2 <i>DoD PKI Requirements</i> | 3 |
| 2.1.3 <i>Physical Access Requirements</i> | 4 |
| 2.2 RECOMMENDATION..... | 4 |
| 2.3 DOD FUNCTIONALITY CONCEPT OF OPERATION (CONOPS) | 4 |
| 2.3.1 <i>Issuance Process</i> | 4 |
| 2.3.2 <i>Data Element Use Process</i> | 5 |
| 2.3.3 <i>PKI Use Process</i> | 5 |
| 3 BACKWARD COMPATIBILITY | 6 |
| 3.1.1 <i>Existing Smart Card Initiatives to CAC Release 1.0</i> | 6 |
| 3.1.2 <i>Beyond CAC Release 1.0</i> | 7 |
| 4 CARD ARCHITECTURE AND PLATFORM..... | 8 |
| 4.1 DEFINITION | 8 |
| 4.1.1 <i>Basic Assumptions</i> | 8 |
| 4.2 CAC RELEASE 1.0 ICC REQUIREMENTS | 8 |
| 4.3 GOALS IN EVALUATING CARD ARCHITECTURE | 10 |
| 4.4 SMART CARD TECHNOLOGY PERSPECTIVES | 11 |
| 4.5 EVALUATION..... | 12 |
| 4.5.1 <i>Interoperability</i> | 12 |
| 4.5.2 <i>Open Architecture/Standards Based</i> | 17 |
| 4.5.3 <i>Non-Obsolescence</i> | 17 |
| 4.5.4 <i>Best Practices</i> | 18 |
| 4.5.5 <i>Post Issuance Functionality</i> | 18 |
| 4.6 OTHER CONSIDERATIONS..... | 19 |
| 4.7 RECOMMENDATIONS..... | 19 |
| 4.7.1 <i>Open Platform</i> | 21 |
| 4.7.2 <i>Java™ 2.1 Smart Card Operating System</i> | 21 |
| 4.7.3 <i>Modern Cryptography with On-card Key Generation</i> | 22 |
| 4.7.4 <i>Large Commercially Available Application Space</i> | 22 |
| 4.7.5 <i>Security</i> : | 22 |
| 5 IDENTIFIED OPEN ITEMS..... | 23 |

APPENDIX 1: REFERENCES..... 25

APPENDIX 2: ABBREVIATIONS AND ACRONYMS..... 28

APPENDIX 3: TERMS AND DEFINITIONS 31

APPENDIX 4: APPLICABLE STANDARDS 34

APPENDIX 5: CAC DATA ELEMENT DEFINITION MATRIX..... 37

APPENDIX 6: WHITE PAPER—SMART CARDS: DESIGNING A HYBRID CARD ARCHITECTURE FROM A WEB-CENTRIC AND CARD-CENTRIC PERSPECTIVE 40

APPENDIX 7: CAC INTEROPERABILITY FINDINGS..... 45

APPENDIX 8: CAC MIDDLEWARE REQUIREMENTS 53

Executive Summary

DEPSECDEF Memorandum dated November 10, 1999, directed that the Common Access Card (CAC) serve as an identification card, building access card, and carrier of DoD PKI credentials. The Smart Card Senior Coordinating Group (SCSCG) established the Chip Allocation Technical Work Group (CAT WG) to examine three key areas:

Key Area #1: DoD Functionality

DoD functionality is defined as all DoD requirements and all allocated space that will be on every issued CAC. This is different from Component specific allocated space. For Release 1.0, the CAT WG broke the DoD functionality into the following areas:

1. Core Data Requirements

As a baseline for discussions, each Component examined data elements used in existing smart card initiatives. The work group focused on those elements that members would consider common across all Components, and concluded that those data requirements from a DoD perspective needed to be minimal and, to the extent possible, static in nature.

Note: DoD identification requirements are a part of the overall core data requirements.

2. DOD PKI Requirements

The DoD PKI PMO provided the number of keys and certificates the CAC needed to support the DoD PKI Class 3 Architecture. In the 10 November 1999 DEPSECDEF memo, there are discussions about providing logical access. The CAT WG focused on the DoD PKI recommendations in fulfilling this requirements; however, we recognize that there are several other methods in which to implement or provide logical access. All other types of implementations should fall within the Component specific area of the CAC.

3. Physical Access Requirements

Requirements for physical access shall be minimally accommodated by the use of the DoD SEIWG standard. The SEIWG can be implemented on several different media residing on a card (e.g. magnetic stripe, barcode, or chip). A recommendation on the type of implementation for the CAC remains open. The SCSCG shall be responsible for directing which media(s) Release 1.0 must support.

Recommendation A

The CAT WG recommends the approval of the following allocation table for CAC Release 1.0:

| CAC Functionality | Space | Overhead | Total |
|---|---------------|---------------|----------------|
| DoD: Data Elements (Maximum Space) | 0.2 Kilobytes | 2.2 Kilobytes | 2.4 Kilobytes |
| DoD: PKI (Maximum Space) | 8.3 Kilobytes | 2.0 Kilobytes | 10.3 Kilobytes |
| Enhancement to CAC Platform (Maximum Space) | 10 Kilobytes | N/A | 10.0 Kilobytes |
| Component Specific Area (Minimum Space) | 7 Kilobytes | N/A | 7 Kilobytes |
| Total | 25.5 | 4.2 | **29.7 |

**Note: The CAT WG recommends that all additional space be designated to the Component specific area.

Key Area #2: Backward Compatibility

Backward compatibility focuses on policy methods used to deal with existing smart card initiatives and subsequent releases of the CAC.

Recommendation B

The CAT WG recommends the approval of the following policy:

1. The CAC shall be backward compatible with existing smart card initiatives such that either the card contains (in the combined DoD and Component Specific areas) the same amount of data as it currently carries or existing applications will be modified to provide the same business functionality. The CAT WG recommends a card architecture that will provide either of the above; however, it is the responsibility of the Components to achieve.

Further clarification and guidance of the Backward Compatibility policy was provided as part of the Smart Card Senior Coordinating Group (SCSCG) Meeting on 9 January 2001. These clarifications address:

- ⌘ Reclassification of previously named "Joint" applications.
- ⌘ Identification of Life Cycle Managers (LCMs)
- ⌘ The optional approach towards the loading and use of these applications.
- ⌘ The limited life span (end of FY 02) of these applications.

The above policy, approved at the 9 January 2001 SCSCG Meeting, is fully compliant with the Configuration Management Plan (CMP) for Component-specific applications. The decision to use these applications rests completely

with the C/S/A. It ensures that the current users of these applications have the capability to continue to use the applications with the CAC. It provides sufficient time for the C/S/A to fund continued support of these applications, if desired, and the Joint Staff to develop proposed joint applications in accordance with the CMP.

2. Subsequent releases of the CAC shall be cognizant of prior requirements. Before each subsequent release, the Smart Card Senior Coordinating Group will review recommendations in accordance with existing features or DoD functionality. If there are modifications or deletions of functionality, the changes will get approval from the Smart Card Senior Coordination Group. In addition, if changes are made to the card architecture, the Components must be advised and given ample time to adjust component specific code or file structures to accommodate those changes. Specifics of this process are addressed in the Smart Card Configuration Management Plan (CMP).

Key Area #3: Card Architecture and Platform

In examining Key Area #3, the following facts about smart card technology are apparent:

- ? ? Historically, the standard for measuring maturity has been interoperability. In this sense, the Smart Card technology is immature. While there are a number of standards already developed by the government and industry, they still fall short of allowing full interoperability. This goal will not be fully met until industry or government forces some final standards.
- ? ? Smart Cards are very small computers. From 8K to 32K of EEPROM, most currently available cards contain reserved space for system overhead. This is analogous to the first PCs, where both processor power and storage were issues. In the early deployment, card overhead will be a source of concern; however, it should lessen very quickly as the technology advances.

The working group established the following goals in evaluating card architecture:

1. Interoperability: Smart cards should be treated as commodities and the infrastructure should operate seamlessly as technology advances. The Department must be able to move with technology as increased functionality and security increases.
2. Open Architecture/Standards Based: The smart card solution should embrace government and industry standards. The solution will include both the mandatory set of rules governing information systems documented in the Joint Technical Architecture as well as established and emerging industry standards that are commercially applied, such as ISO and ANSI standards. This will negate the possibility of committing the DoD to proprietary closed solutions, which poses

many less desirable alternatives, and allows migration towards an open platform. An open architecture is one that is supported by the JTA, multiple vendors, multiple industry standards, and readily used programming language(s) (i.e. visual basic, C++, Java, HTML, XML & others.

3. Non-Obsolescence: As technology advances, the architecture should avoid making unexpected and unapproved obsolescence of previously issued CACs. The CAC architecture should allow advancements in technology on a migration path without re-issuance and/or major changes to end-user business practices.
4. Cost Effective: The chosen technology should provide the least total ownership cost to the government.
5. Best Practices: The chosen technology should follow industry/commercial best practices. The government should gain from technology advancements fueled by the private sector. It should not field a “military specific” solution.
6. Post Issuance Functionality: The CAC Platform must be flexible. Components require the ability to add or delete functionality after issuance. In examining the current logistics of the DEERS/RAPIDS issuance and timelines, functionality for the Component specific area of the CAC potentially will not be fully studied, requirements delineated, and software developed by the initial CAC rollout. Re-issuing cards to provide additional functionality is not an acceptable solution. As a result, the ability to add or delete functionality from the CAC platform is the only current way to accommodate both Component and DoD functional requirements

These goals were the yardstick for selecting the fundamental architecture of the CAC, and act as the foundation to the CAC architectural roadmap.

Recommendation C

Based on the goals outlined above and the realities of the marketplace, the CAT WG recommends the approval of the below requirements. All Release 1.0 CAC platforms shall be fully interoperable with:

?? **Java Card 2.1 Compliance:**

1. An interpretive language platform, it provides the foundation for which objects (or code) can plug into the card platform without being predefined or predetermined space. This supports the Component’s need to **add functionality to the card after issuance.**
2. These types of platforms contain a virtual machine that is the interpretive layer that abstracts on-card code development from potential proprietary constraints of the underlying operating system. As a result, a more open platform can be achieved and **interoperability promoted.**

3. This choice **follows commercial best practices**. In a time of volatile changes, it is best to follow large entities deploying similar technologies. This is the same direction used by American Express Blue Card, the Swiss National Bank, and the Spanish National ID Card project.

? ? **Global Platform** (also known as Visa Open Platform):

1. This standard **provides additional security** mechanisms to manage interpretive platforms' usage of abstracted on-card objects (or code).
2. It uses cryptography to **perform highly sophisticated authentication**. Component specific applications will have a cryptographic footprint, which corresponds, to the appropriate interpretive card platform slot. Whenever, applications are being loaded into the interpretive platform an authentication takes place. If the correct footprint is not present, the card platform will reject the application. This prevents rogue, malicious, or unauthorized objects from being loaded into the platform.
3. The same loading feature allows the applications to float to where space is available on the card. By not tying an application to a specific location on the card, it supports the **non-obsolescence of previously issued cards**.
4. Global platform is standards-based and non-proprietary. The overseeing organization, in which many vendors participate, maintains the specification and acts as a de-facto industry standard for highly secure financial transactions.

? ? **Modern Cryptography Capable of On-card Key Generation:**

1. CAC Release 1.0 must employ a cryptographic co-processor capable of generating key pairs on the card using approved cryptographic algorithms.
2. This feature allows the Department to utilize commercially available cards and processes to make the CAC card and associated cryptographic functions secure.

? ? **Large Commercially Available Application Space**

1. The initial CAC will contain a minimum of 32k bytes. As more capacity cards become commercially available, space availability will change to meet emerging requirements.
2. Chip application space will be reserved for three critical functional areas: PKI; identification; and Component specific requirements.

Key Area #4: Identified Open Items

While reviewing aspects of CAC Release 1.0, the CAT WG uncovered several open items. These items either could not be resolved in the working group or fell outside the bounds of the group's charter. For the success of CAC Release 1.0, it is imperative that these open items are resolved.

Recommendation D

The CAT WG recommends the designed body resolve the below open items.

| Open Items | Resolution Body |
|---|-------------------------------|
| <p>1. <u>Smart Card Reader Specification:</u> Part of the overall CAC architecture is the smart card reader. A point paper, entitled "Smart Card Reader Interoperability: Operation in DoD PKI Class 3 and Target Class 4 Architecture dv 0.7." was distributed by Target Token Work Group. It seems to adequately answer questions about reader and reader specification. This document should be approved.</p> | SCSCG |
| <p>2. <u>Inclusion of Scratch Pad:</u> The CAT WG has discussed creating a few blank data element fields for temporary data storage, which would result in a "scratch pad" area. Discussions within the CAT WG were not completed.</p> | CAT WG |
| <p>3. <u>Security Access Requirement:</u> The SEIWG can be implemented on several different media (magnetic stripe, barcode, or chip). Existing smart card initiatives like CINCPAC Oahu utilize both chip and magnetic stripe. Discussion should take place on which area (s) of the card must support the SEWIG standard.</p> | SCSCG |
| <p>4. <u>Use of On Card Key Generation:</u> The CAT WG recommends a CAC platform that is capable of performing on card key generation for DoD PKI identity and/or e-mail identity credentials. A decision should be made on whether to use this ability or not.</p> | SCSCG |
| <p>5. <u>Continuity of DoD PKI Documentation:</u> The DoD Target PKI User requirements document (29 February 2000) indicates that PKI subscribers shall have the capability "to be able to use public and private key pairs from any DoD workstation regardless of operating system and platform." Is this policy or will this be policy? The marriage of smart card and PKI has constituted relevant policies to be reflected in both areas.</p> | SCSCG delegate to DoD PKI PMO |

| | |
|--|--|
| <p>6. <u>Core Data Access Privileges:</u> Although the CAT WG has identified core data elements, the business rules associated with access and read/write privileges have not been discussed. A body needs to examine and recommend business rules for this area of the CAC.</p> | <p>SCSCG delegate to a work group</p> |
| <p>7. Use of other types of technology There has been a lot of discussion o the use of other types of technology like contact less, MIFARE, or proximity. A body needs to examine this areas and potential requirements.</p> | <p>SCSCG delegate to Security work group</p> |

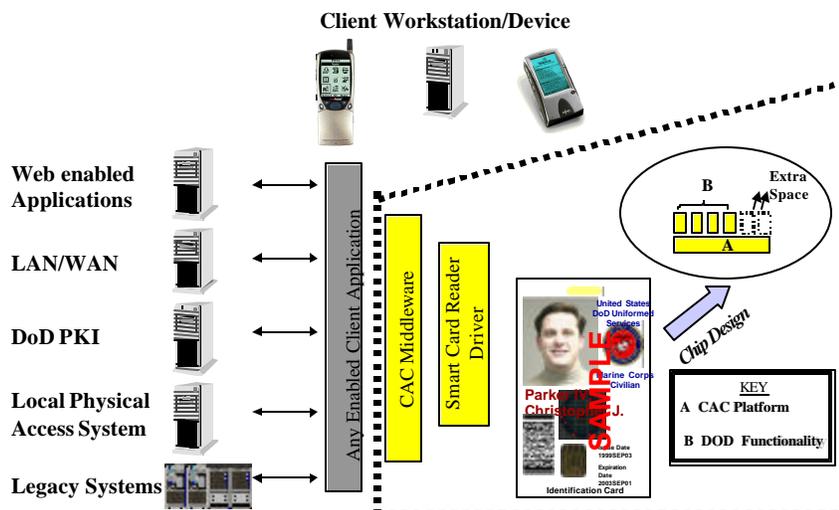
1 Introduction

The Smart Card Senior Coordinating Group (SCSCG) created the Chip Allocation Technical Workgroup (CAT WG), as a cross Service and Component body, to examine and delineate Department of Defense chip-based requirements for the Common Access Card (CAC), or otherwise known as CAC Release 1.0 ICC Requirements.

