



---

***CAC Release 1.0 Middleware Requirements***

---

**Version 2.2**  
**7 March 2002**

Prepared by: Access Card Office

UNCLASSIFIED

# TABLE OF CONTENTS

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>2</b>
<b>2</b>	<b>MIDDLEWARE.....</b>	<b>2</b>
2.1	CLIENT WORKSTATION OPERATING ENVIRONMENTS .....	3
2.1.1	<i>Client Workstation Resource Utilization .....</i>	<i>4</i>
2.1.2	<i>Session Management-Maintain Best Practice.....</i>	<i>4</i>
2.2	MULTIPLE APPLLET IDENTIFICATION (AID) .....	5
<b>3</b>	<b>SUPPORTING MIDDLEWARE MODULES .....</b>	<b>5</b>
3.1	CAC CRYPTOGRAPHIC MIDDLEWARE .....	5
3.1.1	<i>Cryptographic Requirements .....</i>	<i>6</i>
3.1.2	<i>Card Management Utility Requirements .....</i>	<i>8</i>
3.2	CAC DoD DATA MIDDLEWARE .....	9
3.2.1	<i>DoD Data Requirements .....</i>	<i>9</i>
3.3	CREDENTIAL INTEROPERABILITY .....	11
3.4	ANSWER TO RESET (ATR) DISCOVERY AND HANDLING.....	11
<b>4</b>	<b>MIDDLEWARE AND READER QUALIFICATION TESTING.....</b>	<b>12</b>
4.1	QUALIFICATION PROCESS BACKGROUND.....	12
4.2	TESTING PROCEDURES .....	12
4.2.1	<i>Description of Test.....</i>	<i>14</i>
	<b>APPENDIX A: REFERENCES.....</b>	<b>15</b>
	<b>APPENDIX B: GLOSSARY OF ACRONYMS.....</b>	<b>16</b>
	<b>APPENDIX C: TERMS AND DEFINITIONS .....</b>	<b>20</b>

# 1 Executive Summary

This specification was written by the Department of Defense (DoD) Access Card Office (ACO) for the procurement of Middleware to function with the Common Access Card (CAC). The procurement will be executed under the auspices of the DoD Enterprise Software Initiative (ESI) to establish an Enterprise Software Agreement for use by all Services and Components within DoD.

The CAC has presently been issued to 140,000+ personnel within the Department with the intent to issue 4.3 million CAC's within DoD by mid 2003. Full-scale implementation and issuance began within all services in November 2001.

Card issuance is accomplished via the DoD Real Time Automated Personnel Identification System (RAPIDS), a computer system with over 1500 identification card issuance stations worldwide. These systems presently use middleware integrated into RAPIDS to provide a secure issuance environment.

This middleware document supports the client requirements of the DoD Components (Army, Navy, Air Force, Marines, and DoD Agencies) to utilize the CAC.

# 2 Middleware

This section details the technical and functional requirements for middleware as defined in this document.

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 Integrated Circuit Chip (smart card) to read, write and transfer objects. For the purpose of this document, the Common Access Card (CAC) middleware includes Service Providers (SP) modules as defined in PC/SC, Open Card Framework, and GSA Interoperability Specifications.

Minimally, Service Provider(s) shall use the system services provided by the ICC Resource Manager. Firstly, the ICC Resource manager 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

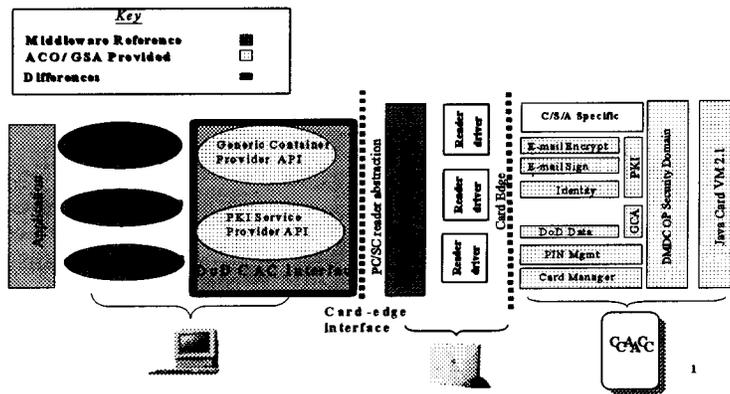
For the CAC Architecture, Service Provider modules are denoted as the CAC Cryptographic Middleware and CAC DoD Data Middleware (Exhibit 1.0 depicts the modules). They shall support the following:

