



DEFENSE INFORMATION SYSTEMS AGENCY

**JOINT INTEROPERABILITY TEST COMMAND
INDIAN HEAD, MARYLAND**



**DEPARTMENT OF
DEFENSE COMMON
ACCESS CARD SPYRUS
MIDDLEWARE TEST
REPORT CARD**

SEPTEMBER 2002

SPYRUS MIDDLEWARE TEST REPORT CARD

Spyrus Rosetta CSI Middleware version 4.0.017 was tested on Windows 2000, Windows NT 4.0 and Windows 95. Testers used three different smart cards to test the middleware; Oberthur GalactiC 2.1-5032 Mask 2.1R, Schlumberger Cyberflex Access 32K CAC (M256EPALP1_SI_9C_02) Softmask 7 Version 2 and the Oberthur Cosmopolic V4.

The below table outlines the requirements met by the Spyrus Rosetta CSI Middleware version 4.0.017.

Table 1. SPYRUS TEST REPORT CARD

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET
MANDATORY		
<p>1. Service Provider(s) shall use the system services provided by the ICC Resource Manager.</p>	<p>a. Shall successfully track installed IFDs and make this information accessible to other applications.</p> <p>b. Shall successfully track known ICC types, along with their associated SP and supported Interfaces, and make this information available to other applications.</p> <p>c. Shall successfully track ICC insertion and removal events to maintain accurate information on available ICCs within the IFDs.</p> <p>d. Shall successfully control the allocation of IFD resources.</p> <p>e. Shall successfully support transaction primitives on access to services available within a given ICC</p>	<p>All Met</p>
<p>2. Service Provider modules are denoted as the DOD CAC Cryptographic Middleware and DOD CAC DOD Data Middleware.</p>	<p>They shall support the following:</p> <p>a. DOD CAC Cryptographic Middleware:</p> <ol style="list-style-type: none"> 1. Shall successfully support Digital Signature and Verification, 2. Shall successfully support Encryption and Decryption, 3. Shall successfully support Secure Authentication, & Certificate-Based Log-on <p>b. DOD CAC DOD Data API:</p> <ol style="list-style-type: none"> 1. Shall successfully support the Read/Write function to DOD Data 	<p>All Met</p>

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET
3. The Middleware is required to provide bundled with the Cryptographic Middleware modules the capability for users to manage their DOD CACs.	a. Shall provide an application or utility capable of viewing all PKI credentials on the DOD CAC, registering PKI credentials within the client OS or browsers, and allowing user PIN changes.	All Met
4. The workstation resource utilization middleware module shall separately meet these requirements.	a. Shall assure the maximum disk space required for DOD CAC middleware installation on a client workstation does not exceed 30 Mbytes and, for a server, shall not exceed 100 Mbytes.	All Met
5. Session Management is required to Maintain Best Practice	<p>a. Shall successfully maintain the DOD vision that multiple 'middleware' products of varying functionality may be present on a single client at the same time. Therefore Middleware vendors are required to work in this environment and provide concise error handling in their middleware product.</p> <p>b. Shall successfully support these multi-vendor products operating in tandem. Vendors shall exhibit care when DOD CACHing data on the client to prevent errors or properly handle error returns.</p> <p>c. 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.</p>	All Met
6. 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.	<p>a. Shall successfully use the application information container, which contains the AIDs of all the applets on the card, as 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.</p> <p>b. Shall successfully support the ability for the middleware to handle these conditions since it is necessary for now until a firm distinction can be made between AIDs and the middleware that interacts with the applets.</p>	All Met
7. 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.	<p>a. Shall successfully 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>1. The PKCS#11 (CSP) implementation shall support all the calls required to support the following mechanisms:</p> <ul style="list-style-type: none"> a. RSA mechanisms (12.1) b. DSA mechanisms (12.2) c. Triple-Length DES 	All Met