This document outlines, in detail, the roadmap taken by the CAT WG in identifying requirements and eventually recommendations. The CAT WG defines the CAC ICC requirements and functionality in the following manner:

- A. **CAC Platform** is the smart card platform upon which all CAC functionality shall reside (Detailed in Section 4.0).
- B. **DoD Functionality**: is the set of chip-based functionality that shall reside on every CAC. The working group shall identify mission essential card-based applications to include, but not be limited to, Public Key Infrastructure (PKI), physical access, and data elements that include DoD identification requirements (Detailed in Section 2.0).
- C. **CAC Middleware** is the CAC specific client software (i.e. middleware) required to allow core chip-based CAC functionality to operate minimally in DII COE platforms. It is expected that in the near-term all of the core chip-based CAC functionality shall require client middleware to operate (Detailed in *Appendix 8*).

CAC Release 1.0 Architecture



1.1 **Reference Documentation**

In examining the requirements for the CAC Release 1.0, the CAT WG used several documents as reference in our discussions and recommendations. All relevant references are located in *Appendix 1*.

2 **DoD Functionality**

2.1 **Definition**

DoD Functionality is the set of chip-based functionality that shall reside on every CAC. The working group shall identify mission essential card-based applications to include, but not be limited to, Public Key Infrastructure (PKI), Physical Access and Data Elements.

2.1.1 Data Element Requirements

As a baseline for discussions, the CAT WG asked each Component to examine data elements used in existing smart card initiatives. This exercise was used to determine which elements should be considered requirements for the DoD portion of the CAC to include those elements to fulfill the DoD identification requirements. The work group focused on those elements that members would consider common across all Components. The members concluded that those data requirements from a DoD perspective needed to be minimal and, to the extent possible, static in nature. In crafting its data recommendation, the CAT WG used architectural methods outlined in “Smart Cards: Designing a Hybrid Card Architecture from a Web-centric and Card-centric Perspective” document distributed to the group (See *Appendix 6*.)

Minimal, static data elements were chosen because those elements were the least volatile. As a result, synchronization issues with the card’s portable database could be avoided. For detail definitions of terms, please review *Appendix 5*. The recommended data requirements are:

- ?? First Name
- ?? Middle Name
- ?? Last Name
- ?? Suffix
- ?? Social Security Number
- ?? Person Designator
- ?? DoD EDI Person Identifier
- ?? Personnel Service Code (or Branch)
- ?? Rank
- ?? Date of Birth
- ?? Gender
- ?? Pay Category (or Pay Plan)

- ?? Pay Plan
- ?? Personnel Category (or Duty Status)
- ?? US Government Agency/Sub Agency Code
- ?? Non-US Government Agency Code
- ?? DoD Contractor Code
- ?? Date Demographic Data Loaded
- ?? Date Demographic Data Expires
- ?? Card Issue Date
- ?? Card Expiration Date
- ?? Card Security Code
- ?? Exchange Status Code
- ?? Commissary Status Code
- ?? Morale, Welfare, & Recreation Status Code
- ?? Personnel Entitlement Condition Code
- ?? Civil Health Care Entitlement Code
- ?? Direct Care Type Code
- ?? Medical Benefit End Date
- ?? Non-Medical Benefit End Date
- ?? Meal Entitlement Code

The CAT WG recommends allocating a maximum of **2.4** Kilobytes (including file overhead) of space to fulfill the above requirement.

2.1.2 DoD PKI Requirements

The DoD's Public Key Infrastructure (PKI) is based on several guiding directives, documents, and functional requirements. The DoD PKI requirements below are relevant solely to the end-user token, and correlate to terminology describing the architectural requirements of the overall system and policy. The CAC Release 1.0 will adhere to the DoD PKI requirements associated with the Class 3 architecture.

Class 3 Requirements:

| Item (RSA 1024 Key Length) | Maximum Space |
|-----------------------------------|----------------------|
| DoD PKI Identity Certificate | 2.0 Kilobytes |
| E-mail Encryption Certificate | 2.0 Kilobytes |
| E-mail Identity Certificate | 2.0 Kilobytes |
| DoD PKI Signature Private | 768 Bytes |
| E-mail Encryption Private | 768 Bytes |
| E-mail Signature Private | 768 Bytes |
| TOTAL | 8.3 Kilobytes |

In the 10 November 1999 DEPSECDEF memo, there are discussions about providing logical access. The CAT WG focused on the DoD PKI recommendations fulfilling this requirements; however, we recognize that there are several other methods in which to implement or provide logical access. All other types of implementations should fall within the Component specific area of the CAC.

2.1.3 Physical Access Requirements

Requirements for physical access shall be minimally accommodated by the use of the DoD SEIWG standard. The SEIWG can be implemented on several different media residing on the card (e.g. magnetic stripe, barcode, or chip). A recommendation on the type of implementation for the CAC remains open. The SCSCG shall be responsible for directing which media(s) Release 1.0 must support.

2.2 **Recommendation**

Based on the requirements above, the CAT WG recommends approval of the following space allocations:

| CAC Functionality | Space | Overhead | Total |
|---|---------------|-----------------|----------------|
| DoD: Data Elements (Maximum Space) | 0.2 Kilobytes | 2.2 Kilobytes | 2.4 Kilobytes |
| DoD: PKI (Maximum Space) | 8.3 Kilobytes | 2.0 Kilobytes | 10.3 Kilobytes |
| Enhancement to CAC Platform (Maximum Space) | 10 Kilobytes | N/A | 10.0 Kilobytes |
| Component Specific Area (Minimum Space) | 7 Kilobytes | N/A | 7 Kilobytes |
| Total | 25.5 | 4.2 | **29.7 |

**Note: This leaves an additional 1.9 kilobytes of unused space that could be allocated to the Component Specific Area of the CAC.

2.3 **DoD Functionality Concept of Operation (CONOPS)**

This section will outline the anticipated concept of operations for each area of the DoD functionality.

2.3.1 Issuance Process

The CAC specified in this document is intended to support Identity, e-mail identity, and e-mail encryption keys/certificates for cryptographic functions. Three (3) sets of asymmetric key pairs and certificates shall be used.

The Identity credentials shall be used for secure authentication. The key pairs may be generated on the card (A policy decision needs to be made on whether mandate the use of on-card key generations. CAT WG recommends the SCSCG provide this guidance). The public key shall be securely transmitted to the Certificate Authority (CA). The CA shall create a X.509 v3 digital certificate using the public key and sign the certificate with its own private key. The X.509 v3 certificate shall then be returned to the card for storage.

The E-mail Identity credentials shall be used for e-mail digital signature functions. These key pairs can be generated on the card (A policy decision needs to be made on whether mandate the use of on-card key generations. CAT WG recommends the SCSCG provide this guidance). The public key shall be securely transmitted to the Certificate Authority (CA). The CA shall create a X.509 v3 digital certificate using the public key and sign the certificate with its own private key. The X.509 v3 certificate shall then be returned to the card for storage.

The E-mail Encryption credentials will be used for encryption functions. These key pairs will be generated in the client workstation's software cryptographic module. Depending of the process, the private key is either sent to the card or stored within the browser in which it shall be exported to the card. The private and public keys shall be securely transmitted to the Certificate Authority (CA). The CA shall escrow the e-mail private key. Once the CA has securely received the both the private and public keys, it will send a signed X.509 v3 digital certificate and associated keys to the card for secure storage.

2.3.2 Data Element Use Process

Data residing on the CAC shall be used to provide information to those applications that contain the necessary Application Programming Interface (API) and authorization to read the information on the card. All of the business logic and most of the processing shall be contained in the application. These applications shall query the card for certain data elements that are required by the application to perform certain business or operational processes, as delineated by Components or functional owners of the application.

2.3.3 PKI Use Process

The CAC will be used in client workstations to perform several PKI-based functions. The functions are:

1. Digital signature
2. Secure authentication
3. E-mail encryption (does not include symmetric or full message encryption)

These PKI functions shall be provided by client workstation applications. For the purpose of the CAC, PKI-enabled applications shall be able to communicate via

standards-based cryptographic middleware (e.g. PKCS #11 and/or Microsoft's Cryptographic Service Provider).

3 Backward Compatibility

3.1.1 Existing Smart Card Initiatives to CAC Release 1.0

The CAT WG recommends the following policy actions:

The CAC shall be backward compatible with existing smart card initiatives such that either the card contains (in the combined DoD and Component Specific areas) the same amount of data as it currently carries or existing applications will be modified to provide the same business functionality. The CAT WG recommends a card architecture that will provide either of the above; however, it is the responsibility of the Components to achieve.

Further clarification and guidance of the Backward Compatibility policy was provided as part of the Smart Card Senior Coordinating Group (SCSCG) Meeting on 9 January 2001. These clarifications include:

- a) "Joint" removed from application title. The names of the Backward Compatible applications have been changed to remove the word "Joint." Although these applications were developed in Oahu with the participation of PACOM and the four Services and were used by these organizations in Oahu, they were never formally coordinated with all CINCs and the Service headquarters. No agreement could be reached on requirements when vetted during Working Group meetings. Therefore, these applications cannot be considered Joint in accordance with the CAC Configuration Management Plan.
- b) Life Cycle Managers (LCMs) identified. The U.S. Air Force will serve as the LCM for the Supply Asset Tracking System (SATS) application. The Department of the Navy Smart Card Office (DONSCO) will serve as the LCM for the Manifest/Tracking, Food Service, Warrior Readiness, and Weapons Issuance applications. This is in compliance with the Common Access Card (CAC) Configuration Management Plan (CMP) for Component-Specific applications.
- c) Loading and Use of applications are optional. Loading of these applications and their associated data elements is completely optional and at the discretion of the cognizant CINC/Service/Agency (C/S/A). The intent is for the CAC to seamlessly interface to these legacy smart card applications.
- d) Applications' life cycle is limited to end of FY 02. The life cycle of these applications will be through FY 02, allowing time for the Joint Staff Functional Community Panel (JS FCP) (working closely with the Defense Logistics Agency (DLA)) to consider them for Department-wide

applications and/or current users to fund continued LCM in their Program Objective Memorandum (POM) as Component-specific applications. The funding provided by the DONSCO will provide for changes required to allow the existing applications to interface properly with the CAC; any additional functional changes will need to be funded by the requesting organization.

The above policy decisions, approved at the 9 January 2001 SCSCG Meeting, are fully compliant with the Configuration Management Plan (CMP) for Component-specific applications. The decision to use these applications rests completely with the C/S/A. It ensures that the current users of these applications have the capability to continue to use the applications with the CAC. It provides sufficient time for the C/S/A to fund continued support of these applications, if desired, and the Joint Staff to develop proposed joint applications in accordance with the CMP.

3.1.2 Beyond CAC Release 1.0

The CAT WG recommends the following policy actions:

Subsequent releases of the CAC shall be cognizant of prior requirements. Before each subsequent release, the Smart Card Senior Coordinating Group (SCSCG) will review recommendations in accordance with existing features or functionality. If there are modifications or deletions of functionality, the changes will get approval from the Smart Card Senior Coordination Group. In addition, if changes are made to the card architecture, the Components must be advised and given ample time to adjust Component specific code or file structures to accommodate those changes. Specifics of this process are addressed in the Smart Card Configuration Management Plan (CMP). Refer to the CMP for the Common Access Card (Final Version 1.0), dated 17 November 2000.

4 Card Architecture and Platform

4.1 Definition

The Card Architecture and Platform include the CAC Release 1.0 card platform and appropriate middleware.

4.1.1 Basic Assumptions

All members of the CAT WG agreed to the below assumptions in evaluating CAC card architecture and platform options.

1. CAC Release 1.0 shall provide a platform that contains space for DoD-based functionality (i.e. functionality that All active duty, selected reserve, civilians, and seated contractors will receive) and Component specific functionality.
2. The Components shall be able to add/delete Component specific functionality after card issuance.

4.2 CAC Release 1.0 ICC Requirements

| | Option 1 | Option 2 | Option 3 | Option 4 |
|-------------------------------|---|---|---|---|
| Card Operating System | Java Card 2.1 plus Proprietary Operating System | Windows Powered Smart Card OS | MULTOS | Other Proprietary Operating Systems |
| Standards: | ISO 7816, 1-4 EMV Java Card 2.1 Open Platform 2.0.1 or higher | ISO 7816, 1-7 EMV Open Platform 2.0.1 or higher | ISO 7816, 1-7 EMV | ISO 7816, 1-7 EMV |
| Micro-controller/Processor: | Minimum: 32K micro-controller (with 32K of available EEPROM) Minimum: 8-bit processor Must contain a cryptographic co-processor | Minimum: 32K micro-controller (with 32K of available EEPROM) Minimum: 8-bit processor Must contain cryptographic co-processor | Minimum: 32K micro-controller (with 32K of available EEPROM) Minimum: 8-bit processor Must contain cryptographic co-processor | Minimum: 32K micro-controller (with 32K of available EEPROM) Minimum: 8-bit processor Must contain cryptographic co-processor |
| Card Functionality (Available | ?? DoD Provided | ?? DoD Provided | ?? DoD Delineated | ?? DoD |

| | Option 1 | Option 2 | Option 3 | Option 4 |
|--|--|--|---|--|
| EEPROM will contain): | ?? Data Applet DoD Provided PKI Applet capable of generating and storing 3 Digital Certificates and associated key pairs in accordance with CONOPS Section 3.3.1 & 3.3.3 | ?? Data FAT File DoD Provided PKI FAT File capable of generating and storing 3 Digital Certificates and associated key pairs in accordance with CONOPS Section 3.3.1 & 3.3.3 | ?? Data File Structure DoD Delineated PKI file structure capable of generating and storing 3 Digital Certificates and associated key pairs in accordance with CONOPS Section 3.3.1 & 3.3.3. | ?? Delineated Data File Structure DoD Delineated PKI file structure capable of generating and storing 3 Digital Certificates and associated key pairs in accordance with CONOPS Section 3.3.1 & 3.3.3. |
| Cryptography: Encryption Algorithms: Digest Algorithms: Key Exchange Algorithms: Signature Algorithms: | DES Triple DES Skipjack (Optional) SHA-1 MD5 (Optional) RSA RSA, PKCS#1 Format <i>⚡</i> Minimum support 1024 bit key length <i>⚡</i> Hardware Random Number Generation | DES Triple DES Skipjack (Optional) SHA-1 MD5 (Optional) RSA RSA, PKCS#1 Format <i>⚡</i> Minimum support 1024 bit key length <i>⚡</i> Hardware Random Number Generation | DES Triple DES Skipjack (Optional) SHA-1 MD5 (Optional) RSA RSA, PKCS #1 Format <i>⚡</i> Minimum support 1024 bit key length <i>⚡</i> Hardware Random Number Generation | DES Triple DES Skipjack (Optional) SHA-1 MD5 (Optional) RSA RSA, PKCS#1 Format <i>⚡</i> Minimum support 1024 bit key length <i>⚡</i> Hardware Random Number Generation |
| On Card Key Generation Performance Criteria: | Maximum Average 180 seconds | Maximum Average 180 seconds | Maximum Average 180 seconds | Maximum Average 180 seconds |
| Security: | <i>⚡</i> Minimum: FIPS 140-1, Level 1 Certification for entire card platform <i>⚡</i> Provide | <i>⚡</i> Minimum: FIPS 140-1, Level 1 Certified for entire card platform <i>⚡</i> Provide | <i>⚡</i> Minimum: FIPS 140-1, Level 1 Certified for entire card platform <i>⚡</i> Provide | <i>⚡</i> Minimum: FIPS 140-1, Level 1 Certified for entire card platform <i>⚡</i> Provide |

| | Option 1 | Option 2 | Option 3 | Option 4 |
|--|---|---|---|---|
| | information on protection techniques used to combat Differential Power Analysis and Simple Power Analysis attacks | information on protection techniques used to combat Differential Power Analysis and Simple Power Analysis attacks | information on protection techniques used to combat Differential Power Analysis and Simple Power Analysis attacks | information on protection techniques used to combat Differential Power Analysis and Simple Power Analysis attacks |

