Draft Middleware Specification

Version X.X
MM/DD/YYYY

Contents

1. Introduction

1.1. Background

Relevant Agency smart card program background information.

1.2. Purpose

The Middleware Requirements Specification is intended to define the standard set of services, interfaces and configuration options that must be implemented by all middleware operating in the Agency and to define the environments that must be supported. Additionally, this specification identifies recommended and optional capabilities that middleware providers should consider implementing to differentiate their products and provide added value.

1.3. Audience

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

1.4. Document Scope

This specification applies to middleware that operates on personal computer desktops.

This document is related to one other related Agency document.

- *Agency Connection Guidance* -Provides technical details and Agency best practices for managing smart card connections and card state.

1.5. Document Objectives

The objective of this document is to provide unambiguous, clear, and testable requirements for middleware vendors.

1.6. Assumptions and Constraints

Each Agency will execute middleware acquisitions using processes and procedures available to that organization. It is expected that this document will serve as the centerpiece of the acquisition and it is expected additional requirements (such as technical support or unique capabilities) will be specified by each Agency in Section 6.

1.7. Abbreviations

BSI	Basic Services Interface
CSP	Cryptographic Service Provider
P11	Public Key Cryptography Standard #11

2. Middleware Background

2.1. Middleware Definitions

Middleware is defined as the software application that serves as the interface between host applications (such as email) and the smart card.

Functionally, middleware provides access to cryptographic services, smart card data, and smart card management features.

Cryptographic Services
Cryptographic services are the set of functions necessary for cryptographic operations, such as signing and encrypting an email. Middleware provides cryptographic services through three standards-based interfaces, MSCAPI, P11, and BSI.

Smart Card Data
Smart Card Data is defined as data which resides on the smart card, but is not related to cryptographic functionality. Personnel identification number or blood type may be examples of smart card data. Smart card data is accessed through the BSI, or by middleware directly.

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

3. Middleware Specifications

3.1. Requirements Structure

3.1.1. Core Agency

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

Core Agency requirements are listed in section 4.

3.1.2. Optional

Optional requirements are those in which a Agency mandate isn't an appropriate approach. The majority of these requirements will be based on each individual purchaser's preference and or unique circumstances. A good example of an optional requirement is an installation package—Service A may require an MSI file, while Command "B" will require a Tivoli package.

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

Optional requirements are listed in section 5.

3.1.3. Agency

Service specific requirements will be identified in section 6.

4. Core Agendy Requirements

4.1. PKI Requirements

4.1.1. CSP

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

4.1.1.2. Middleware shall provide a smart card compliant CSP, as documented in Smart Card CSP Notes, available from the http://download.microsoft.com/download/win2000pro/Utility/V2.0/W98NT42KMe/EN-US/cspdk.exe website

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

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

4.1.2. P11

4.1.2.1. Middleware shall support PKCS#11 functions listed in Appendix C, P11 Functions

4.1.2.2. Vendor shall provide a list of all unsupported P11 functions.

4.1.3. BSI Requirements

4.1.3.1. Middleware shall provide a BSI implementation consistent with the specifications and requirements listed in Appendix D.

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

4.2. Agency Smart Card

4.2.1. Minimum Supported Smart Card Types:

4.2.1.1. Oberthur GalactIC 2.1-5032 Mask 2.1R

4.2.1.2. Schlumberger Cyberflex Access 32K smart card (M256EPALP1_SI_9C_02 Softmask 7 Version 2)

4.2.1.3. Oberthur CosmopolIC V4

4.2.2. New Smart Card Types

4.2.2.1. Middleware vendor shall provide support for the ability to utilize future card types as issued for the smart card program.

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

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

4.2.3. Card Applets

4.2.3.1. Middleware shall support all Agency Smart Card applets. (e.g. ID applet, Generic Container Applets, PKI Applets, PIN Management Applets, Access Control Applets, and all other future and present Agency applets).

4.2.4. Certificates

4.2.4.1. Middleware shall support all X.509 issued certificates.

4.2.4.2. Middleware shall support Agency PKI policy and certificates.

4.2.4.3. Middleware shall process and use certificates for PK services in accordance with key usage and key extension policies.