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET
	<p>(12.19) d. SHA-1 mechanisms (12.26)</p> <p>* All CALLs as part of all functions for the above mechanisms must be supported.</p> <p>2. The Microsoft CryptoAPI (CSP) implementation shall support all the APIs defined in the following groups: Base Cryptography functions</p> <p>a. Certificate & certificate store functions b. Certificate verification functions c. Auxiliary functions</p> <ul style="list-style-type: none"> • Data management functions • Data Conversions functions • OID functions <p>* All CALLs are to be supported for all the above functions.</p> <p>b. Shall successfully implement modules in accordance with the "DOD CAC Developer's Kit v2.0"</p> <p>c. Shall successfully implement utilizing the cryptographic services defined in the "DOD CAC Developer's Kit v2.0"</p> <p>d. Shall successfully 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> <p>e. Shall successfully implement secure channel in accordance with Global Platform 2.0 or higher</p> <p>f. Shall be able to handle multiple context or sessions within the same module in accordance with Requirement 6. Specifically it shall: Provide services to insure that an application's transaction sequence with the DOD CAC is not disrupted by other applications running on the user's</p>	

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET
	<p>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.</p> <p>g. Shall provide single sign-on support for smart card PIN verification by middleware. Prior to requesting a PIN from the user, the middleware must first perform the VerifyPIN command to the card with no 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>8. The DOD CAC cryptographic middleware will have bundled with it a client workstation application or utility capable of managing the DOD CAC.</p>	<p>a. Shall have the capability to manage the card by:</p> <ol style="list-style-type: none"> 1. Displaying (read only – PIN not required) the utility version number. 2. Requiring PIN entry to access any services from the card except for card identification information 3. Allowing the user the capability to change their PIN. 4. The Cryptographic Middleware may provide a PIN CHANGE UTILITY. However, the utility will be required to enforce the DOD PIN Policy of a six to eight 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. 5. Not allowing user any other write access to the card <p>b. Shall have the capability to manage the card's certificates. It shall:</p> <ol style="list-style-type: none"> 1. Require PIN entry to access any service from the card except for card identification information <ol style="list-style-type: none"> a. Provide for migration, display (read only), and 	<p>All Met</p>

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET
	<p>deletion of certificates (and pointers to keys) to program's registry, client browser, client messaging system, or operating system on the client workstation</p> <ol style="list-style-type: none"> 2. Display (read only) a list of certificates on the card, including unique name and expiration date. <ol style="list-style-type: none"> a. Display (read only) certificate data. <p>c. Shall have the capability to manage the cryptographic middleware. It shall:</p> <ol style="list-style-type: none"> 1. Display (read only – PIN not required) the middleware version number. 2. Have the capability to manage parameters (if any) required by the middleware – PIN not required, e.g., <ol style="list-style-type: none"> a. Port assignments for the reader b. Timeout periods. <p>e. Shall have the capability to display help information. It shall:</p> <ol style="list-style-type: none"> 1. Provide a description of all functions, from a user standpoint, provided by the utility. 2. Provide a description of all functions, from a user standpoint, provided by the middleware. 3. Provide a trouble shooting tutorial from a user standpoint. 	
<p>9. This module provides the necessary "glue" to get the DOD data elements residing on the DOD CAC to operate. It is responsible for exposing high-level interfaces to <i>non-cryptographic</i> services that include common interfaces to a DOD CAC as well as access to file and authentication services.</p>	<ol style="list-style-type: none"> a. Shall successfully be implemented in accordance with PC/SC and/or OCF for service providers b. Shall successfully implement modules in accordance with the "DOD CAC Developer's Kit v2.0" c. Shall successfully implement utilizing the generic container API defined in the "DOD CAC Developer's Kit v2.0" d. Shall successfully operate with PC/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>All Met</p>