4.3 GOALS in Evaluating Card Architecture

The working group established the following goals in evaluating card architecture:

1. **Interoperability.** Smart cards should be treated as commodities and the infrastructure should operate seamlessly as technology advances. This means that the Department can move with technology as it provides increased functionality and increased security.
2. **Open Architecture/Standards Based.** The smart card solution should embrace government and industry standards. The solution will include both the mandatory set of rules governing information systems documented in the Joint Technical Architecture as well as established and emerging industry standards that are commercially applied, such as ISO and ANSI standards. This will negate the possibility of committing the DoD to proprietary closed solutions, which poses many less desirable alternatives, and allows migration towards an open platform. An open architecture is one that is supported by the JTA, multiple vendors, multiple industry standards, and readily used programming language(s) (i.e. visual basic, C++, Java, HTML, XML & others
3. **Non-Obsolescence.** As technology advances, the architecture should not make previously issued CACs obsolete. The CAC architecture should allow it to advance with new technology on a migration path without having to re-issue cards and change end-user business practices.
4. **Cost Effective.** The chosen technology should be the least total ownership cost to the government.
5. **Best Practices.** The chosen technology should follow industry/commercial best practices. The government should gain from technology advancements fueled by the private sector. It should not field a "military specific" solution
6. **Post Issuance Functionality.** The CAC Platform must be flexible. Components require the ability to add or delete functionality after issuance. In examining the current logistics of the DEERS/RAPIDS issuance and timelines, functionality for the Component specific area of the CAC potentially will not be fully studied,

requirements delineated, and software developed anytime close to the initial CAC rollout. Re-issuing cards to provide additional functionality is not an acceptable solution. As a result, the ability to add or delete functionality from the CAC platform is the only current way to accommodate both Component and DoD functional requirements

These goals were the yardstick for selecting the fundamental architecture of the CAC and laying down the roadmap.

4.4 ***Smart Card Technology Perspectives***

As a basis for understanding how the smart card technology has evolved over time, the following historical perspectives are provided.

Card Operating System (COS) Perspectives

Since the smart card (also known as chip card) was invented by a Frenchman in 1974 and until mid-1990's, the COS has been traditionally written by the card manufacturer or licensed from a third party by the card manufacturer. Normally, the COS was masked (burned) into the read-only-memory (ROM) of the chip at the time chips were manufactured by the chip manufacturer.

In the late 1980's, erasable and reusable user memory called EEPROM was incorporated into the chip allowing the COS and user data structures to share the same EEPROM space. The card manufacturers often use the EEPROM space for the COS as a temporary code space while the COS is being debugged to minimize the cost and time delay associated with frequent masking in ROM space.

During the mid to late 1990's, the smart card has emerged and is touted as the enabling technology for secure access and as a viable multi-application platform. There have been two industry consortiums that have been instrumental in the smart card becoming a multi-application platform. One is the Java™ Card Consortium lead by Sun Microsystems and the other is Open Card Consortium lead by Visa International.

With the recent effort made in the Java™ Card 2.1 Application Programming Interface (API) Specification, the smart card manufacturers can produce smart card platforms where card applications are independent of the smart card platform as long as the COS is compliant to the Java™ Card API.

With the recent effort made in Open Platform Card Specification V2.0, card life cycle definitions such as card application security domain and card application download functions are defined such that card issuers can manage the card application security and card application load and deletion throughout the card life cycle.

Card Reader Perspectives

Traditionally, the smart card suppliers manufacture smart card readers. Most smart card readers are intelligent and contain their own proprietary terminal operating systems that make the readers not interoperable with each other.

In 1996, PC and smart card industry consortium lead by Microsoft developed the PC/SC Interoperability Specification 1.0 that made the smart card readers compliant to the specification independent to smart cards as well as the PC platforms.

PC Smart Card Application Perspectives

In general, to synchronize the card application functions with the PC-based card application functions, there has to be a link between the two applications functions executed in the smart card and the PC.

Traditionally, most of PC-based smart card applications have implemented their own functional APIs to overcome the differences among the COSs functions as well as card cryptographic functions.

The above mentioned PC/SC Interoperability Specification 1.0 defines the Service Provider (middleware) concept where generic card cryptographic as well as non-cryptographic service functions can be implemented as service provider modules linking the PC-based application functions to the card-based application functions. These generic Service Provider modules will make the PC-based smart card-aware applications independent of the smart card platforms and readers.

4.5 Evaluation

The purpose of this section is to provide insight into the options available and to lay the foundation for a recommended CAC Card Architecture and Platform.

4.5.1 Interoperability

In the previous sections, the DoD functions were identified and platform options defined. The CAC requires a multi-application smart card environment that involves application interoperability with card platforms; secures application load; and associated security functions. In this section, a set of criteria shall be specified for discussion of an overall *Interoperability Model*, review of viable options, and selection of a preferred option.

In the context of the CAC, interoperability means that any CAC enabled system must be able to establish communications between any CAC and CAC reader at the physical and link layers. In addition, all CAC middleware (card service providers) must implement a common set of basic services and a common interface to those services.

In the subsections that follow, the CAC Interoperability requirements will be described in accordance with a selected set of international standards and specifications.

For further technical explanations regarding Interoperability, refer to *Appendix 7 – CAC Interoperability Findings* and *Appendix 8 – CAC Middleware Requirements*.

The Options to consider must be viewed in the context of the two major categories: 1) Card Application Interoperability, and 2) Card Service Provider (Middleware) Interoperability.

4.5.1.1 Card Application Interoperability

Card Application Interoperability is the ability of a card platform to provide card application (code) commonality. This area holds true for both cryptographic and non-cryptographic features of the card.

Below is a comparison of the potential CAC requirement options (See Section 4.2) and how those options handle card application interoperability.

Option 1: Open Platform¹ coupled with Sun Microsystems' Java™ Card

Java allows platform independent and secure system development with ease of system maintenance. Combined together with Java Card specification, Open Platform allows application independent platform, firewall detection between applications, dynamic loading of applications and use of industry standard, Java language and Virtual Machine.

Open Platform Card Specification is designed to tightly integrate with the Java Card specification and provide a thorough implementation guide for manufacturers to ensure complete, consistent, secure and interoperable smart card products.

Option 2: Open Platform² coupled with Microsoft's Windows for Smart Card

As of the drafting date of this document, there is no commercially available Windows powered smart card product from Microsoft. In late 1999, Microsoft made an adjustment to its scheduled releases of Windows for Smart Card product to respond to the demand from the industry. But, Microsoft has not

¹ VISA Open Platform Card Specification, Version 2.0.1; and Terminal Specification, Version 1.5

² VISA Open Platform Card Specification, Version 2.0.1; and Terminal Specification, Version 1.5

made any definite commitment for the release of Open Platform compliant Windows for Smart Card product.

Option 3: MULTi-application Operating System MULTOS:

MULTOS is a product offering from the MAOSCO Consortium. MAOSCO Consortium members, as a group, are responsible for the ongoing maintenance and development of the MULTOS specification. The core of the MAOSCO Consortium is comprised of 14 world leading companies from the smart card industry that include American Express, MasterCard, Fujitsu Group, Hitachi, Motorola, G&D and Siemens.

Key elements promoted by the MAOSCO Consortium are a security architecture; co-residence of multiple, inter-operable, platform independent applications; and dynamic remote loading and deletion of applications over the lifetime of a card.

Option 4: Other Proprietary Operating Systems

Currently, there are no commercially available proprietary operating systems that are capable of providing card applications interoperability in a standards-based manner.

4.5.1.2 Card Service Provider (Middleware) Interoperability

Card Service Provider (Middleware) Interoperability is the ability of smart card-aware applications, running in client workstations, to be transparent to the smart cards and readers. For most smart card architecture, there is a need for middleware to get smart card-aware applications to work.

In this category, there are viable option for Windows-based environment and an non-Windows-based environment. For cryptographic functions, the card service provider shall minimally communicate via Public Key Cryptographic Standard #11 (PKCS#11) and/or Microsoft's Cryptographic Service Provider (MS CSP)

PC/SC Working Group for Windows operating environment

PC/SC Working Group was formed in May 1996 (by Microsoft, Bull, HP, Schlumberger and Siemens,) to address the need for PC to smart card interoperability. The objectives of the Group was to define (1) comprehensive standards for smart card readers and cryptographic services, (2) application and vendor neutral platform and (3) support industry initiative such ISO 7816 and Europay MasterCard Visa (EMV). PC/SC Interoperability Specification is the defacto industry standard for client workstation to smart card reader interoperability. In addition, a majority of smart card middleware has been implemented using PC/SC as a guideline.

Open Card Consortium for Non-Windows operating environment

Open Card Consortium (OCC) was formed in April 1996 as an industry work group to address the interoperability of smart cards and computing devices. Open Card Framework (OCF) developed by OCC is an open specification for smart card access in smart card interface devices. OCF provides architecture and a set of APIs that enable application developers and service providers to build and deploy smart card-based solutions in any Open Card-compliant environment. OCF has been developed for harmonization and extensibility with PC/SC, Java Card and Open Platform specifications. While PC/SC operates within the Windows-based platform, OCC operates with non-Windows platform using Java programming language and environment.

A partial list of founding members of PC/SC Interoperability Working Group includes Sun Microsystems, IBM, Visa International, Gemplus, Schlumberger, Bull and Netscape.

4.5.1.3 Analysis and Rationale for Selected Interoperability Model Option

The potential approaches for an interoperability model vary. First, PC/SC Working Group lead by Microsoft has laid a strong foundation among card, card reader devices and PC for physical, electrical and communication channel interoperability. Its specification is based on International Standards Organization (ISO) 7816 Part 1, 2 and 3 standards. Its specification is well accepted among Windows-based platform, smart card and smart card reader manufacturers. In fact, Microsoft operates a PC/SC certification laboratory for the smart card reader manufacturers. PC/SC Interoperability Specification is the defacto industry standard for PC to smart card interoperability. Open Card Framework is comparable to PC/SC Interoperability Specification, but for the non-Windows operating environment.

Second, Mondex International owned by MasterCard created MULTOS technology. MAOSCO Consortium owns the intellectual property of the MULTOS operating system and licenses the right to produce MULTOS Cards to smart card manufacturers. Each smart card manufacturer does not add any value to the licensed operating system. MULTOS was developed using its proprietary language called MEL, and it has not attracted the worldwide array of developers as realized by Java world. Since it was originally created by a team from financial sector, MULTOS had a better defined card life cycle management scheme than Java Card. But, with the development of Open Platform Card Specification by Visa International, the advantage of implementing MULTOS has evaporated.

Third, Open Platform Card Specification by Visa International coupled with Sun Microsystems' Java™ Card Specifications has provided the smart card industry

a stronger choice for card application independent multi-application smart card platform with multiple sources of card manufacturers. Almost 100% of card manufacturers have already licensed Java™ Card VM and API technology which allows each card manufacturers to add value by implementing the licensed technology on top of their proprietary smart card platforms working with multiple IC chip manufacturers.

A Table summarizing the Interoperability Approaches and their Relative Strength versus the Criteria are show below.

| Interoperability Approaches | Card Application Interoperability | | | | Middleware Interoperability | |
|-----------------------------|-----------------------------------|---|--------|----------------------|-----------------------------|---------------------|
| | Open Platform With Java Card | Open Platform with Windows for Smart Card | MULTOS | Other Proprietary OS | PC/SC | Open Card Framework |
| Adoption | HIGH | LOW | MEDIUM | LOW | HIGH | MEDIUM |
| Maturity | HIGH | LOW | HIGH | LOW | HIGH | HIGH |
| Availability | HIGH | LOW | MEDIUM | LOW | HIGH | HIGH |

Based upon the above, the CAT WG recommends adoption of Open Platform with Java for Card Application Interoperability. As to middleware, there is no conflict between PC/SC and Open Card Framework. Both solutions apply – one for Windows-based operating environment and one for non-Windows based operating environment.

4.5.2 Open Architecture/Standards Based

In examining the requirements for the CAC Release 1.0, the CAT WG used several documents as reference in our discussions and recommendations. All relevant standards references are contained in *Appendix 4*.

4.5.3 Non-Obsolescence

The goal for all smart cards issued is that they should be upgradeable without obsolescing previously issued cards. However, existing applications, cards and readers are not compatible with the planned multi-application CAC infrastructure. Current smart cards are based on proprietary card operating systems, which do not have updateable code area/space, and for which there are no card-based applications. In future rollouts, backward compatibility is achievable. Possible options for avoiding or preventing obsolescence include updateable security domains for each application, which includes certificate update or replacement.

4.5.4 Best Practices

The DoD and the U.S. Federal Government are not alone in trying to achieve ubiquity within the smart card industry. Joining other “best of practice” industry initiatives to achieve this result is an intentional element for DoD’s acquisition strategy. A well-developed strategy shall provide increased sources of interoperable components, better competitive pricing and more easily achieved system implementations and maintenance.

Existing best practices include the European Digital Signature initiatives that have begun to pervade PKI/IETF X509 digital certificates into smart card hardware tokens. These include the Spanish Mint (FMNT Ceres Project), the Finnish Citizen services Electronic ID card (FIN EID), and others in private industry such as the US Financial Institution’s (FI’s) Identrus, and American Express “*Blue*” card projects.