4.3. Middleware Operating Environment

4.3.1. Operating System Requirements

Middleware shall operate with the following operating systems:

Operating Systems Supported by Middleware		
Windows NT	Windows 2000	Windows XP Professional

4.4. Card Readers

4.4.1. Middleware shall operate and comply with PC/SC and the Agency Smart Card Reader Specification.

4.5. Application Support

4.5.1. Email

4.5.1.1. The middleware shall provide cryptographic services to the e- mail application and operating system combinations as listed in Appendix A, Figure 5, Primary Email and OS Combinations to: Sign, decrypt, and encrypt e-mail messages and Sign, decrypt, and encrypt e-mail messages with attachments.

4.5.2. Cryptographic Logon

4.5.2.1. The middleware shall have the ability to use any appropriate Agency certificate to perform a cryptographic authentication for the following operating systems: Windows 2000, Windows XP, Windows XP Pro. .

4.5.2.2. The middleware shall have the capability to enumerate through all certificates on the smart card to determine the correct certificate and key pair for certificate based access control.

4.5.2.3. Middleware shall not require the use of persistent storage (either on smart card or on disk) of login configuration information in order for cryptographic logon capability to function.

4.5.3. Client Authentication

4.5.3.1. The middleware shall provide the ability to initiate an SSL V3 client-side authentication for the operating system and browser combinations listed in on the web server applications listed in Appendix A, Figure 4, Web Servers.

4.6. GUI

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

4.6.1.2. Middleware shall place an icon in the system tray for indicating middleware activity and launching the middleware graphical interface.

4.6.1.3. Middleware shall only display features that are configurable for the middleware environment.

4.7. Middleware Resource Parameters

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

4.7.2. The smart card 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.

4.7.3. When installed on a system equivalent to a 133 MHz Pentium-compatible CPU with 32 Mbytes of RAM, the processing time consumed by the smart card middleware shall not exceed 10% (ten percent) of the system's total resources at rest.

4.8. Middleware Installation

4.8.1. Middleware shall not install card reader drivers.

4.8.2. Middleware shall install regardless if a reader driver is previously installed on the workstation.

4.8.3. Middleware shall indicate to the end user of the limited functionality imposed by installation of middleware without a reader attached.

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

4.8.5. Middleware shall not remove any registry settings or files that are shared by other applications or not wholly linked to vendor-specific functionality. For example, if a middleware package upgrades the browser's crypto strength to 128 bit, they would not remove it because it is shared by other non-middleware applications.

4.9. Middleware Configuration

4.9.1. Middleware shall have the ability to enable or disable all configurable settings for the end user at time of installation.

4.9.2. Middleware configuration settings shall be set and configured in accordance with Appendix A, Figures 1,2,3

4.9.3. Middleware shall provide an option to automatically register (or make available for use) all user certificates stored on the smart card in both Netscape and Explorer environments.

4.9.4. Middleware shall provide an option to remove smart card certificates from workstation on card removal events.

4.9.5. Middleware shall register Agency certificate chain during installation for both Netscape and Explorer environments.

4.10. PIN Management

4.10.1. PIN Services

4.10.1.1. Middleware shall provide a single PIN service which will have the ability to handle PIN management for both MS-CAPI and P11 interfaces. For example, if a user enters a PIN for use with MS-CAPI, and then uses the P11 interface within the specified PIN timeout

period, the user should not have to re-enter the PIN since the same PIN service would handle the PIN requirements for both P11 and MS-CAPI modules.

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

4.10.1.3. Middleware shall have the ability to disable all PIN timeout features.

4.10.1.4. PIN Timeout configurations shall be configured and maintained in accordance with Appendix A, Figure 3.

4.10.2. PIN Change

4.10.2.1. Middleware shall have the ability to change PINs after the end user has entered the correct PIN.

4.10.2.2. Middleware shall not allow PIN change without a valid PIN entry.

4.10.2.3. Middleware shall require the end user to verify the new PIN before submitting the PIN change request to the smart card.

4.10.3. PIN Validation

4.10.3.1. Middleware shall require all new PINS to no less than 6 and no greater than 8 numerics in length.

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

4.10.3.3. In the event an invalid PIN is entered, the Middleware shall notify the user of the violation.

4.11. Compliance with Smart Card Connection and State Guidance

4.11.1. To the extent possible, Middleware shall follow the best practices and guidance provided in the *Smart Card Connection Guidance* document.

4.12. Documentation

4.12.1. End User Documentation

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

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

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

4.12.1.4. Help documentation shall be searchable.

4.12.1.5. Help documentation shall have a table of contents.

4.12.1.6. Help documentation shall be indexed.

4.12.1.7. Middleware shall provide a "Read Me" document that describes any known bugs or compatibility issues.

4.12.1.8. Help topics shall not include features or functionality not included in the middleware.

4.12.2. Administrator Documentation

4.12.2.1. Vendor shall provide online documentation as to the setup, installation and configuration of the middleware.

4.12.2.2. Middleware vendors shall provide online documentation as to the location, name, and values of all registry keys used in option configuration settings.