Supported Functionality	Type of CAC Middleware Modules
Digital Signature and Verification, Encryption and Decryption, Secure Authentication, & Certificate-Based Log-on	CAC Cryptographic Middleware
Read/Write DoD Data	CAC DoD Data API

In addition to the middleware modules, it is required to provide bundled with the Cryptographic Middleware modules the capability for users to manage their CACs. This will be in the form of an application or utility capable of viewing all PKI credentials on the CAC, registering PKI credentials within the client OS or browsers, and allowing user PIN changes.

It is strongly recommended that the Cryptographic Middleware be digitally signed in order to facilitate the digital verification of the Cryptographic Middleware upon each invocation. This will provide a higher level of assurance in the integrity of the Cryptographic Middleware. Exhibit 1.0 depicts CAC architecture for this middleware procurement.

**Exhibit 1.0 CAC Middleware Architectural Illustration**



**2.1 Client Workstation Operating Environments**

Since there is an array of different DoD-approved workstation operating systems, there may be a necessity for separate software packages for each operating environment. Each potential software package is required to meet all of the requirements detailed in this document.

Below is a list of targeted platforms to be supported by CAC Release 1.0 middleware. Vendors may submit products supporting any of the operating systems below. However, each product will be separately tested in accordance with Section 4 of this specification with the cost for each test borne by the vendor.

- Windows (95b, NT 4.0 native mode SP4 or higher, Windows 2000)
- Linux 6.0 (or greater)
- HP-UX 11.x-12.x
- Solaris 2.51, 2.6, 7, and 8
- RedHat Linux 6.2
- MAC OS 8.0 (or greater)

### **2.1.1 Client Workstation Resource Utilization**

Below are the resource utilization parameters for all CAC middleware modules. Each middleware module shall separately meet these requirements.

1. The maximum disk space required for CAC middleware installation on a client workstation shall not exceed 30 Mbytes and, for a server, shall not exceed 100 Mbytes.
2. The CAC middleware shall function properly on a client workstation configuration equivalent to a 133 MHz minimum Pentium-compatible CPU with a minimum of 32 MB RAM.
3. When installed on a system equivalent to a 133 MHz Pentium-compatible CPU with 32 Mbytes of RAM, the processing time consumed by the CAC Middleware shall not exceed 10% (ten percent) of the overall time required for an application to access information on the CAC.

### **2.1.2 Session Management-Maintain Best Practice**

In commercial smart card environments the solution provided to customers has tended to be single-vendor centric. The DoD envisions that multiple 'middleware' products of varying functionality may be present on a single client at the same time. For instance, a fully featured COTS middleware product may be handling the desktop functions of encrypt /decrypt / and digitally sign while an additional 'application specific' product may be interfacing to service specific (i.e. ARMY or NAVY) data that is kept in a separate security domain on the card.

Middleware vendors are required to work in this environment and provide concise error handling in their middleware product. Additionally, as these multi-vendor products may be operating in tandem, vendors shall exhibit care when caching of data on the client to prevent errors or properly handle error returns. This functionality will be included in qualification testing and specific strengths and weakness shall be annotated in each vendor's product grade when certification testing is accomplished.

All external user interface processes of supplied Middleware modules shall be compatible with, support, and not interfere with the accessibility (FAR Subpart 39.2) features of the operating system in which they are installed.