DoD’s acquisition plan shall support an evolving technology paradigm. As the cards become more capable and secure, the acquisition road map shall pace COTS best practices moving forward

The leader in deploying smart cards in the private sector is the Financial Industry with security being their top concern. The infrastructure suppliers are tracking very closely to the stringent security needs of the Financial Industry. As such, DoD can be the beneficiary of the evolving emphasis on security and open platforms that enable interoperability.

4.5.5 Post Issuance Functionality

The CAC Platform must be flexible. Components require the ability to add or delete functionality after issuance. In examining the current logistics of the DEERS/RAPIDS issuance and timelines, functionality for the Component specific area of the CAC potentially will not be fully studied, requirements delineated, and software developed before the initial CAC rollout. Re-issuing card to provide additional functionality is considered an unacceptable solution. As a result, the ability to add or delete functionality from the CAC platform is the only current way to accommodate both Component and DoD functional requirements.

Critical parts of the CAC operational requirement that have not yet been clearly defined are: 1) standardized CAC application development framework; 2) methods and means for secure delivery of CAC applications from the application providers to the CAC platform; and 3) usage of a common application loader.

4.6 Other Considerations

Other considerations that surfaced as part of the evaluation process include the following items.

1. Plan a migration to worldwide Industry standards:
While we acknowledge the importance of FIPS, the Department of Defense should promote the convergence to worldwide industry standards like Common Criteria. This could shorten the time to market for certified products and potentially provide the DoD with the cost saving from using worldwide standards and evaluation criterias.
2. Availability of smart cards with larger ROM sizes:
Based on the ICC manufacturers, chips with larger ROM size (64 KB or greater) will be available late in 1st quarter FY01. This added capacity will allow for more suppliers to free up more user memory space for applications. In addition, more potential suppliers will be available from which to choose.
3. GSA Common Access ID Card procurement:
DoD acknowledges the interoperability requirement that is a major part of the Federal government smart card procurement. GSA's plan is to prepare and establish a "*Government Smart Card Technical Interoperability Guidelines*" as part of the first milestone after contract award. DoD will participate in the process. It is anticipated that the process will take 45 days to complete. It is not certain how long it may take the smart card suppliers to comply with the adopted Guidelines. DoD is aware that NIST will require conformance testing as well. DoD believes that the outcome of the effort undertaken by GSA will be mutually beneficial in terms of validation of the options selected and decisions made.

4.7 Recommendations

Once the requirements were examined and completed, the CAT WG crafted a group of potential CAC Release 1.0 ICC Requirements that met varies levels of the Components requirements (Section 4.2). The CAT WG met on numerous occasions with representatives from Industry. Open and informative discussions were conducted with Industry on current and future trends, standards, potential costs, and availability of several different technologies.

These discussions, Service/Component requirements, costs, and availability of technology acted as four pillars in comparing the group of potential CAC Release 1.0 ICC Requirements. Ultimately, these four pillars helped the group in selecting a single requirement that best met all of these criteria. The CAT WG recommends approval of the below table as the Department of Defense ICC requirements for CAC Release 1.0. All Release 1.0 CAC shall be fully interoperable with:

| | CAC Release 1.0 ICC Recommendation |
|---|---|
| Card Operating System | Java Card 2.1 plus Proprietary Operating System |
| Standards: | ISO 7816, 1-7 EMV Java Card 2.1 Certified Global Platform 1.0 or higher |
| Micro-controller/Processor: | Minimum: 32K micro-controller (with 32K of available EEPROM) Minimum: 8-bit processor Must contain a cryptographic co-processor |
| Card Functionality (Available EEPROM will contain): | ?? DoD Provided Data Applet ?? DoD Provided PKI Applet capable of generating and storing 3 Digital Certificates and associated key pairs in accordance with CONOPS Section 3.3.1 & 3.3.3 |
| Cryptography: Encryption Algorithms: | DES Triple DES Skipjack (Optional) |
| Digest Algorithms: | SHA-1 MD5 (Optional) |
| Key Exchange Algorithms: | RSA |
| Signature Algorithms: | RSA, PKCS#1 Format ?? Minimum support 1024 bit key length ?? Hardware Random Number Generation |
| On Card Key Generation Performance Criteria: | Maximum Average 180 seconds |
| Security: | ?? Minimum: FIPS 140-1, Level 1 Certification for entire card platform ?? Provide information on (both hardware and software) protection techniques used to combat Differential Power Analysis and Simple Power Analysis Attacks |

4.7.1 Open Platform

This specification provides additional security mechanisms to manage card applications. It uses cryptography to perform highly sophisticated authentication. Component specific applications will have a cryptographic footprint that corresponds to the appropriate card application. Whenever card applications are being loaded into the card platform, an authentication takes place. If the correct footprint is not present, the card platform will reject the card application. This prevents rogue, malicious, or unauthorized objects from being loaded into the platform.

The same loading feature allows the card applications to float to where space is available on the card. By not tying a card application to a specific location on the card, it supports the non-obsolescence of previously issued cards.

Open Platform is an industry-based and non-proprietary specification. Global Platform is the overseeing organization in which many suppliers as well as representatives from public and private sectors participate. This organization maintains the specification and acts as a de-facto industry standard organization for highly secure financial transactions.

4.7.2 Java™ 2.1 Smart Card Operating System

As the Java™ language platform, it provides the foundation for which a card application can plug into the card platform without being allocated to a predefined or predetermined space. This supports the Components' needs to add functionality to the card after issuance and non-obsolescence.

The Java™ card platform contains a virtual machine (the interpretive layer) and the Java™ card API that frees card application development from potential proprietary constraints of the underlying operating system provided by each card supplier. As a result, a more open card platform can be achieved and interoperability promoted.

This choice follows commercial best practices. In a time of volatile changes, it is best to follow industry leaders. This is the same direction being used by American Express "*Blue Card*", the Swiss National Bank, and the Spanish National ID Card project.

4.7.3 Modern Cryptography with On-card Key Generation

CAC Release 1.0 shall employ a cryptographic co-processor capable of generating key pairs on the card by using an on-board hardware random number generator and key validation firmware. This feature allows the Department to use commercially available cards and processes to make the CAC and associated cryptographic functions more secure.

4.7.4 Large Commercially Available Application Space

The initial CAC will contain a minimum of 32 KB of EEPROM (user) space and this will increase to meet emerging requirements, as larger cards become commercially available. On card application space will be reserved for three critical functional areas: the PKI; the identification applet; and the Component application requirements.

4.7.5 Security:

CAC Release 1.0 shall be FIPS 140-1, level 1 compliant. Potential vendors shall provide information on the both hardware and software protection techniques used to combat differential power analysis (DPA) and simple power analysis (SPA) attacks.

5 Identified Open Items

While reviewing aspects of CAC Release 1.0, the CAT WG uncovered several open items. These items either could not be resolved in the working group or fell outside the bounds of the group's charter. For the success of CAC Release 1.0, it is imperative that these open items are resolved.

The CAT WG recommends the designed body resolve the below open items.

| Open Items | Resolution Body |
|--|-------------------------------------|
| <p>8. <u>Smart Card Reader Specification:</u> Part of the overall CAC architecture is the smart card reader. A point paper, entitled "Smart Card Reader Interoperability: Operation in DoD PKI Class 3 and Target Class 4 Architecture dv 0.7." was distributed by Target Token Work Group. It seems to adequately answer questions about reader and reader specification. This document should to be approved.</p> | SCSCG |
| <p>9. <u>Inclusion of Scratch Pad:</u> The CAT WG has discussed creating a few blank data element fields for temporary data storage, which would result in a "scratch pad" area. Discussions within the CAT WG were not complete.</p> | CAT WG |
| <p>10. <u>Security Access Requirement:</u> The SEIWG can be implemented on several different media (magnetic stripe, barcode, or chip). Existing smart card initiatives like CINCPAC Oahu utilize both chip and magnetic stripe. Discussion should take place on which area (s) of the card must support the SEWIG standard.</p> | SCSCG |
| <p>11. <u>Use of On Card Key Generation:</u> The CAT WG recommends a CAC platform that is capable of performing on card key generation for DoD PKI identity and/or e-mail identity credentials. A decision should be made on whether to use this ability or not.</p> | SCSCG |
| <p>12. <u>Continuity of DoD PKI Documentation:</u> The DoD Target PKI User requirements document (29 February 2000) indicates that PKI subscribers shall have the capability "to be able to use public and private key pairs from any DoD workstation regardless of operating system and platform." Is this policy or will this be policy? The marriage of smart card and PKI has constituted relevant policies to be reflected in both areas.</p> | SCSCG delegate to DoD PKI PMO |
| <p>13. <u>Core Data Access Privileges:</u> Although the CAT WG has identified core data elements,</p> | SCSCG delegate to a |

| | |
|---|--|
| <p>the business rules associated with access and read/write privileges have not been discussed. A body needs to examine and recommend business rules for this area of the CAC.</p> | <p>work group</p> |
| <p>14. Use of other types of technology There has been considerable discussion of the use of other types of technology like contact-less, MIFARE, or proximity. A body needs to examine these areas and potential requirements.</p> | <p>SCSCG delegate to Security work group</p> |

Appendix 1: References

- [1] U.S. Department of Defense, DEPSECDEF memorandum, "Smart Card Adoption and Implementation", 10 November 1999
- [2] U.S. Department of Defense, Dr. John Hamre/Defense Management Council (DMC) decision on 24 September 1999 to adopt DoD Smart Card
- [3] U.S. Department of Defense, DEPSECDEF memorandum, "Department of Defense Public Key Infrastructure", 6 May 1999
- [4] With regard to Smart Card Decisions, DoD CIO:
 - Authorized to modify existing DEPSECDEF PKI guidance to accommodate CAC
 - Directed to execute initial CAC implementation NLT 30 December 2000
 - Directed to establish Smart Card Configuration Management Control Board (SCCMCB)
 - Established Smart Card Senior Coordinating Group (SCSCG) chaired by the Navy.
- [5] Department of the Navy Smart Card Office, "Technology Concept of Operation", March 2000
- [6] Department of the Navy Smart Card Office, "Smart Card Strategic Plan", July 1999
- [7] Department of the Navy Smart Card Office, "Smart Card Strategic Implementation Plan", October 1999
- [8] Department of the Navy, "Information Management & Information Technology Strategic Plan – FY2000/2001"
- [9] Department of the Navy Smart Card Office, "Smart Card Business Plan", November 1999
- [10] Department of the Navy Smart Card Office, "Smart Card in Cobra Gold '98", Business Case Analysis, July 1999
- [11] U.S. Department of Defense, Special Report to Congress, "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier", DRAFT version 10 January 2000
- [12] U.S. Department of Defense, OUSD (P & R) and Defense Manpower Data Center, "Common Access Card Technical Specifications – Pilot II Demonstration", DRAFT version January 2000
- [13] U.S. Department of Defense, Defense Manpower Data Center, "CAC Pilot II Architecture", DRAFT version 13 March 2000
- [14] U.S. Department of Defense, Defense Manpower Data Center, "DEERS & RAPIDS (Background Information and Support of Smart Card and Authentication Initiatives)", Information Brief, 12 January 2000

- [15] U.S. Department of Defense, Defense Manpower Data Center, "CAC Configuration Management Plan", DRAFT version
- [16] U.S. Department of Defense, Defense Manpower Data Center, "Common Access Card and PKI Integration – Proposed Strategy", DRAFT version
- [17] U.S. Department of Defense, Defense Manpower Data Center, CAC Execution Plan, DRAFT version 10 March 2000
- [18] U.S. Department of Defense, Defense Manpower Data Center, "PKI and Common Access Card Shared Issues Requiring Resolution", identified at Post-Pilot Assessment Meetings in Monterey, CA, week of 20-24 March 2000
- [19] U.S. General Services Administration, GSA Office of Smart Card Initiatives, "Government Smart Card Technical Interoperability Guidelines, Version 1.0", 3 September 1998
- [20] U.S. Department of Defense Public Key Infrastructure Target Class 4 Token Security Requirements, Draft Version 1.00, 14 February 2000
- [21] Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS Pub) 140-1, National Institute of Standards and Technology, 11 January 1994
- [22] Security Requirements for Cryptographic Modules, Draft for Comment, Federal Information Processing Standards Publication (FIPS Pub) 140-2, National Institute of Standards and Technology, 17 November 1999
- [23] Digital Signature Standard (DSS), Federal Information Processing Standards Publication (FIPS Pub) 186-2, National Institute of Standards and Technology, 27 January 2000
- [24] Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), American National Standards Institute (ANSI) X9.31-1998, May 1998
- [25] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI) X9.62-1998, ??? 1998
- [26] Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0, 29 October 1999
- [27] Public Key Infrastructure Implementation Plan for the Department of Defense, Version 2.0, 29 October 1999
- [28] U.S. Department of Defense X.509 Certificate Policy, Version 5.0, 15 December 1999
- [29] OKENEER Authentication Protocol for Smart Cards, Version 1.0, 23 January 1998
- [30] Java™ Card 2.1 API Specification, Sun Microsystems
- [31] VISA Open Platform Card Specifications, Version 2.1.1, 31 December 1999™

[32]U.S. Department of Defense, Smart Card Reader Interoperability: Operation in DoD
PKI Class 3 and Target Class 4 Architecture, Draft Version 0.6, 3 April 2000

Appendix 2: Abbreviations and Acronyms

| | |
|--------------|---|
| ACO | Access Card Office |
| ALU | Application Load Unit |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| CA | Certification Authority |
| CAC | Common Access Card |
| CAT WG | Chip Allocation Technical Work Group |
| CINC | Commander in Chief |
| CMS | Card Management System |
| COS | Card Operating System |
| COTS | Commercial-Off-The-Shelf |
| CP | Certificate Policy |
| CPMWG | Certificate Policy Management Working Group |
| CSPI | Cryptographic Service Provider Interface |
| C/S/A | CINC, Service or Agency |
| DEERS/RAPIDS | Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System |
| DIA | Defense Intelligence Agency |
| DEPSECDEF | Deputy Secretary of Defense |
| DIICOE | Defense Information Infrastructure Common Operation Environment |
| DoD | Department of Defense |
| DMDC | Defense Manpower Data Center |
| DSA | Digital Signature Algorithm |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Standards |
| FPKI | Federal Public Key Infrastructure |
| FY | Fiscal Year |
| GSA | General Services Administration |

| | |
|----------|---|
| GOTS | Government Off-The-Shelf |
| GUI | Graphical User Interface |
| H/W | Hardware |
| IA | Information Assurance |
| ICC | Integrated Circuit Chip (or card) |
| ISO | International Standards Organization |
| IT | Information Technology |
| I&RTS | Integration & Runtime Specification |
| JORD | Joint Operational Requirements Document |
| JTA | Joint Technical Architecture |
| KEA | Key Exchange Algorithm |
| KMS | Key Management System |
| LAN | Local Area Network |
| LCS | Life Cycle Support |
| LRA | Local Registration Authority |
| MARC | Multi-application Reader Card |
| MS CAPI | Microsoft Cryptographic Application Programming Interface |
| MTBOMF | Mean Time Between Operational Mission Failures |
| MTBOMFHW | Mean Time Between Operational Mission Failures for Hardware |
| MTBOMFMW | Mean Time Between Operational Mission Failures for Middleware |
| MULTOS | Multi-application Operating System for smart cards |
| NSA | National Security Agency |
| NIAP | U.S. National Information Assurance Partnership |
| NIMA | National Imagery and Mapping Agency |
| NIST | National Institute of Standards and Technology |
| NVM | Non-Volatile Memory |
| OCF | Open Card Framework |
| O&M | Operations and Maintenance |
| OPTF | Open Platform Terminal Framework |
| OS | Operating System |
| PC | Personal Computer |
| PCMCIA | Personal Computer Memory Card international Association |
| PIN | Personal Identification Number |

| | |
|--------|---|
| PKCS | Public Key Certificate Standards |
| PKI | Public Key Infrastructure |
| PM | Program Manager |
| PMO | Program Management Office |
| POM | Program Objectives Memorandum |
| RA | Registration Authority |
| R&D | Research and Development |
| R&M | Reliability and Maintainability |
| RAM | Random Access Memory |
| RDBMS | Relational Database Management System |
| ROM | Read Only Memory |
| R/A/M | Reliability, Availability, and Maintainability |
| S/A | Service or Agency |
| SBU | Sensitive But Unclassified |
| SCSUG | Smart Card Security User Group |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SSN | Social Security Number |
| S/W | Software |
| TAFIM | Technical Architecture Framework for Information Management |
| TPDU | Transmission Protocol Data Unit |
| TTS | Target Token Strategy |
| UI | User Interface |
| US | United States |
| USB | Universal Serial Bus |
| VO | Verifying Official |
| VM | Virtual Machine |
| WAN | Wide Area Network |
| WG | Working Group |

Appendix 3: Terms and Definitions

Active Mode. The condition in which a smart card is interacting with middleware through a Card Acceptance Device.

