DEPARTMENT OF DEFENSE
HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
DoD CENTER MONTEREY BAY • 400 GIGLING ROAD
SEASIDE, CALIFORNIA 93955-6771

To: DoD Identity Protection and Management Senior Coordinating Group (IPMSCG) Test and Evaluation Work Group (TEWG)

From: Defense Manpower Data Center (DMDC)

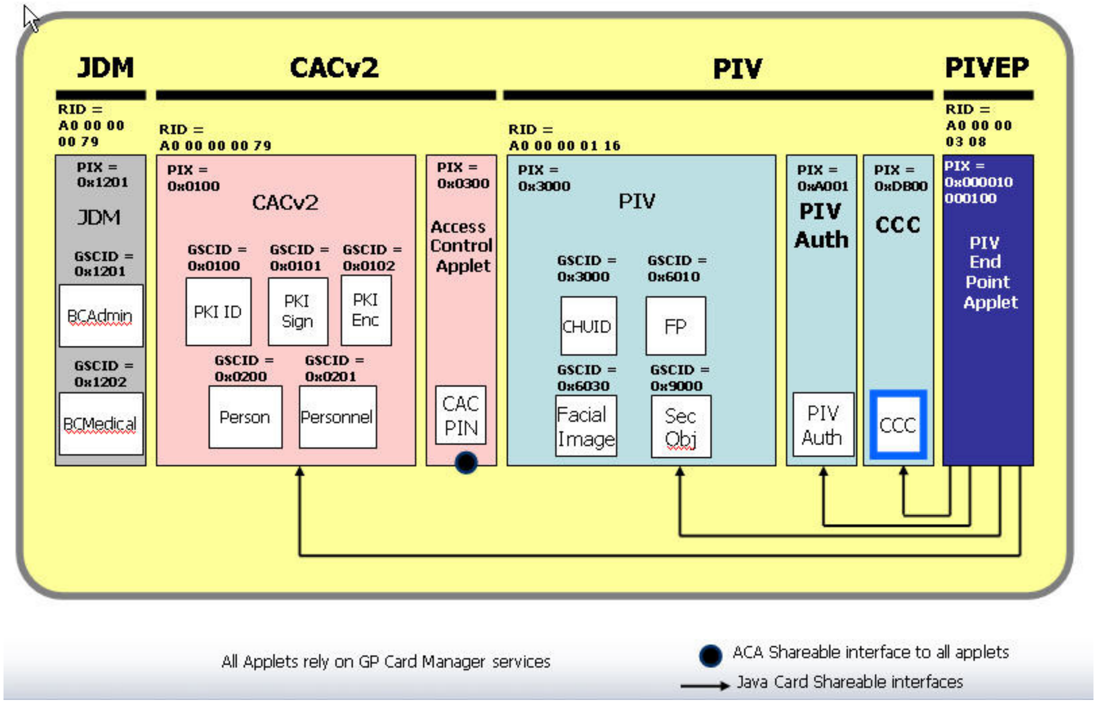
Date: February 13, 2009

Re: Technical Bulletin: CAC Data Model Change in 144K Dual Interface Cards

1.0 Introduction

This memo advises you of changes in the CAC data model in the upcoming 144K dual interface cards, namely the Gemalto TOP DL GX4 FIPS 144K and Oberthur ID-One Cosmo 128 D v5.5. Starting with these cards, the “New Consolidated PIV+CACv2 Data Model” will be used. This change in the CAC data model should not impact any applications that are compliant with NIST Government Smart Card Interoperability Specifications (GSC-IS) v2.1 (also known as NIST Regulation 6887) and NIST SP800-73-1.

The following diagram and table describe the “New Consolidated PIV+CACv2 Data Model”.



Application Name	AID	OID	Description
ACA	A0000000790300	0300	Access Control Applet
CCC	A000000116DB00	DB00	Card Capability Container
PIV	A0000001163000	3000	CHUID
		6010	Fingerprints
		6030	Facial Image
		9000	Security Object
PIV Authentication Key	A000000116A001	A001	PIV Authentication Key
CACv2	A0000000790100	0100	Identity Key
		0101	Digital Signature Key
		0102	Key Management Key
		0200	DoD Person
		0201	DoD Personnel
JDM	A0000000791201	1201	BCAdmin
		1202	BCMedical
PIV EP	A000000308000010000100		PIV EP

NOTE: *Refer to the “Appendix A – Existing CAC PIV Data Model” to assist in the comparison between the “Existing CAC PIV Data Model” and the “New Consolidated PIV+CACv2 Data Model”.*

2.0 Justifications of the Data Model Change

The “New Consolidated PIV+CACv2 Data Model” has been introduced for the following reasons:

- Provides better performance at issuance to mitigate the impact of larger keys (e.g. RSA 2048bits)
- RSA 2048-bits End-Entity Keys Support
    - PIV Authentication Key
    - PIV Digital Signature Key
    - PIV Key Management Key
    - CAC Identity Key
- Leverage NIST GSC-IS v2.1 and NIST SP800-73-1
- Data Model Simplification

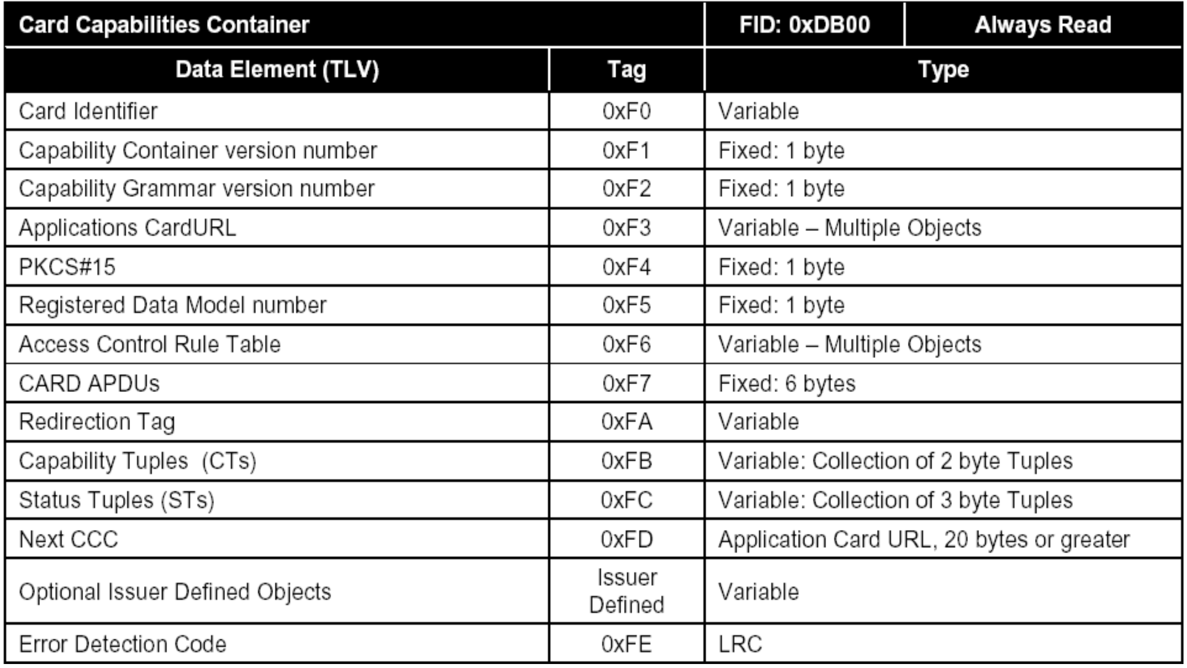
- EOL of the CACv1 card edge (per Director DMDC Memo, “Obsolescing Legacy CAC Interfaces—Technical Notification,” 5 February 2008)

- Efficient use of the RAM in the upcoming 144K dual interface cards

- Consistency with the FIPS 201 part 3 PIV container structure and access

The “New Consolidated PIV+CACv2 Data Model is strictly compliant with NIST GSC-IS v2.1 specifications. In this specification, it introduces the concept of CCC (Card Capability Container) which is used for card discovery by the applications communicating to the CAC. Reading the CCC is a required operation for all NIST GSC-IS v2.1 compliant applications.

The CCC container is one of the mandatory containers in the NIST GSC-IS v2.1 and NIST SP800-73-1. The following table is an overview of the CCC content extracted from the NIST GSC-IS v2.1. The table represents the default content of the CCC.