## **2.2 Multiple Applet Identification (AID)**

The DoD is in process of registering Department specific Application Identifiers (AIDs) for all DoD owned and licensed applets. As an interim measure, middleware vendors must be aware that for some period there may be two AIDs for the same applet. The application information container, which contains the AIDs of all the applets on the card, should be the first place the middleware should look on the card for the applet AIDs. An alternative would be for the middleware to read from configuration data to get the AIDs. This would allow for AID changes, if necessary, as a temporary fix and help avoid re-issuing of middleware due to coding changes.

The ability for the middleware to handle these conditions is necessary for now until a firm distinction can be made between AIDs and the middleware that interacts with the applets. This will help avoid issues concerning the same applet with different AIDs.

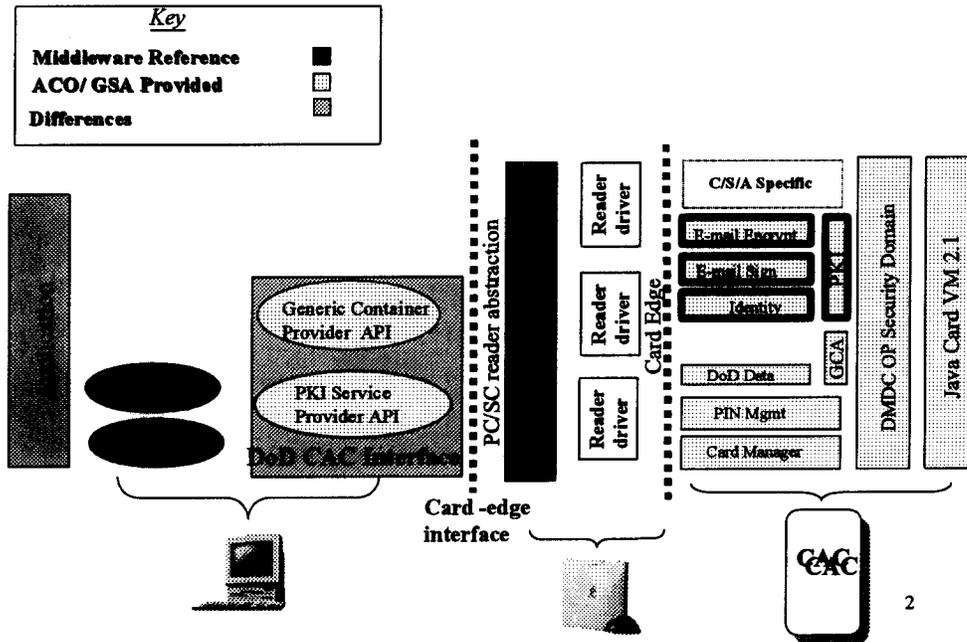
## **3 Supporting Middleware Modules**

### **3.1 CAC Cryptographic Middleware**

This module provides the necessary "glue" to get the DoD PKI credentials residing on the CAC to operate. It encapsulates access to cryptographic functionality provided by the CAC through high level programming interfaces. It exposes the CAC cryptographic functions to PKI applications running on a client workstation. Exhibit 2.0 lays out the CAC Cryptographic Middleware within the CAC Architecture.

As a matter of policy, the middleware will not be permitted to provide any additional crypto function or utility in the areas of initializing key material, injecting key material, re-keying, etc. The DoD reserves the right to provide the function of locking the card (upon three incorrect PIN entries) and unlocking the card at the RAPIDS stations. These functions are not the purview of commercial middleware packages. Questions concerning this policy may be forwarded to the Access Card office.

### ***Exhibit 2.0 CAC Cryptographic Middleware Illustration***



### 3.1.1 Cryptographic Requirements

The table below outlines requirements for CAC cryptographic middleware:

Requirements	Applicability
<p>Implement both Public Key Cryptography Standards (PKCS #11) and Microsoft Cryptographic Service Provider (CSP). This can be implemented within single or separate modules.</p> <p>The PKCS#11 (CSP) implementation shall support all the calls required to support the following mechanisms:</p> <ul style="list-style-type: none"> <li>▪ RSA mechanisms (12.1)</li> <li>▪ DSA mechanisms (12.2)</li> <li>▪ Triple-Length DES (12.19)</li> <li>▪ SHA-1 mechanisms (12.26)</li> </ul> <p>* - All CALLs as part of all functions for the above mechanisms must be supported.</p>	X