APDU (Application Protocol Data Units) – Standard communication messaging protocol between a card acceptance device and a smart card.

Application Provider – Entity that owns an application and is responsible for the application's behavior.

Asymmetric Cryptography – A cryptographic technique that uses two related transformations, a public key transformation (defined by the public key component) and a private key transformation (defined by the private key component); these two key components have a property so that it is computationally infeasible to discover the private key, even if given the public key.

Certificate Authority (CA) – *A Trusted Third Party*. CAs are entities (e.g., businesses) that are trusted to sign (issue) certificates for other entities. It is assumed that CAs will only create valid and reliable certificates as they are bound by legal agreements.

Cryptogram – Result of a cryptographic operation.

Decryption – The reversal of a corresponding encryption; decryption is performed using a symmetric secret key or an asymmetric private key to retrieve the original message.

Digital Signature – An asymmetric cryptographic transformation of data that allows the recipient of the data to prove the origin and integrity of the data; it protects the sender and the recipient of the data against forgery by third parties; it also protects the sender against forgery by the recipient.

Encryption – The reversible transformation of data by a cryptographic algorithm to produce a cryptogram; encryption can be performed using a symmetric key or asymmetric key.

Entity – An entity is a person, organization, program, computer, business, bank, or something else you are trusting to some degree.

Identity – A known way of addressing an entity. In some systems the identity is the public key; in others it can be anything from a UNIX UID to an E-mail address to an X.509 Distinguished Name.

Middleware. A specific standards-based software and/or Application Program Interface (APIs) that allows an application running on a device to communicate with the card to read, write, and transfer objects (i.e.-cryptographic algorithms, certificates, and asymmetric key pairs).

Operational Mission Failure. An operational mission failure for a smart card is the failure of one of the media on the card (ICC, magnetic stripe, bar code) to fail to operate. Data cannot be read from the media or written to the ICC. An operational mission failure for a smart card system is the failure of a smart card application operating on a host platform (PC) to stop operating.

Passive Mode. The condition in which a smart card is not interacting with middleware. Also may be referred to as the standalone mode.

Private Key – The private component of an asymmetric key pair; the private key is always kept secret by its owner; the private key is used to decrypt cryptograms that are encrypted using the corresponding public key; it is also used to digitally sign messages for authentication.

Public key – The public component of the asymmetric key pair; the public key is exposed and available to users but often is encapsulated within a certificate.

Public Key Certificate – A digitally signed statement from one entity, binding the public key (and some other information) and the identity of the owner of the corresponding private key. The owner may be an individual, a system or device, an organization, or function.

Public Key Infrastructure – The resources (people, systems, processes and procedures) that provide services to register and identify new certificate owners, retrieve certificates, and determine the current validity of certificates.

Public Key-Enabled Application – A software application that uses PK technology to: authenticate its users (people, systems and devices), ensure information is not changed or modified either during transmission or storage, hold users responsible and accountable for their actions and representations (i.e., preventing subsequent denial of responsibility), or encrypt information between parties where prior arrangement is neither known nor practical. PK-enabled applications rely on a PKI to create certificates that correctly associate a public key with the name of the owner of the associated private key, to retrieve certificates, and to determine the current validity (e.g., obtain a Certificate Revocation List [CRL]).

Secure Multipurpose Internet Mail Extension -(Multipurpose Internet Mail Extensions) A common method for transmitting non-text files via Internet e-mail, which was originally designed for ASCII text. MIME encodes the files using one of two encoding methods and decodes it back to its original format at the receiving end. A MIME header is added to the file which includes the type of data contained and the encoding method used. S/MIME (Secure MIME) is a version of MIME that adds RSA encryption for secure transmission. See base64, quoted printable encoding, UUcoding, BinHex and Wincode.

Signature – A value computed over a collection of data, the signed data, using the private key of an entity (the signer).

Smart Card. A microprocessor-based integrated circuit card compliant with the requirements of ISO 7816.

Smart Card Application. The implementation of a well-defined and related set of functions that perform useful work on behalf of the user. It may consist of software and/or hardware elements and associated user interfaces.

Smart Card System. The smart card, having its own micro-controller, is innately designed to be an off-line, portable medium. It is a standalone self-contained system that interacts with smart card-specific middleware residing in devices (i.e., PC, PDA, or phone). Legacy systems and other applications communicate with the standalone smart card system via this middleware.

Symmetric Cryptography – A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

System accuracy. The percentages of objects that originate either on the card or application that are received flawlessly by the card or application. Inaccuracies that are not detected automatically may require field level manual intervention to correct

System reliability. System Reliability is the rate of smart card specific errors that are not caused by user miscues/errors (i.e., removing the smart card from reader while processing).

Trusted Third Party (TTP) – An entity that other entities believe reliable for purposes of performing some service. The TTP generally has no bias and is neutral for purposes of performing the service.

U.S. National Information Assurance Partnership (NIAP) – is a collaborative effort of the U.S. National Institute of Standards and Technology (NIST) and the U.S. National Security Agency (NSA) and is the Certification/Validation Body formed to implement the Common Criteria in the United States.

Appendix 4: Applicable Standards

| Standard | Technology/ Function | Title |
|------------------------|-------------------------|--|
| ISO/IEC 7810 | Identification Card | Physical Characteristics: Specifies the materials that make up the composition of the card. |
| ISO/IEC 7811-1 | Magnetic Strip | Identification cards Recording technique - Part 1: Embossing |
| ISO/IEC 7811-2 | Magnetic Strip | Identification cards Recording technique - Part 2: Magnetic stripe |
| ISO/IEC 7811-3 | Magnetic Strip | Identification cards Recording technique - Part 3: Location of embossed characters on ID-1 cards |
| ISO/IEC 7811-4 | Magnetic Strip | Identification cards Recording technique - Part 4: Location of read-only magnetic tracks -- Tracks 1 and 2 |
| ISO/IEC 7811-5 | Magnetic Strip | Identification cards Recording technique - Part 5: Location of read-write magnetic track -- Track 3 |
| ISO/IEC 7811-6 | Magnetic Strip | Identification cards Recording technique - Part 6: Magnetic stripe -- High coercivity |
| ISO/IEC 7812-1 | Magnetic Strip | Identification cards Identification of issuers - Part 1: Card numbering system; major industry verifiers |
| ISO/IEC 7812-2 | Magnetic Strip | Identification cards Identification of issuers - Part 2: Application and registration procedures |
| ISO/IEC DIS 7812-2 | Magnetic Strip | Identification cards Identification of issuers - Part 2: Application and registration procedures |
| ISO/IEC 7813 | Magnetic Strip | Identification cards: Financial transactions specifications for magnetic stripe on card |
| ISO 4217 | | Specification for currencies and funds |
| ISO 8583 | Cryptography | Bank card originated messages -Interchange message specifications--Content for financial transaction |
| ISO 8583 | Cryptography | Financial transaction card originated messages --Interchange messages -- Interchange message specifications |
| ISO 8583-3 | | |
| ISO 9992-1 | | Messages between card and terminal |
| ISO 9992-2 | | Messages between card and terminal |
| ISO 10202 | Data | Financial transaction specifications |
| ISO/IEC 4287 | Card Characteristics | Surface Roughness Terminology - Part 1: Surface and its Parameters. |
| ISO/IEC 7816-1, | Card Characteristics | Identification Cards-Part 1:Physical Characteristics such as exposure limits to physical phenomena & flexibility |
| ISO/IEC 7816-2, | IC cardswith contacts | Identification Cards - Part 2: Dimensions and Location of the Contacts |
| ISO/IEC 7816-3 | IC cards with contacts | Identification cards - Part 3: Electronic signals and transmission protocols (ie communication w/ card reader) |
| ISO/IEC 7816-3 Amend 1 | IC cards with contacts | Identification cards - Part 3: Amendment 1: Specifies T=1 asynchronous transmission protocol |
| ISO/IEC 7816-3 Amend 2 | IC cards with contacts | Identification cards - Part 3 Amendment 2: Revision of transmission protocol type selection |
| ISO/IEC 7816-4 | IC cards with contacts | Identification cards - Part 4: Inter-industry commands for interchange |
| ISO/IEC 7816-5 | IC cards with contacts | Identification cards - Part 5: Numbering system and registration procedure for application identifiers |
| ISO/IEC 7816-6 | IC cards with contacts | Identification cards - Part 6: Inter-industry data elements |
| ISO/IEC 7816-7 | IC cards with contacts | Identification cards - Part 7: Inter-industry commands for Structured Card Query Language (SCQL) |
| ISO/IEC 7816-8 | IC cards with contacts | Identification cards - Part 8: Security related inter-industry commands |
| ISO/IEC 7816-9 | IC cards with contacts | Identification cards - Part 9: Additional inter-industry commands and security attributes |
| ISO/IEC 7816-10 | IC cards with contacts | Identification cards - Part 10: Electronic signals and answer to reset for synchronous cards |
| ISO 14443 | IC cards -- contactless | Physical characteristics for contactless integrated circuit chip cards |

| Standard | Technology/ Function | Title |
|--|-------------------------------|--|
| | | |
| ISO/IEC 10373 | Test Methods | Identification cards -Test methods |
| ISO/IEC 10373-1 | Test methods | Identification cards - Part 1: General characteristics tests |
| ISO/IEC 10373-2 | Test methods | Identification cards -Part 2: Cards with magnetic stripes |
| | | |
| FIPS PUB 46-2 | PKI/Encryption | Data Encryption Standards |
| FIPS PUB 48 | PKI/Encryption | Guide on the Technical Evaluation for Automated Personal ID |
| FIPS PUB 83 | PKI/Encryption | Guide on User Authentication for Network Access Control |
| FIPS PUB 112 | PKI/Encryption | Password Usage |
| FIPS PUB 140-1 | PKI/Encryption | Security Requirements for Cryptographic Modules |
| FIPS PUB 180-1 | PKI/Encryption | Secure Hash Standards |
| FIPS PUB 186-1 | PKI/Encryption | Digital Signature Standard |
| FIPS PUB 190 | PKI/Encryption | Guide to use of Advanced authentication Technology Alternatives |
| FIPS 196 | PKI/Encryption | Entity Authentication Using PKI Cryptography |
| X.509 v3 | PKI/Encryption | Certificate Policy: Digital Certificate Format |
| | | |
| ANSI X3.92 | PKI/Encryption | Data Encryption Standards |
| ANSI X9.15-1990 | | Specification for financial message exchange between card acceptor and acquirer |
| ANSI X9.69 | PKI/Encryption | Cryptographic Key Management Extensions |
| | | |
| ANSI X3.182-1990 | Bar Codes | Guidelines Bar Code Print Quality |
| Automatic Identification Manufacturers (AIM) USA, | Bar Codes | BC-1-1995, Uniform Symbology Specification Code 39, June 1993 |
| Automatic Identification Manufacturers (AIM) USA, | Bar Codes | PDF-417, July 1994 |
| PKCS # 1 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): RSA Encryption Standard |
| PKCS # 3 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Diffie-Hellman Key-Agreement Standard |
| PKCS # 5 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Password-Based Encryption Standard |
| PKCS # 6 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Extended-Certificate Syntax Standard |
| PKCS # 7 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Cryptographic Message Syntax Standard |
| PKCS # 8 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Private-Key Information Syntax Standard |
| PKCS # 9 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Selected Attribute Types |
| PKCS # 10 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Certificate Request Syntax Standard |
| PKCS # 11 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Cryptographic Token Interface Standard |
| PKCS # 12 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Personal Information Exchange Syntax Standard |
| PKCS # 13 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Elliptical Curve Cryptography Standard |
| PKCS # 15 | PKI/Encryption | Public-Key Cryptography Standards (PKCS): Cryptographic Token Information Format Standard |
| | | |
| NIST | Smart Card Protection Profile | National Institute of Standards and Technology : Smart Card Protection Profile (NIST Draft 1) |
| | | |
| Biometric API | Biometric API | Guidelines for application developers to incorporate biometric applications. Biometric Consortium |
| NSA | Biometrics | Guidelines for Placing Biometrics in Smart Cards: Specs on biometric template/ 512 bytes or less on card |
| Security Enterprise Integration Working Group (SEIWG), | Magnetic Stripe | SEIWG-012, Prime Item Product Specification Magnetic Stripe Credential (MSC), Feb 28, 1994 |

| Standard | Technology/ Function | Title |
|----------------------------|------------------------------------|---|
| <i>Open Card Framework</i> | Smart Card Interoperability | Open Card Framework, Version 1.2, January 2000 |
| <i>PC/SC Work Group</i> | Smart Card Interoperability | Interoperability Specification for ICCs and Personal Computer Systems, Part 1 through 8, Revision 1.0 |
| <i>VISA Open Platform</i> | Open Card & Terminal Specification | VISA Open Platform Card Specification, Version 2.0.1; and Terminal Specification, Version 1.5 |