4.12.2.3. Middleware vendors shall provide a complete and detailed list of all changes, additions, updates, or deletions made to an end user workstation after installation.

4.12.2.4. Middleware vendors shall provide a complete list of any artifacts or upgrades left after an uninstall.

4.12.2.5. Vendor shall provide documentation for any application or utilities included in the middleware.

4.12.2.6. For supported third party installation products, middleware shall provide administrator documentation for using such products.

4.12.3. BSI Documentation for Application Developers

4.12.3.1. Vendor shall provide documentation that would aid application developers in the use of their BSI library.

4.12.3.2. Vendor shall provide a sample application, with source code, which demonstrates the use of their BSI library.

4.12.3.3. The sample application shall include the use of at least one function from each of the three sections of the BSI (utility, storage, and cryptographic).

4.12.3.4. Java, Visual Basic and C language versions of the sample application shall be provided.

4.13. Process Descriptions

4.13.1. Middleware Functions

4.13.1.1. The middleware vendor shall provide, in detail, a flow chart or other descriptive material describing their cryptographic logon implementation. This material shall describe, at a minimum, how the appropriate certificate is identified and used during the cryptographic login process.

4.13.1.2. The middleware vendor shall provide, in detail, a flow chart or other descriptive material describing their card authentication (PIN) time-out implementation.

4.13.1.3. For any feature or functionality not required by this document, the vendor shall provide a detailed list of those features, how they are used, and their benefit to the Agency.

4.14. Use of Scratch Pad Space

4.14.1. Middleware shall fulfill all core Agency middleware requirements without using the smart card for middleware-specific data storage.

4.14.2. Middleware shall not write or modify any middleware-specific data in any GCA container on the smart card to meet core middleware requirements

4.14.3. Middleware shall not depend on CCF data to function.

4.15. Support

4.15.1. Tech Support

4.15.1.1. Middleware shall readily display workstation and middleware configuration information in a manner readily available to the end user. At a minimum, including browser version, operating system, patch level, crypto strength, and P11/CSP library versions and .dll name when available.

4.15.2. Middleware Updates

4.15.2.1. Middleware shall have an automated mechanism to update the middleware. Vendor must provide, in detail, the mechanism(s) used to update the middleware for supporting new card types, bug fixes, and service releases. Attention should be paid to reducing Agency's cost exposure, technology requirements, ease of use, and security concerns.

5. Optional Requirements

5.1. General

5.1.1.1. Middleware vendor may provide a listing of other applications that can utilize the smart card PKI services. Areas of interest to the Agency are, but not limited to VPN, PKE (e.g. DTS), and thin client environments.

5.1.1.2. Middleware may provide a utility or other method for building custom installation images for the middleware for both initial installation and maintenance.

5.1.1.3. Middleware may provide advanced installation features that support COTS enterprise management products.

5.1.1.4. Middleware shall operate at a minimum with all other smart card types supported and/or manufactured by that vendor. Middleware may optionally support card types from other vendors.

5.1.1.5. Middleware may optionally provide a visual indication of smart card activity.

5.2. Middleware Operating Environment

5.2.1. Middleware may optionally provide support for the following operating systems: Linux, Solaris, Apple OS.

5.2.2. The middleware may provide cryptographic services to the email application and operating system combinations as listed in Appendix A, Figure 6, Secondary Email and OS Combinations to sign, decrypt, and encrypt e-mail messages and sign, decrypt, and encrypt e-mail messages with attachments.

5.2.3. For the email applications listed in Appendix A, Figure 5, Primary Email and OS Combinations, and Appendix A, Figure 6, Secondary Email and OS Combinations, middleware may optionally configure the email client for use of PKI services.

5.2.4. Middleware may optionally provide cryptographic authentication to other Network Operating Systems..

5.3. Middleware Configuration

5.3.1. The middleware may provide a means to manipulate the configuration values from a single middleware user interface.

5.4. PIN Services

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

5.4.2. Middleware may provide the ability for applications to "opt out" of the CAM mechanism

5.5. Documentation

5.5.1. Middleware vendor may provide a detailed listing of 3rd party or industry certifications.

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

5.6. Support

5.6.1. Tech Support

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

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

5.6.1.3. Middleware may provide a hyperlink to a vendor middleware product support website.

5.6.2. Vendor Support

5.6.2.1. Vendor may provide 24 hour written response to level 1 level 2 bugs, as categorized in Appendix A Figure 7, Bug Classifications.