Requirements	Applicability
<p>The Microsoft CryptoAPI (CSP) implementation shall support all the APIs defined in the following groups:</p> <ul style="list-style-type: none"> <li>▪ Base Cryptography functions</li> <li>▪ Certificate &amp; certificate store functions</li> <li>▪ Certificate verification functions</li> <li>▪ Auxiliary functions                             <ul style="list-style-type: none"> <li>- Data management functions</li> <li>- Data Conversions functions</li> <li>- OID functions</li> </ul> </li> </ul> <p>* - All CALLs are to be supported for all the above functions.</p>	X
<p>Implement modules in accordance with the "CAC Developer's Kit v2.0"</p>	X
<p>Shall implement utilizing the cryptographic services defined in the "CAC Developer's Kit v2.0"</p>	X
<p>Shall operate with PS/SC smart card readers and driver components for all devices. Optionally, it shall operate with PC/SC (M.U.S.C.L.E) and OCF smart card readers and driver components for Java OS, Unix, Linux, and Macintosh operating environments</p>	X
<p>Shall implement secure channel in accordance with Global Platform 2.0 or higher</p>	X
<p>Shall be able to handle multiple context or sessions within the same module in accordance with Section 2.2.2. Specifically it shall:</p> <ul style="list-style-type: none"> <li>• Provide services to insure that an application's transaction sequence with the CAC is not disrupted by other applications running on the user's workstation. These services are typically provided by LOCK and UNLOCK functions that can be utilized by a calling application to prevent other applications from making calls to the card that might change the currently selected applet or the values of card internal data. Upper middleware layers (like the PKCS #11 and MS CSP layers) must insure that applications do not abnormally terminate when calls are made that find the card to be unavailable because of another application's use of the LOCK functionality.</li> </ul>	X

Requirements	Applicability
<p>Middleware must provide single sign-on support for smart card PIN verification. Prior to requesting a PIN from the user, the middleware must first perform the VerifyPIN command to the card with no (cont) PIN data to check if the PIN has already been verified. It is recognized that this requirement will not guarantee single sign-on functionality as an application may prompt the user for a PIN before interacting with the middleware.</p>	<p>X</p>

### 3.1.2 Card Management Utility Requirements

The CAC cryptographic middleware will have bundled with it a client workstation application or utility capable of managing the CAC. The below table outlines the requirements:

Requirements	Applicability
<p>Shall have the capability to manage the card by:</p> <ul style="list-style-type: none"> <li>• Displaying (read only – PIN not required) the utility version number.</li> <li>• Requiring PIN entry to access any services from the card except for card identification information</li> <li>• Allowing the user the capability to change their PIN.</li> <li>• The Cryptographic Middleware may provide a PIN CHANGE UTILITY. However, the utility will be required to enforce the DoD PIN Policy of a 6-8 digit numeric PIN. Utility will allow the user to change his PIN by submitting his current PIN and then providing a new PIN. Note that any resulting PIN must be in a six to eight digit numeric format.</li> <li>• Not allowing user any other write access to the card</li> </ul>	<p>X</p>
<p>Shall have the capability to manage the card's certificates. It shall:</p> <ul style="list-style-type: none"> <li>• Require PIN entry to access any service from the card except for card identification information <ul style="list-style-type: none"> <li>□ Provide for migration, display (read only), and deletion of certificates (and pointers to keys) to program's registry, client browser, client messaging system, or operating system on the client workstation</li> </ul> </li> <li>• Display (read only) a list of certificates on the card, including unique name and expiration date.</li> </ul>	<p>X</p>