Appendix 5: CAC Data Element Definition Matrix

| <i>R E F #</i> | <i>CATEGORY</i> | <i>ALIAS</i> | <i>DATA ELEMENT ATTRIBUTE</i> | <i>Size (Bytes)</i> | <i>DATA ELEMENT DEFINITION</i> | <i>DoD REFERENCE</i> | <i>COMMENT</i> |
|----------------------------|-----------------|---------------------------|---|-------------------------|--|--------------------------|--|
| 1 | Identification | First Name | Person Forename Text | 20 | The text of a person forename. | DDDS ID # 49782 | |
| 2 | Identification | Gender | Sex Category Code | 1 | The code that represents a classification of a person of an organism according to the reproductive functions. | DDDS ID # 11697 | |
| 3 | Identification | Person Designator | Person Designator Type Code | 1 | The code that represents a specific kind of person designator. | DDDS ID # 13680 | Included "Designator" in attribute |
| 4 | Identification | Last Name | Person Surname Text | 26 | The text of a person surname. | DDDS ID # 49789 | In DDDS as 30 bytes; a change has been submitted to make 26 bytes |
| 5 | Identification | Middle Name | Person Middle Name Text | 20 | The text of a person middle name. | DDDS ID # 49783 | |
| 6 | Identification | Social Security Number | Person Designator Identifier | 15 | The identifier that represents a person. | DDDS ID # 11185 | |
| 7 | Identification | Suffix | Person Cadency Name Text | 4 | The text of a person cadency name. | DDDS ID # 49780 | |
| 8 | Identification | Person Identifier | DoD Electronic Data Interchange (EDI) Person Identifier | 10 | The identifier that is used to represent the person within a Department of Defense Electronic Data Interchange. | | |
| 9 | Benefits | Date of Birth | Person Birth Calendar Date | 8 | The calendar date when a person was born. | DDDS ID # 11322 | |
| 10 | Organization | Branch | Uniformed Service Branch Classification Code | 1 | The code that represents a Uniformed Service branch classification. | DDDS ID # 52292 | |
| 11 | Organization | Rank | Rank | 6 | The abbreviated name of a Uniformed-Service-Rank. | DDDS ID #23514 | |
| 12 | Organization | Personnel Category | Personnel Category Code (active, reserve, guard, DoD Civil service, DoD Contractor) | 1 | The code that represents how the DoD personnel and/or finance center views the sponsor based on accountability and reporting strengths. | | |
| 13 | Organization | Government Agency | US Government Agency/Subagency Code | 4 | The code that indicates the government agency an Other Civil Service of Government Agencies personnel member works for. Is used to determine the benefits provided by DoD. Valid for Other Civil Service of Government Agencies only. | | |

| | | | | | | | |
|----|--------------|-------------------------------|---|------|---|-----------------|--|
| 14 | Organization | Non-Government Agency | US Non-Government Agency Code | 2 | The code that indicates the non-government agency or other agency a personnel member works for. Used to determine the benefits provided by the DoD. | | |
| 15 | Organization | Pay Category | Pay Plan Code | 2 | The code that represents a pay plan. | DDDS ID # 20374 | Reduced, with element #15 from a total of 6 bytes to 4 bytes |
| 16 | Organization | Pay Grade | Pay Plan Grade Code | 2 | The code that represents a sequential level of pay within a Pay Plan. | DDDS ID # 20369 | Reduced, with element #14 from a total of 6 bytes to 4 bytes |
| 17 | Benefits | Contractor Code | DoD Contractor Function Code | 1 | A code that indicates the type of work a DoD contractor does or agency they work for; used for benefits determination. | | |
| 18 | PKI | Identity Certificate | DoD PKI Authentication Certification Data | 2000 | The data contained in this person's authentication certificate used for the DoD private key infrastructure. | | |
| 19 | PKI | Signature E-Mail Certificate | S/MIME Certification Signature Data | 2000 | The data contained in the person's public signature key for the secure multipurpose Internet mail extension certificate. | | |
| 20 | PKI | Encryption E-Mail Certificate | S/MIME Certificate Encryption Data | 2000 | The data contained in the person's public encryption key for the secure multipurpose Internet mail extension certificate. | | |
| 21 | PKI | Private Key Identifier | DoD PKI Authentication Private Key Identifier | 768 | The identifier for the person's authentication used for the DoD private key infrastructure. | | |
| 22 | PKI | Encryption Identifier | S/MIME Encryption Private Key Identifier | 768 | The identifier used for the person for the secure multipurpose Internet mail extension private encryption key. | | |
| 23 | PKI | Signature Identifier | S/MIME Signature Private Key Identifier | 768 | The identifier used for the person for the secure multipurpose Internet mail extension private signature key. | | |
| 24 | Benefits | Meal Entitlement Code | Meal Plan Type Code | 2 | The code that indicates what meal plan the holder of this common access card is a participant (may interface with current applications) | | Retained from legacy smart card |
| 25 | Benefits | Exchange Code | Exchange Benefit Status Code | 1 | The code that indicates the status of the person's exchange benefits. | | |
| 26 | Benefits | Commissary Code | Commissary Benefit Status Code | 1 | The code that indicates the status of the person's commissary benefits. | | |
| 27 | Benefits | MWR Code | MWR Benefit Status Code | 1 | The code that indicates the status of the person morale, welfare, and recreation benefits. | | |

| | | | | | | | |
|----|-----------------|--|--|---|---|-------------------------|--|
| 28 | Benefits | End Date | Non-Medical Benefits Association End Calendar Date | 8 | The end date of the person's association with the DoD non-medical personnel programs on the Common Access Card (e.g., if eligibility needs to be shorter than data currency end date) | | |
| 29 | Benefits | Entitlement Code | Civilian Health Care Entitlement Type Code | 1 | The code that represents what type of civilian health care privileges the person has. | | |
| 30 | Benefits | Type Code | Direct Care Benefit Type Code | 1 | The code that represents what type of direct care benefits the person has. | Requested, ID # Pending | |
| 31 | Benefits | Medical Benefits End Date | Medical Benefits Association End Calendar Date | 8 | The end date the person's association with the DoD medical benefit programs on the common access card. | | |
| 32 | Benefits | Entitlement Condition | Personnel Entitlement Condition Type Code | 2 | The code that represents the type of condition that occurred while a sponsor was in a personnel category and organization that affects the entitlements of the sponsor and/or the sponsor's family members. | | Allows systems to more clearly define an individual's affiliation to DoD; distinguishes between a Reservist and a Reservist on Active Duty or a Civilian and a Civilian on Overseas Assignment |
| 33 | Card Management | Date Demographic Data was Loaded on Chip | CAC Demographic Data Begin Calendar Date | 8 | The date data elements are loaded in demographic applet. This date is mutually exclusive of benefit dates. | | Supports change in status for benefit purposes |
| 34 | Card Management | Date Demographic Data on Chip Expires | CAC Demographic Data End Calendar Date | 8 | The date data element currency in demographic applet expires. This date is mutually exclusive of benefit dates. | | Supports change in status for benefit purposes |
| 35 | Card Management | Card Security Code | Card Instance Identifier | 3 | The identifier used to uniquely identify each card issued to a person | | |
| 36 | Card Management | Card Issue Date | Identification Card Issue Calendar Date | 8 | The date when the person's current or former ID card was issued. | | Facilitates issuance of PKI certificates |
| 37 | Card Management | Card Expiration Date | Identification Card Expiration Calendar Date | 8 | The date when the person's current ID card is expected to expire. | | Facilitates issuance of PKI certificates |
| 38 | Identification | Blood Type | Blood Type Bar Code | 2 | The code that represents a blood type | DDDS ID # 28274 | |

Appendix 6: White Paper—Smart Cards: Designing a Hybrid Card Architecture from a Web-centric and Card-centric Perspective

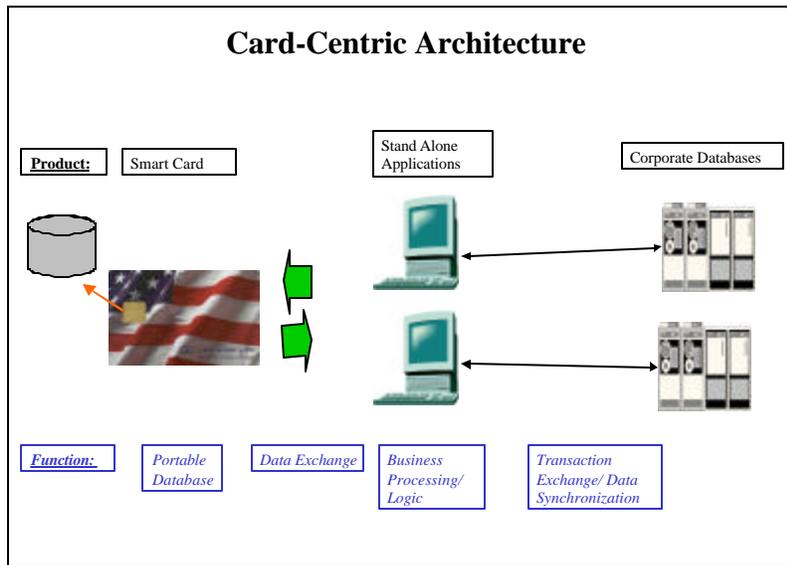
Overview

The world is evolving to a more web-based application service environment. In the past, smart cards have been used as portable data carriers; however, technical invocations and evolutions have positioned smart cards as a cornerstone in enabling other technologies. It will serve as a medium to securely access services provided by web-based application solutions. Today, large corporate enterprises as well as national/local governments are faced with the task of designing a card architecture that is suitable for both the present and future. This system should serve in a portable data as well as the future web-centric, distributed data environments.

This white paper contrasts the advantages and disadvantages of a Card-Centric versus Web-Centric perspectives. The Department of the Navy Smart Card Office champions an alternative path that exploits the advantages of both while minimizing the disadvantages of each.

Card-Centric Perspective

In a card-centric environment, the card contains sufficient information to perform processing functions off-line to include both static and dynamic data. The data on the card is a subset of data contained on a centralized database or separate storage device. However, the database is viewed as merely back-up storage to the card content. The card is designed to function independently off-line without the need to be connected to the centralized database (See Diagram A). The functional requirements of the applications dictate the level of card security. Examples of Card-Centric deployments include: Western Governors' Association (WGA) Health Passport Project, French Health Card, German Health Card, Dutch Defense Ministry ID Card, and the UK Postal Service ID Card.

Diagram A: Illustration of Card-Centric Architecture

a. Advantages

- ?? Since the card can perform functions off-line, the network load is reduced. Therefore, the availability of the network is less critical
- ?? The card could support flexible security architecture depending upon the card functionality and the security environment
- ?? In combat situations, the increased availability of data on the card can provide for the dynamic updating of data until the central database can be accessed

b. Disadvantages

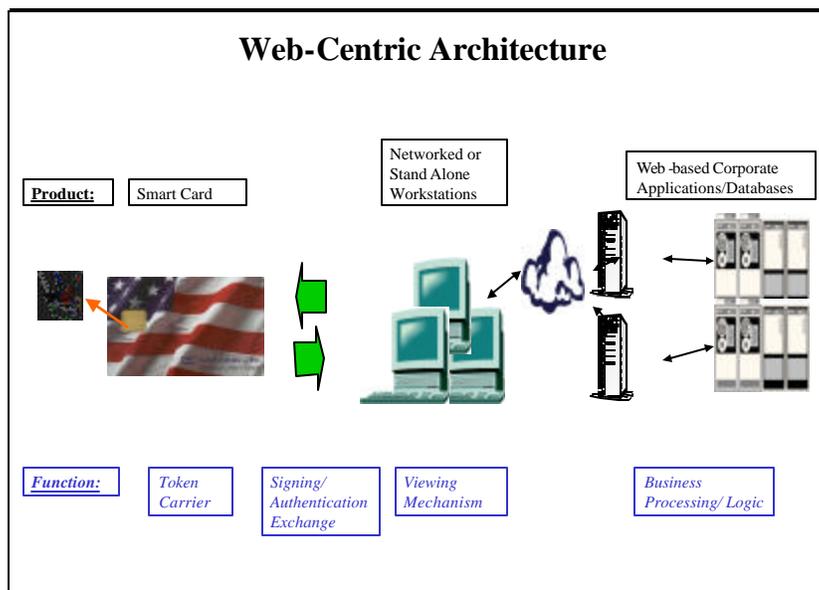
- ?? Since the card can operate off-line, the data can be leading or lagging the centralized database contributing to outdated data on the card and the database. If the card acts on outdated data on the card, then the accuracy of data can be in question. Hence, there is a need to synchronize the data between the card and the database
- ?? Since there is an increased emphasis on processing card data at the point of interaction (POI), the POI device must have enhanced processing capability and also must have off-line authentication capability along with authorization to change card data. The drawback is the need for increased processing and store/forward capability of the POI
- ?? The process of defining the common data elements to satisfy large enterprise environment with multiple legacy databases would require a more lengthy process
- ?? The card memory size must be larger to accommodate the increased data requirements. Thus, the cost of the card will be higher
- ?? In combat situations, the increased availability of data on the card will require well-defined Department-wide policy. Combat requirement and rules will need to be clearly defined. Data outside of Geneva Convention requirements

could become detrimental to the well being of the service members and their families

Web-Centric Perspective

In a web-centric environment, the data on the card does not exist or it is used sparingly as a link or pointer to web-based solutions. These web-based solutions will contain all necessary dynamic as well as static data elements. The card provides the capability to be used as an authentication device to validate access and support non-repudiation via digital signature (See Diagram B). An example of a Web-Centric deployment is American Express' "Blue Card".

Diagram B: Illustration of Web-Centric Architecture



a. Advantages

- ?? Data synchronization requirements are minimized since all data elements are maintained in web-based applications or databases
- ?? Since all the card functions are centrally performed on-line, centralized control and monitoring of the card-based application services are possible

b. Disadvantages

- ?? The increased on-line demand places an increased burden on the availability and bandwidth of communications
- ?? Unauthorized web-based hacker attacks could result in degradation or denial of service

Answer: A Mixture of Both

As shown above, there are distinct disadvantages of a pure card-centric or web-centric approach. To arrive at a more acceptable alternative, one must recognize that current environment cannot be served by adopting either one approach or the other.

Characteristics of the current environment include:

- ?? The databases of most large corporate enterprises and government entities are designed for vertical applications. Consequently, the data elements are defined per application per organization. Defining the common data elements with common definition, which can be used across multiple applications and multiple service organizations, would be a complex and time consuming process
- ?? The current suite of applications supporting most large organizations/enterprises are not all web-based and, as such, are not positioned to support a pure web-centric approach.
- ?? The current communications infrastructure for most large organizations/enterprises (in terms of availability and bandwidth) to support a pure web-centric approach will require advances in capability and technology.

Given the above, an alternative based upon a mixture of the two approaches appears to be more desirable. Therefore, a Hybrid Card Architecture (HCA) based upon a mixture of card-centric and web-centric is recommended to minimize the disadvantages and potential risks associated with either distinct approach. Examples of Hybrid Card Architecture deployments include: Finland's National ID Card (FinID) and Spain's National ID Card (Ceres).