5.6.2.2. Vendor may provide a fix for level 1 and level 2 bugs within 5 business days of notification or submit a formal request for waiver with justification during this time period.

5.6.2.3. Vendor may cooperate with the Agency on the timing and functionality of service releases.

5.6.2.4. Vendor may provide 180 day middleware EOL notice.

5.6.2.5. Vendor may provide support for 1 year after product End of Life.

5.6.2.6. Support for new card types may be considered routine middleware maintenance.

5.6.2.7. New card type support may be provided no later than 90 days from the date the vendor receives a request from the Agency.

5.6.2.8. Support for new smart card applets may be considered routine maintenance.

5.6.2.9. Support for applet changes may be provided no later than 90 days after the vendor receives a request from the Agency.

5.6.2.10. Vendor may optionally provide a shared bug tracking environment with the Agency.

5.6.2.11. Vendor may release from time to time service releases to improve performance, increase functionality, or fix level 3 and below bugs.

5.6.2.12. Future Enhancements

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

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

6. Agency

{THIS SECTION WILL BE COMPLETED AT EACH INDIVIDUAL ACQUISITION]

Appendix A

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

Figure 1 Configurable Options

Certificate Registration Key			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration]			
Key Values	**Type**	**Setting**	**Default Setting**
AutoReg	REG_DWORD	0x00000000 (Feature is off) **-OR-** 0x00000001 (Feature is on)	0x00000001
AutoUnRegOnLogoff	REG_DWORD	0x00000000 (do not un-register on logoff) **-OR-** 0x00000001 (un-register on logoff)	0x00000000
AutoUnRegOnRemove	REG_DWORD	0x00000000 (do not un-register on card removal) **-OR-** 0x00000001 (un-register on card removal)	0x00000000
Setting Description			
AutoReg	If turned off, middleware will not register the smart card certificates. If on, the middleware will register the certificates		
AutoUnRegOnLogoff	Middleware will/ will not unregister certificates on the logoff event		
AutoUnRegOnRemove	Middleware will / will not unregister certificates on card removal event		
Example			
[HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Cryptography\Certificate Registration] "AutoReg"=dword:00000001 "AutoUnRegOnLogoff"=dword:00000001 "AutoUnRegOnRemove"=dword:00000000			

Figure 2

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

Figure 3

Web Servers and Browsers			
OS	**MS IIS**	**Netscape iPlanet**	**Apache**
95b	5.5	5.5	5.5
98	5.5, 4.76	5.5, 4.76	5.5, 4.76
NT	5.5, 4.76	5.5, 4.76	5.5, 4.76
W2K	5.5, 4.76	5.5, 4.76	5.5, 4.76
XP	6.0, 4.76	6.0, 4.76	6.0, 4.76
6.0= MS Internet Explorer 6.0, 5.5=MS Internet Explorer 5.5, 4.76=Netscape Navigator 4.76 w/PSM 1.4*			

Figure 4

* Note: Support for the Netscape Navigator is optional, but may be required for certain acquisitions which involve RA/LRA support or where other requirements necessitate the use of Netscape Navigator.

Primary Email OS Combinations				
Operating System	**Email Clients**			
	Outlook 98	Outlook 2K SP2	Outlook 2002	Outlook XP
Windows NT		X		
Windows 2000		X	X	X
Windows XP		X	X	X

Primary E-mail and OS Combinations
Figure 5

Secondary Email OS Combinations				
Operating System	**Email Clients**			
	Outlook 98	Outlook 2K SP2	Outlook 2002	Outlook XP
95b	X			
98	X			

Secondary Email and OS Combinations
Figure 6

Middleware Bug Classifications	
The Agency Shall be the sole determinant of middleware bug classifications.	
Category	Definition
1- Critical	The failure causes a system crash or unrecoverable data loss or jeopardizes personnel.
2- High	The failure causes impairment of critical system functions and no work around solution exists.
3- Medium	The failure causes impairment of critical system functions, though a work around solution does exist.
4- Low Required	The failure causes inconvenience or annoyance.
5- Low Desired	None of the above, or the anomaly concerns an enhancement rather than a failure.

Bug Classifications
Figure 7

Appendix B- CSP Functions

Appendix C- P11 Functions

Appendix D- BSI Functions

Appendix E- BSI Header Files