Requirements	Applicability
<ul style="list-style-type: none"> <li>• Display (read only) certificate data.</li> </ul>	
Shall have the capability to manage the (cont) cryptographic middleware. It shall: <ul style="list-style-type: none"> <li>• Display (read only – PIN not required) the middleware version number.</li> <li>• Have the capability to manage parameters (if any) required by the middleware – PIN not required, e.g.,                             <ul style="list-style-type: none"> <li>□ Port assignments for the reader</li> <li>□ Timeout periods.</li> <li>□ And other configuration parameters.</li> </ul> </li> </ul>	X
Shall have the capability to display help information. It shall: <ul style="list-style-type: none"> <li>• Provide a description of all functions, from a user standpoint, provided by the utility.</li> <li>• Provide a description of all functions, from a user standpoint, provided by the middleware.</li> <li>• Provide a trouble shooting tutorial from a user standpoint.</li> </ul>	X

### 3.2 CAC DoD Data Middleware

This module provides the necessary “glue” to get the DoD data elements residing on the CAC to operate. It 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. Exhibit 3.0 lays out the CAC DoD Data Middleware within the CAC Architecture.

CAC DoD data refers to those data elements residing on the CAC that are centrally managed by the Department of Defense. These elements will be stored in a specific container(s) in which the CAC Data Middleware will access to read and write.

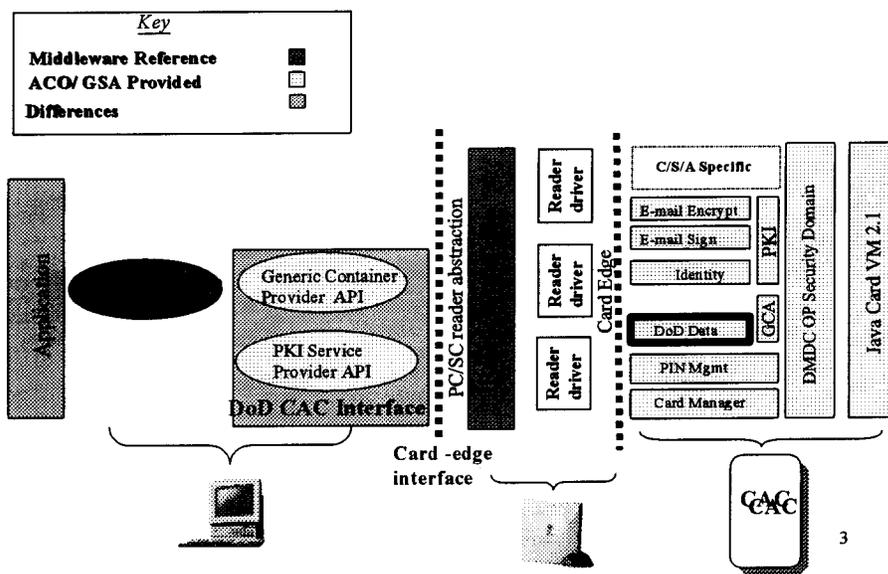
#### 3.2.1 DoD Data Requirements

The below table outlines the requirements for CAC DoD Data middleware:

Requirements	Applicability
Shall be implemented in accordance with PC/SC and/or OCF for service providers	X
Implement modules in accordance with the “CAC Developer’s Kit v2.0”	X
Shall implement utilizing the generic container API defined in the “CAC Developer’s Kit v2.0”	X
Shall operate with PC/SC smart card readers and driver components for all devices. Optionally, it	X

Requirements	Applicability
shall operate with PC/SC (M.U.S.C.L.E) and OCF smart card readers and driver components for Java OS, Unix, Linux, and Macintosh operating environments	
<p>Shall be able to handle multiple context or sessions within the same module in accordance with Section 2.2.2. Specifically it shall:</p> <ul style="list-style-type: none"> <li>• Provide services to insure that an application's transaction sequence with the CAC is not disrupted by other applications running on the user's workstation. These services are typically provided by LOCK and UNLOCK functions that can be utilized by a calling application to prevent other applications from making calls to the card that might change the currently selected applet or the values of card internal data. Upper middleware layers must insure that applications do not abnormally terminate when calls are made that find the card to be unavailable because of another application's use of the LOCK functionality.</li> </ul>	X

**Exhibit 3.0 CAC DoD Data Middleware Illustration**



### 3.3 Credential Interoperability

Middleware vendors were invited to a meeting at DMDC-WEST on 30 May 2001 to discuss how to accommodate the different proprietary formats used by multiple vendors to store USERNAME /PASSWORD/ and PROPRIETARY POINTER DATA on the CAC. At that time, a short-term solution was discussed that allows all vendors to use the existing card space (now used by ActivCard for the RAPIDS Verifying Officers (VOs)) to support their middleware. This short-term solution is specified below.