The characteristics of a new Hybrid Card Architecture would include:

- ?? Core set of static data. This data should consist of demographic data that is common to all with a single set of data definitions
- ?? PKI-based functionality that will serve the need of a web-centric approach by providing strong authentication and non-repudiation
- ?? Application and/or organization specific set of data (static and/or dynamic). It should be defined by the application/organizational entities utilizing the data. All cardholders will not require this type of information. As a result, the card architecture/system should be designed to accommodate secure updates/enhancements of cards post-issuance. It will be difficult to keep up with new application/organization specific requirements, hence this type of data should not be on the card at issuance, but rather loaded at a later time.
- ?? A migration from current VPN-based as well as legacy network application services to web-centric application services as the world moves toward more "on-line"

Conclusions

The evolution of smart card provides a technology that can serve the needs of both card-centric and web-centric design approaches. The card memory sizes continue to increase to satisfy the demand for more data storage on the card while the processing power of the chip accelerates to support the resource demands by the new multi-application card operating systems and public key cryptography. Likewise the expansion of our communication infrastructures holds considerable promise in

supporting the growing requirements for availability and bandwidth associated with more web-based applications.

As the world evolves to a web-based environment, smart card capabilities continue to keep pace as an enabling technology for PKI-based security architecture that is the key requirement for web-centric approach. In addition to the PKI support capability, smart cards can also support secure multi-application platform requirements that are required for the card-centric approach. Since smart card technology is available to support both design approaches as evidenced above, choosing a design architecture becomes an exercise in minimizing the disadvantages and potential risks while exploiting the advantages. Leading large enterprises to a hybrid card architecture.

Appendix 7: CAC Interoperability Findings

Introduction

The CAC architecture corresponds to accepted industry standards and procedures. The CAC model is derived from commercial industry benchmarks. Smart cards today are procured according to existing industry standards, which unfortunately do not go far enough to guarantee 100% interoperability. This proposed CAC architecture builds from these industry standards and moves the smart cards closer to interoperability. As with any new system, the initial cards will require certification/validation that they meet a common interoperable capability. Moving forward this will become easier, not through the efforts of the DoD but other organizations (such as Visa, MasterCard, American Express, and European Union programs, etc.) also pushing for this same result.

The CAC architecture shall migrate over time as the industry renews its innovation base. The proposed architecture for the DoD shall also evolve as industry best practices incorporate an evolutionary approach that maintains vintage compatibility for a guaranteed 3 year window (as this is the maximum proposed lifetime of the CAC).

This section introduces a CAC architecture for the Smart Card and PC platform, discusses the components and how those components need to inter-operate with each other. Open Platform³ (Global Platform) Card Specification V2.0.1 published by Visa International and JavaTM Card API 2.1 Specification published by Sun Microsystems are referenced as the normative guidelines for the interoperability of card-based application. The PC/SC specification titled "Interoperability Specification for ICCs and Personal Computer Systems, Part 1 through 8, Revision 1.0" published by the PC/SC Work Group is the normative reference for the interoperability between the card-based and the PC-based application.

The PC/SC specification was developed by major participants of the smart card and PC industry to facilitate the interoperability necessary to allow Integrated Circuit Card (ICC) technology to be effectively utilized in the PC environment. However, the PC/SC specification does not address card-based application interoperability in a card platform as well as card security management throughout the card life cycle states; namely, operationally ready, initialized, secured, card manager locked and terminated.

Through the Open Platform initiative, Visa International has worked with the chip card industry to deliver a hardware-neutral, vendor-neutral and application-independent card management standard. The Open Platform⁴ Card Specification

³ VISA Open Platform Card Specification, Version 2.0.1

⁴ VISA Open Platform Card Specification, Version 2.0.1

V2.0.1 provides a common security and card management architecture to create an interoperable multi-application smart card system.

7.2 CAC architecture

The chart, in Exhibit 7.2, below depicts the CAC architecture as it correlates to PC/SC Specification version 1.0. It shall be used as the foundation for describing the major components of the Architecture as well how they must inter-operate to achieve interoperability.

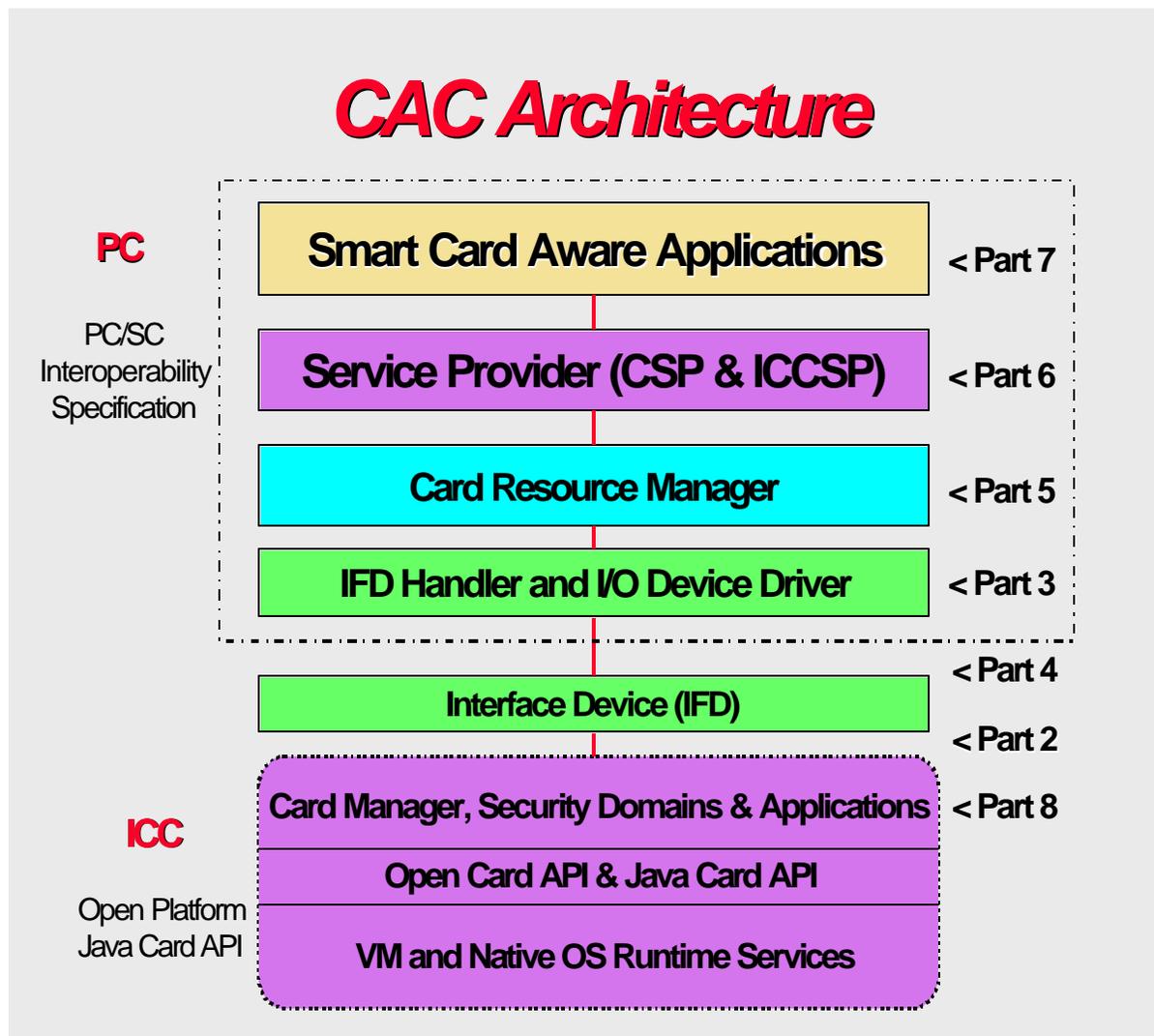


Exhibit 7.2 – CAC architecture

The PC/SC Interoperability Specification describes the minimum functionality required of ICCs, ICC Interface Devices (IFDs) and PCs to allow interoperability

among compliant elements as provided by a variety of vendors. The specification as a whole seeks to achieve the following:

- ?? Maintain consistency with existing ICC-related and PC-related standards while expanding upon them where necessary and practical.
- ?? Enable interoperability among components running on various platforms (platform neutral).
- ?? Enable applications to take advantage of products and components from multiple manufacturers (vendor neutral).
- ?? Enable the use of advances in technology without rewriting application-level software (application neutral).
- ?? Facilitate the development of standards for application-level interfaces to ICC services in order to enhance the fielding of a broad range of ICC-based applications in the PC environment.
- ?? Support an environment that encourages the widest possible use of ICCs as an adjunct to the PC environment.

Its eight (8) parts define the specification. These are intended to apply only to devices and software intended to operate as a part of an overall system that includes a personal computer. These parts are labeled accordingly on *Exhibit 7.2 - CAC architecture* shown previously and shall be discussed below.

Part (1) – Introduction and Architecture Overview

This part is defined in terms of the software and hardware components that comprise the architecture. The components include:

- ??Integrated Circuit Card (ICC) - commonly called a “smart card”.
- ??Interface Device (IFD) – commonly called a “smart card reader”.
- ??Interface Device Handler (IFD Handler)
- ??ICC Resource Manager
- ??Service Provider (SP)
 - ICC Service Provider (ICCSP)
 - Cryptographic Service Provider (CSP)
- ??ICC-Aware Application

Part (2) – Interface Requirements for Compatible IC Cards and Readers

This part discusses requirements for physical, electrical and low-level data communications protocol compatibility between ICC and IFD. This material corresponds to that covered in ISO 7816 Parts 1,2 and 3.

Part (3) – Requirements for PC-Connected Interface Devices

This part discusses interface requirements for the PC-connected peripherals designed to interface to ISO 7816-compatible ICC. This specification is compatible with IFD Subsystems (IFD Handlers and Device Drivers) using any available PC I/O channel to communicate with the IFD.

Part (4) – IFD Design Considerations and Reference Design Information

This part discusses design information on several types of IFD and special design information related to the I/O channel used by those IFDs to communicate with the PC.

Part (5) – ICC Resource Manager Definition

This part describes responsibilities of the ICC Resource Manager. Refer to *Appendix 8* for details.

Part (6) – Service Provider Interface Definition

This part deals with the Service Provider element of this CAC architecture. Refer to *Appendix 8 – CAC Middleware Requirements* for details.

Part (7) – Application Domain and Developer Design Considerations

This part describes the way ICC-aware applications can use the functionality provided by the ICC subsystem. By using the ICC Resource Manager and the ICC Service Provider layers, an application can use ICC functionality with some level of independence from a specific IFD or a specific ICC.

Part (8) – Recommendations for ICC Security and Privacy Devices

This part defines recommendations for ICCs that support “generic” end-user security and privacy requirements. In this context, generic means support of a broad spectrum of applications and existing open systems standards within the networked PC environment.

The Open Platform⁵ Card Architecture is comprised of a number of components that ensure hardware and vendor-neutral interfaces to on-card applications as well as off-card management systems. The CAC architecture shows components in an ICC that includes applications from Application Providers (APs).

All applications are assumed to exist in a secure runtime environment that includes a hardware-neutral and vendor-neutral API such as Java Card API to support application portability. The Card Manager is the primary Open Platform⁶ card component that acts as the central administrator for an Open Platform⁷ card.

Special key and security management applications called Security Domains are created to ensure complete separation of keys among the multiple Application Providers.

The Open Platform⁸ API provides applications access to card management services administered by the Card Manger.

⁵ VISA Open Platform Card Specification, Version 2.0.1

⁶ VISA Open Platform Card Specification, Version 2.0.1

⁷ VISA Open Platform Card Specification, Version 2.0.1

⁸ VISA Open Platform Card Specification, Version 2.0.1

7.3 ICC Platform Physical Security

Chip manufacturers have been developing chip security solutions to satisfy the security requirement of the ICC Protection Profile developed by Smart Card Security User Group⁹ (SCSUG). Security requirements of Class 4 DoD PKI token from NSA and ICC Protection Profile from SCSUG (memberships include both NSA and NIST) need to converge. Until convergence occurs, issues of interoperability will continue to persist.

7.5 Vendor Independent Card Application

Since the mid-1990s, a significant breakthrough occurred in the ICC industry with the introduction of open systems standard for application development. The three leading technologies are Java™ Card, Windows for Smart Cards and MULTOS. These technologies provide common programming standards allowing application portability among different vendors' card implementations, or otherwise none as interpretive platforms. CAC shall be a multi-application platform where valid card-based applications can be downloaded, installed and deleted dynamically. An example of the architectural components based on the Open Platform is shown in *Exhibit 7.5*.

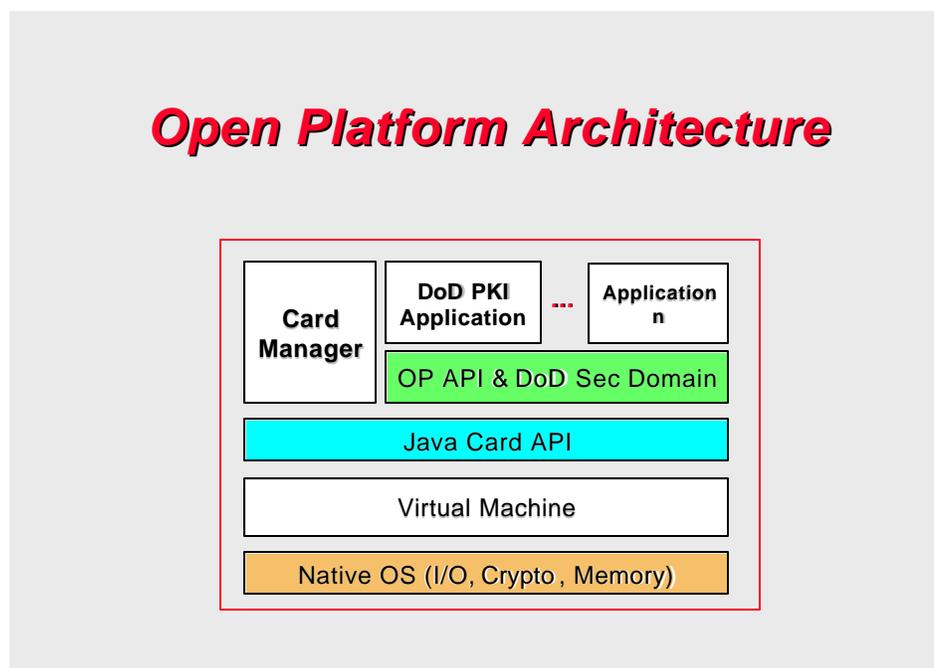


Exhibit 7.5 – Open Platform Architecture

⁹ SCSUG – formed in June, 1999, under the sponsorship of NIAP and composed of major credit card brands (financial payment systems).

7.6 Card Application Independent PC Application

The Application Protocol Data Unit (APDU) serves to ensure that the application running in the ICC can communicate or inter-operate with the application running in the PC or Terminal. ISO 7816, Part 4, defines the set of commands and status indicators that comprise the 'tool box' to be used by both the application in the PC or Terminal and the application in the ICC. Refer to *Exhibit 7.6 - APDU interface*.