REQUIREMENT	MEASURE OF SUCCESS	MET/NOT MET		
	<p>e. Shall successfully be able to handle multiple context or sessions within the same module in accordance with requirement 6. Specifically it shall: Provide services to insure that an application's transaction sequence with the DOD 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.</p>			
<p>10. A list of targeted platforms to be supported by DOD CAC Release 1.0 middleware:</p> <p>Note: The middleware product must clearly identify which operating system it supports. A middleware product may support one or more of these platform, but is not required to support all operating systems.</p>	<p>Windows 95b Windows NT 4.0 (beginning with native mode SP 4) 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)</p>	<p>Met on the following OS's; Windows 95b Windows NT 4.0 (beginning with native mode SP 4) and Windows 2000.</p>		
<p>LEGEND:</p> <table border="0"> <tr> <td data-bbox="186 1123 803 1375"> <p>AID – Application Identifiers API – Application Programming Interface CAC – Common Access card CSP – Cryptographic Service Provider DES – Data Encryption Standard DOD – Department of Defense FAR - Federal Acquisition Regulation HP-UX – Hewlett Packard - Unix ICC –Integrated Circuit Chip IFD – Interface Device MAC - Macintosh Mbytes – Mega Bytes MS – Microsoft MUSCLE – Movement for the Use of Smart Cards in a Linux Environment</p> </td> <td data-bbox="820 1123 1429 1375"> <p>NT – New Technology OCF – Open Card Framework OS – Operating System PC/SC – Personal Computer/Smart Card PIN – Personnel Identification Number PKCS – Public Key Cryptography Standards PKI – Public Key Infrastructure RAPIDS – Real-Time Automated Personnel Identification System RSA - Rivest, Shamir, & Adleman (public key encryption technology) SHA - Secure Hash Algorithm SP – Service Pack V - Version</p> </td> </tr> </table>			<p>AID – Application Identifiers API – Application Programming Interface CAC – Common Access card CSP – Cryptographic Service Provider DES – Data Encryption Standard DOD – Department of Defense FAR - Federal Acquisition Regulation HP-UX – Hewlett Packard - Unix ICC –Integrated Circuit Chip IFD – Interface Device MAC - Macintosh Mbytes – Mega Bytes MS – Microsoft MUSCLE – Movement for the Use of Smart Cards in a Linux Environment</p>	<p>NT – New Technology OCF – Open Card Framework OS – Operating System PC/SC – Personal Computer/Smart Card PIN – Personnel Identification Number PKCS – Public Key Cryptography Standards PKI – Public Key Infrastructure RAPIDS – Real-Time Automated Personnel Identification System RSA - Rivest, Shamir, & Adleman (public key encryption technology) SHA - Secure Hash Algorithm SP – Service Pack V - Version</p>
<p>AID – Application Identifiers API – Application Programming Interface CAC – Common Access card CSP – Cryptographic Service Provider DES – Data Encryption Standard DOD – Department of Defense FAR - Federal Acquisition Regulation HP-UX – Hewlett Packard - Unix ICC –Integrated Circuit Chip IFD – Interface Device MAC - Macintosh Mbytes – Mega Bytes MS – Microsoft MUSCLE – Movement for the Use of Smart Cards in a Linux Environment</p>	<p>NT – New Technology OCF – Open Card Framework OS – Operating System PC/SC – Personal Computer/Smart Card PIN – Personnel Identification Number PKCS – Public Key Cryptography Standards PKI – Public Key Infrastructure RAPIDS – Real-Time Automated Personnel Identification System RSA - Rivest, Shamir, & Adleman (public key encryption technology) SHA - Secure Hash Algorithm SP – Service Pack V - Version</p>			

NOTE: The procurement will be executed under the auspices of the Department of Defense (DOD) Enterprise Software Initiative to establish an Enterprise Software Agreement for use by all Services and Components within DOD. Test card issuance is accomplished via the DOD Real Time Automated Personnel Identification System (RAPIDS).

TEST EQUIPMENT CONFIGURATION

Table 2. Test Equipment Configuration

Client Configuration	Pentium III, 1GHz, 256 MB RAM, 40 GB Hard Drive		
Server Configuration	Pentium 4, 1.7 GHz, 512 MB RAM, 40 GB Hard Drive		
<p>LEGEND:</p> <table border="0"> <tr> <td data-bbox="297 1837 803 1873"> <p>GHz - Gigahertz GB - Gigabyte</p> </td> <td data-bbox="820 1837 1307 1873"> <p>MB - Megabyte RAM – Random Access Memory</p> </td> </tr> </table>		<p>GHz - Gigahertz GB - Gigabyte</p>	<p>MB - Megabyte RAM – Random Access Memory</p>
<p>GHz - Gigahertz GB - Gigabyte</p>	<p>MB - Megabyte RAM – Random Access Memory</p>		