Middleware vendors will require 'scratch pad' space to store specific data to enable their product to operate. Presently, this 'scratch pad' space is utilized to support the VO Function for the RAPIDS Workstation. By agreement of the Smart Card Senior Coordinating Group (SCSCG), this space is open to all vendors for use as long as a backup and restore function is available to allow use of multiple middleware packages. The current RAPIDS client middleware does possess a backup utility to maintain VO functionality in the multi-vendor environment. This function will be tested with other offerings to insure compliance. In order to use the space that can be backed up and restored, a vendor needs to know the Applet Identifier (AID) of the containers specified storage containers. The following AIDs are provided:

AID	TYPE	Documented Use
• A0000000790300	ID PIN	Management Applet
• A0000000790100	PKI ID	Private Key
• A0000000790101	PKI	E-Mail Signature Key
• A0000000790102	PKI	E-Mail Decryption Key
• A0000000790200	Generic	Employee
• A0000000790201	Generic	Personnel
• A0000000790202	Generic	Benefits
• A0000000790203	Generic	XBenefits(not currently used)
• A00000007902FB	Generic	Certificate Information
• A00000007902FD	Generic	Credentials
• A00000007902FE	Generic	Certificate Container (contains certificates associated with PKI applet instances)
• A0000000791201	Generic	"Backward Compatibility" - administrative
• A0000000791202	Generic	"Backward Compatibility" - medical

Associated Access Control Rights (ACR) data is available in the GSA Card Edge Specification. Space allocated is 1.6 Kbytes.

### 3.4 Answer to Reset (ATR) Discovery and Handling

When new card types and manufacturers are implemented by the DoD, products must accommodate updates to the CAC's Answer to Reset (ATR) commands as

well as any card specific interfaces for middleware operation. It is expected that, as new CAC platforms are certified and approved, middleware products must be capable of seamlessly incorporating new ATRs and card specific attributes in a timely manner. Vendors must minimally provide a website download distribution mechanism available to DoD customers (at no charge) to maintain the operation of CAC cards regardless of card vendor or model. Additional mechanisms beyond the web site download are encouraged.

## **4 Middleware and Reader Qualification Testing**

### ***4.1 Qualification Process Background***

All middleware candidates will be required to pass a functionality test process in order to certify their products as DoD "Common Access Card Compliant". The Joint Interoperability Test Command (JITC) at Indian Head, Maryland, will administer this qualification process.

This test facility will also be available for vendors of reader products. They may also have JITC test their products and be certified to work with each CAC version as well as with each middleware product.

**Vendors may be required to pay for this testing and to provide the test facility with a single copy of the product that they wish to qualify. The products tested will continue to be utilized in the test bed for both regression and interoperability testing as long as the product versions are in either government or commercial inventory.**

The contact at JITC for testing information is:

Mr. Kevin Holmes  
Phone: (301) 744-2763  
Email: holmesk@ncr.disa.mil

### ***4.2 Testing Procedures***

Testing will certify that middleware products are capable of providing the following services as a base requirement:

1. Encrypt email via DoD PKI Certificates
2. Decrypt email via DoD PKI Certificates
3. Digitally sign email and documents
4. Verify digitally signed email and documents
5. Provide for PIN change in accordance with NSA regulations (6-8 digit numeric only)
6. Access, read and provide to applications the DoD data container. Validation will be accomplished by a DMDC application that can view all DoD data written to the card.