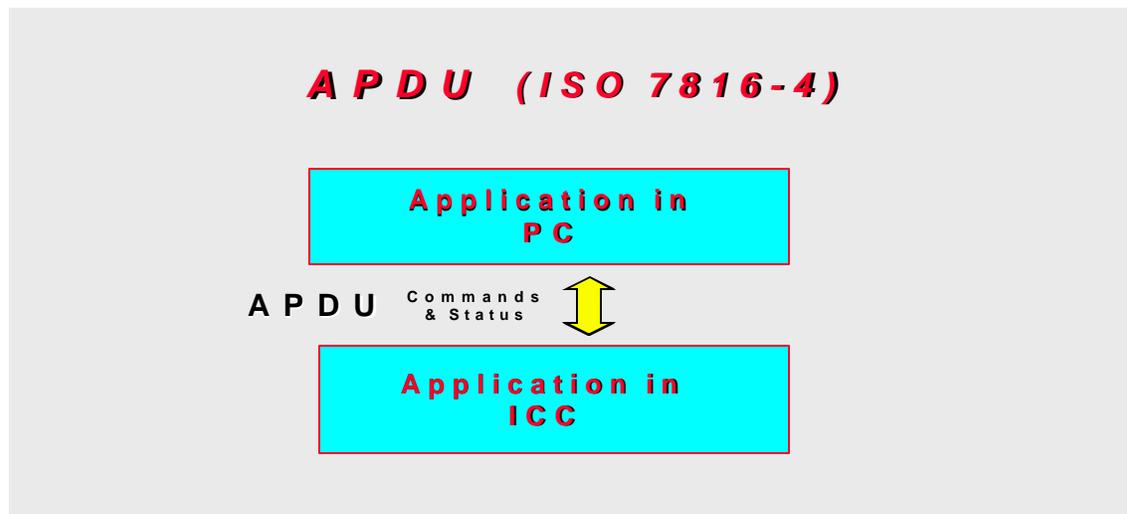


Exhibit 7.6 – APDU Interface

7.7 ICC Electrical Compatibility

The CAC design shall follow industry norms including those defined by the International Standards Organization (ISO). *Appendix 4 – Applicable Standards* includes those standards and specifications that the CAC shall follow. The ISO 7816 Part 3 standard specifies electrical interface characteristics and data communication protocol between ICC and IFD. PC/SC Interoperability Specification Part 2 requires the compatibility with the ISO 7816-3 standard.

7.8 IFD Vendor Independent PC

PC/SC Interoperability Specification Part 3 and 4 provides this interoperability.

7.9 Card Platform Independent PC Application

PC/SC Interoperability Specification - Part 6 defines Service Provider responsible for encapsulating functionality available in a specific ICC and making it accessible through high-level programming interfaces. The specification defines programming

interfaces for common functionality such as file access, authentication and cryptographic services. Cryptographic Service Provider (CSP) allows the ICC cryptographic functions accessible to ICC-aware Applications and ICC Service Provider (ICCSP) allows non-cryptographic functions. These Service Provider components provide transparency of card platform to the ICC-aware Applications running in PC.

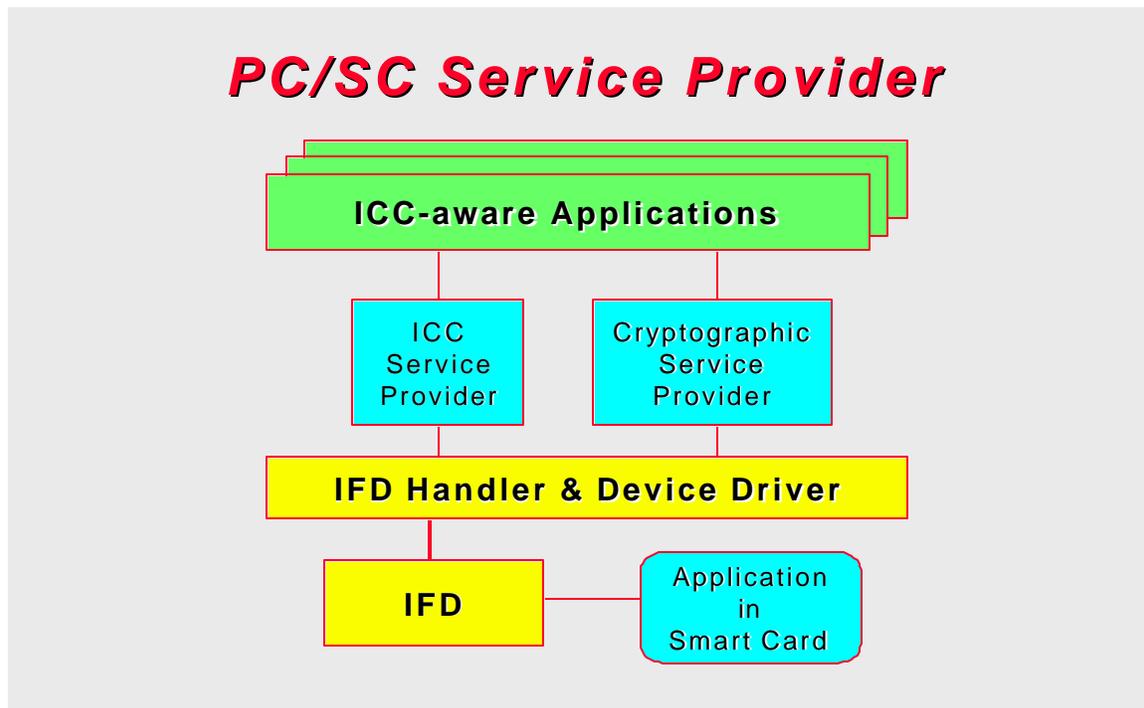


Exhibit 7.9 – PC/SC Interoperability Layers (abridged)

7.10 Transparent Application Loader

Applications running in the CAC will go through the application life cycle states. The application life cycle states are:

INSTALLED
 SELECTABLE
 PERSONALIZED
 BLOCKED
 LOCKED
 LOGICALLY_DELETED

The Card Manager sets the life cycle of an application to its initial state of INSTALLED during the application installation process. The Card Manger also manages the registry of applications installed and loaded in a CAC.

CAC applications shall be installed and loaded via Card Manger's APDU commands defined in the Open Platform¹⁰ Card Specification V2.0.1 as depicted in *Exhibit 6.10 – Application Loader Interface*.

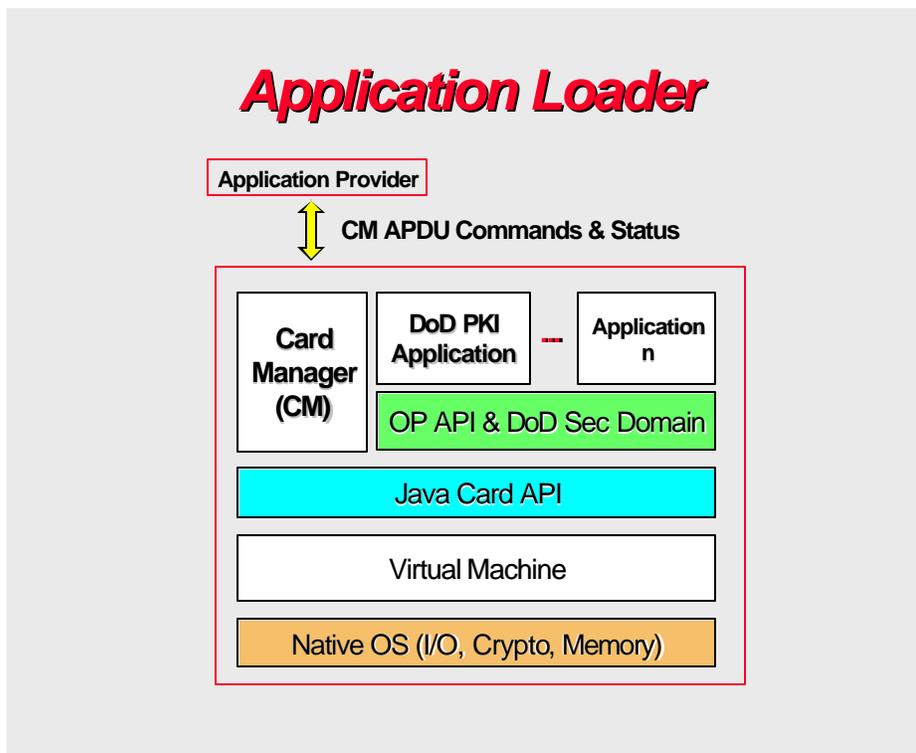


Exhibit 7.10 – Application Loader Interface

7.11 Applicable Standards and Specifications

To ensure seamless card holder access across a wide range of smart card-enabled applications, the components of the CAC Platform must adhere to the appropriate series of standards or industry specifications to fulfill the mission of interoperability. The *Applicable Standards* covering the potential array of technology mediums employed are included in *Appendix 4*.

¹⁰ VISA Open Platform Card Specification, Version 2.0.1

Appendix 8: CAC Middleware Requirements

8.1 Background

The term “Middleware” is defined as a specific standards-based software and/or Application Programming Interface (API) that allows an application running on a device to communicate with the ICC (smart card) to read, write and transfer objects. For the purpose of this section, CAC middleware component includes Service Provider (SP) as defined in the PC/SC Interoperability Specifications. CAC middleware component is depicted in Exhibit 8.1, CAC Middleware.

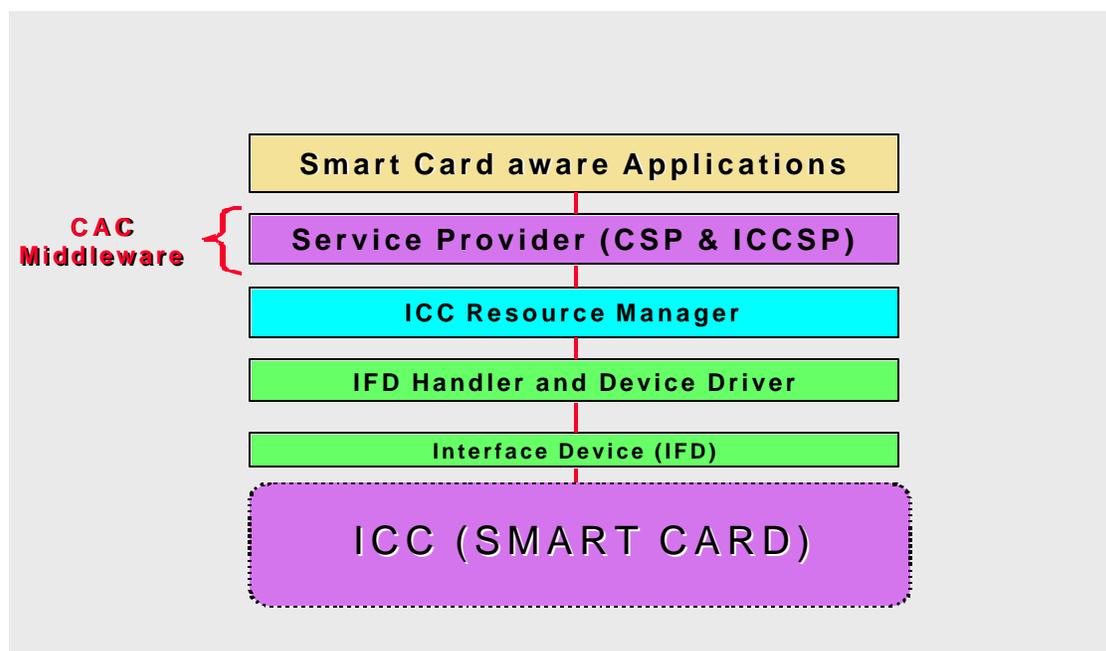


Exhibit 8.1 – CAC Middleware

The Service Provider uses the system service provided by the ICC Resource Manager. It is assumed to be a system-level component and should be provided by the operating system supplier. It is responsible for managing the ICC-relevant resources and for supporting controlled access to the Interface Device (IFD) and the ICC through the IFD. The functions of the ICC Resource Manager include:

- ?? Tracking installed IFDs and making this information accessible to other applications.
- ?? Tracking known ICC types, along with their associated SP and supported Interfaces, and making this information available to other applications.

- ?? Tracking ICC insertion and removal events to maintain accurate information on available ICCs within the IFDs.
- ?? Controlling the allocation of IFD resources.
- ?? Supporting transaction primitives on access to services available within a given ICC

The Service Provider is further subdivided into a Cryptographic Service Provider (CSP) component which exposes cryptographic services provided by the ICC that are accessible to external applications, and a non-cryptographic ICC Service Provider (ICCSP) component.

The following sub-sections further define the CSP and ICCSP components related to Core CAC applications as well as Component dependent applications.

8.2 DoD PKI Middleware Requirement

DoD PKI Middleware shall employ a single CSP that has the following generic cryptographic services:

- ?? Key generation
- ?? Key management
- ?? Digital signature
- ?? Message digest
- ?? Bulk encryption
- ?? Key import and export

The DoD PKI CSP encapsulates access to cryptographic functionality provided by the CAC through high level programming interfaces. The CSP expose the CAC cryptographic functions to PKI applications running on a client workstation.

It shall be an open and non-proprietary solution. Implementation shall be in such a manner that it employs both PKCS#11 and Microsoft Cryptographic Service Provider standards. In addition, the DoD PKI CSP shall be implemented with a clear migration path of current cryptographic interoperability issues such as PKCS #15 with a defined set of APDU, PKCS #12, PKCS #1 and ICC on-board key generation and key storage.

The detailed specification of the services to be performed by the DoD PKI CSP will developed with Component involvement with the GSA smart card contract vehicle.

8.3 Physical Security Access Middleware Requirement

The CAC provides multiple technologies for implementing physical security access. Components could choose magnetic stripe, bar code or ICC IFDs to perform this application. The details of using ICC smart card readers (IFDs) will developed with Component involvement with the GSA smart card contract vehicle.

8.4 Core Data and Other Application Middleware Requirement

There will be other applications other than PKI and physical access as defined above. Minimally, there will be core data applications as defined in the DoD functionality of the CAC. These applications shall employ services exposed by non-cryptographic ICC Service Provider (ICCSP). ICCSP implementations shall be in accordance with PC/SC or OCF standards.

The ICCSP is responsible for exposing high-level interfaces to non-cryptographic services that include common interfaces to a CAC as well as access to file and authentication services. Depending on implementation, there could be multiple ICCSP to handle each specific non-cryptographic card applications.

The ICCSP shall implement the interface for managing a CAC (or specific card application) and provides mechanisms for connecting and disconnecting to the overall CAC pr specific card application. In addition, the ICCSP shall implement file access and authentication services that will encapsulate functionality defined by Open Platform¹¹ (also known as Global Platform) Card Specification 2.0.1 and ISO 7816-4.

The generic file access services define mechanisms for the following tasks:

- ?? Locating files by name
- ?? Creating or opening files
- ?? Reading and writing file contents
- ?? Closing a file
- ?? Deleting a file
- ?? Managing file attributes

¹¹ VISA Open Platform Card Specification, Version 2.0.1

The generic authentication services define mechanisms for the following tasks:

- ?? Cardholder verification
- ?? ICC authentication
- ?? Application authentication to the ICC

The detailed specification for these 'other applications' will be defined with Component involvement with the GSA smart card contract vehicle.