These services will be required to work with the following commercially-based products:

Products	Encrypt/Decrypt	Digitally Sign/Verify
Microsoft Outlook (Version 2000)	x	x
Microsoft Internet Explorer (Version 5.5-128 bit)	x	x
Netscape Navigator (Version 4.73)	x	x
Microsoft Word (Version 2000)	x	x

The initial set of readers will be chosen from a subset of the readers initially found compatible with the DoD CAC from the National Security Agency Reader Test Report dated, 14 March 2001. However, the base set of standards for readers that will be functionality certified is that they must be PC/SC compliant with both drivers and hardware meeting PC/SC qualification standards.

**JITC will use the Reader/Middleware baseline established during development and developmental testing as the initial baseline. Once JITC tests a vendor's product and ACO approves it for use, it will become part of the baseline. JITC will test future products against the baseline that includes all ACO approved vendor products.**

The current card set that will be compliant with initial testing will consist of the following card stock:

1. Oberthur GalactIC 2.1-5032 Mask 2.1R
2. Schlumberger Cyberflex Access 32K CAC (M256EPALP1\_SI\_9C\_02 Softmask 7 Version 2

Vendors may contact the Access Card Office (ACO) for test cards that are representative of both products. The POC at the ACO is:

Mr. Michael Butler  
 DMDC/ACO  
 Phone: 703-696-7395  
 Email: Butlertmp@osd.pentagon.mil

## 4.2.1 Description of Test

Test will consist of 'round robin' testing of each vendors product against the base set of CAC functions, the base set of applications, chosen readers, and the card stock in question. If the card accomplishes each of the tasks in the testing requirement list with all mandated products, the middleware product (or reader) shall be posted for DoD customer's information in choosing a product.

Upon completion of the basic functionality test described above, the products shall be tested for any other functionality within the product. The feature set shall be documented as additional features for customer information and the fact that the extended features of any product do not interfere with the core functions (tested above) shall be noted.

Final testing shall be Middleware Interoperability. In this case, each middleware package shall be tested against any previously functioning products to insure that there is interoperability between the products. If there are problems in shifting between middleware products, then the test shall document the impacts to the user of any incompatibilities.

## Appendix A: References

<i>Referenced Documents</i>				
<i>No.</i>	<i>Title</i>	<i>Rev.</i>	<i>Date</i>	<i>Internet Web Address</i>
1.	CAC Release 1.0 ICC Requirements	v1.1	2/08/2001	<a href="http://www.dmdc.osd.mil/smartcard/images/CACRelease1ICCRequirementsv1.pdf">http://www.dmdc.osd.mil/smartcard/images/CACRelease1ICCRequirementsv1.pdf</a>
2.	CAC Release 1.0 Reader Specification	v1.0	9/25/2000	<a href="http://www.dmdc.osd.mil/smartcard/images/CACRelease1ReaderSpecificationv1Specification.pdf">http://www.dmdc.osd.mil/smartcard/images/CACRelease1ReaderSpecificationv1Specification.pdf</a>
3	Public Key Cryptography Standards	-	-	<a href="http://www.rsasecurity.com/rsalabs/pkcs/">www.rsasecurity.com/rsalabs/pkcs/</a>
4	Microsoft Cryptographic Service Provider	-	-	<a href="http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/cryptcsp/aboutcsp_54rj.htm">http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/cryptcsp/aboutcsp_54rj.htm</a>
5.	GSA Interoperability Specification	V1.0	8/29/2000	<a href="http://www.dmdc.osd.mil/smartcard/images/GSAinteroperabilitySpecification.pdf">http://www.dmdc.osd.mil/smartcard/images/GSAinteroperabilitySpecification.pdf</a>
6.	CAC Developer Kit	v2.0	-	<a href="http://www.dmdc.osd.mil/smartcard/owa/ShowPage?p=CACDEVELOPERSKIT">http://www.dmdc.osd.mil/smartcard/owa/ShowPage?p=CACDEVELOPERSKIT</a>
7.	CAC Application Programming Interface		11/08/2000	<a href="http://www.dmdc.osd.mil/smartcard/images/CACApplicationProgrammingInterface.pdf">http://www.dmdc.osd.mil/smartcard/images/CACApplicationProgrammingInterface.pdf</a>
8.	IATF – Defense-in-Depth Strategy for IA	Rel3.0	09/2000	<a href="http://www.iaatf.net">www.iaatf.net</a>
9.	NSTISSP #11 National Information Assurance Acquisition Policy	Rel1.0	01/2000	<a href="http://www.nstissc.gov">www.nstissc.gov</a>

## Appendix B: Glossary of Acronyms

ACO	Access Card Office
ACR	Access Control Rights
AID	Application Identifier
ALU	Application Load Unit
APDU	Application Protocol Data Unit
API	Application Programming Interface
BSI	Basic Services 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
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSPI	Cryptographic Service Provider Interface
Component	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
GINA	Graphical Identification and Authentication
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)
IFD	Interface Device
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunications Union
I&RTS	Integration & Runtime Specification
JCE	Java Cryptographic Extensions
JDK	Java Developer's Kit
JITC	Joint Interoperability Test Command
JORD	Joint Operational Requirements Document
JS-API	Java Security-Application Programming Interface
JTA	Joint Technical Architecture
KEA	Key Exchange Algorithm
KMS	Key Management System
LAN	Local Area Network
LCS	Life Cycle Support
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MARC	Multi-application Reader Card
MIME	Multipurpose Internet Mail Extensions
MSCSP	Microsoft Cryptographic Service Provider
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
M.U.S.C.L.E.	Movement for the Use of Smart Cards in a Linux Environment ( <a href="http://www.linuxnet.com">www.linuxnet.com</a> )
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
OID	Object Identifier
O&M	Operations and Maintenance
OPTF	Open Platform Terminal Framework
OS	Operating System
PC	Personal Computer
PC/SC	Personal Computer/Smart Card. Refers to interoperability Specification for ICCs and Personal Computer Systems, Part 1 through 8, Release 1.0 and Release 2.0 (Draft).
PCMCIA	Personal Computer Memory Card international Association
PIN	Personal Identification Number
PK	Public Key
PKCS	Public Key Certificate Standards
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POM	Program Objectives Memorandum
QPL	Qualified Product List
RA	Registration Authority
R&D	Research and Development
R&M	Reliability and Maintainability
RAM	Random Access Memory

<b>RAPIDS</b>	<b>Real-Time Automated Personnel Identification System</b>
<b>RDBMS</b>	<b>Relational Database Management System</b>
<b>ROM</b>	<b>Read Only Memory</b>
<b>R/A/M</b>	<b>Reliability, Availability, and Maintainability</b>
<b>S/A</b>	<b>Service or Agency</b>
<b>SBU</b>	<b>Sensitive But Unclassified</b>
<b>SCSCG</b>	<b>Smart Card Senior Coordinating Group</b>
<b>SCSUG</b>	<b>Smart Card Security User Group</b>
<b>S/MIME</b>	<b>Secure/Multipurpose Internet Mail Extensions</b>
<b>SP</b>	<b>Service Provider</b>
<b>SPS</b>	<b>Service Provider Software</b>
<b>SSN</b>	<b>Social Security Number</b>
<b>S/W</b>	<b>Software</b>
<b>TAFIM</b>	<b>Technical Architecture Framework for Information Management</b>
<b>TPDU</b>	<b>Transmission Protocol Data Unit</b>
<b>TTP</b>	<b>Trusted Third Party</b>
<b>TTS</b>	<b>Target Token Strategy</b>
<b>UI</b>	<b>User Interface</b>
<b>US</b>	<b>United States</b>
<b>USB</b>	<b>Universal Serial Bus</b>
<b>VO</b>	<b>Verifying Official</b>
<b>VM</b>	<b>Virtual Machine</b>
<b>WAN</b>	<b>Wide Area Network</b>
<b>WG</b>	<b>Working Group</b>

## Appendix C: 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 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) that causes it 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.