<table>
<tr><th colspan="2">Card Capabilities Container</th><th>FID: 0xDB00</th><th>Always Read</th></tr>
<tr><th>Data Element (TLV)</th><th>Tag</th><th colspan="2">Type</th></tr>
<tr><td>Card Identifier</td><td>0xF0</td><td colspan="2">Variable</td></tr>
<tr><td>Capability Container version number</td><td>0xF1</td><td colspan="2">Fixed: 1 byte</td></tr>
<tr><td>Capability Grammar version number</td><td>0xF2</td><td colspan="2">Fixed: 1 byte</td></tr>
<tr><td>Applications CardURL</td><td>0xF3</td><td colspan="2">Variable – Multiple Objects</td></tr>
<tr><td>PKCS#15</td><td>0xF4</td><td colspan="2">Fixed: 1 byte</td></tr>
<tr><td>Registered Data Model number</td><td>0xF5</td><td colspan="2">Fixed: 1 byte</td></tr>
<tr><td>Access Control Rule Table</td><td>0xF6</td><td colspan="2">Variable – Multiple Objects</td></tr>
<tr><td>CARD APDUs</td><td>0xF7</td><td colspan="2">Fixed: 6 bytes</td></tr>
<tr><td>Redirection Tag</td><td>0xFA</td><td colspan="2">Variable</td></tr>
<tr><td>Capability Tuples (CTs)</td><td>0xFB</td><td colspan="2">Variable: Collection of 2 byte Tuples</td></tr>
<tr><td>Status Tuples (STs)</td><td>0xFC</td><td colspan="2">Variable: Collection of 3 byte Tuples</td></tr>
<tr><td>Next CCC</td><td>0xFD</td><td colspan="2">Application Card URL, 20 bytes or greater</td></tr>
<tr><td>Optional Issuer Defined Objects</td><td>Issuer Defined</td><td colspan="2">Variable</td></tr>
<tr><td>Error Detection Code</td><td>0xFE</td><td colspan="2">LRC</td></tr>
</table>

This container is free-access for reading and can be read via **Read Buffer** APDU (as per NIST GSC-IS v2.1). Vendors who develop applications for the CAC 144K, only two CCC-fields are really of interest:

1. Card Capability Container version number and

2. Applications CardURL.

Both the Card Capability Container version number and Applications CardURL must be read and controlled. The field, Applications CardURL, describe how the association scheme between Application ID (Instance ID) and Card Object ID (OID) is encoded in the CAC.

2.1 Card Capability Version Number (Tag 0xF1)

Version data is stored in Compact BCD (Binary Coded Decimal) format, e.g., version 2.1 (major version 2, minor version 1) is stored as a single byte value = 0x21.

***NOTE**: If this field does not equal to 0x21, then the CCC container is invalid and must not be analyzed further.*

2.2 Applications CardURL (Tag 0xF3)

The Applications CardURL consists of multiple Simple-TLV structures, one for each GSC-IS container in the ICC card. This field is assigned with tag value 0xF3. Each single structure contains the following fields as specified in NIST GSC-IS v2.1:

- 5-byte GSC-RID: A0.00.00.01.16 (Hex) for the GSC-IS Data Model or A0.00.00.00.79 (Hex) for the CAC Data Model.
- 1-byte Card Application Type: 01 (Hex) for Generic Containers, 04 (Hex) for PKI, 02 (Hex) for SKI.
- 2-byte Object ID: The unique OID for each container object (key objects, generic container object, etc.).
- 2-byte Application ID: The unique ID for the container application, combined with the RID to create the applet 7-byte AID. These 2 bytes are the 2 last bytes of the Applet Instance containing the object.
- Access Profile, not used here, value is 00 (Hex).
- 5-bytes for the PIN ID (1 byte) + Access Key Info (4 bytes) are not used in this card configuration, and so are set to nulls (00 Hex).

While analyzing the Application CardURL, the calling application knows how the objects are organized in the card memory and where to access them. This field must be read by any NIST GSC-IS v2.1 compliant application in order to find out the card layout and where the CAC objects are located.

3.0 Example of the Card Capability Container for the "New Consolidated PIV+CACv2 Data Model"

The following table lists the content of the Card Capability Container for the "New Consolidated PIV+CACv2 Data Model":

Card Capability Container		**FID: 0xDB 00**	**Always Read**
Data Element (TLV)	**Tag**	**Bytes (Hex)**	**Content (Hex)**
Card Identifier	0xF0	01	<<variable>>
Capability Container version number	0xF1	01	21
Capability Grammar version number	0xF2	01	21
Application CardURL	0xF3	10	A0 00 00 00 79 01 02 00 01 00 00 00 00 00 00 00

	0xF3	10	A0 00 00 00 79 01 02 01 01 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 00 79 04 01 00 01 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 00 79 04 01 01 01 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 00 79 04 01 02 01 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 01 16 01 30 00 30 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 01 16 01 60 10 30 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 01 16 01 60 30 30 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 01 16 01 90 00 30 00 00 00 00 00 00 00
	0xF3	10	A0 00 00 00 79 01 12 01 12 01 00 00 00 00 00 00
	0xF3	10	A0 00 00 00 79 01 12 02 12 01 00 00 00 00 00 00
	0xF3	10	A0 00 00 01 16 04 A0 01 A0 01 00 00 00 00 00 00
PKCS#15	0xF4	01	00
Registered Data Model number	0xF5	01	10
Access Control Rule Table	0xF6	11	07 A0 00 00 00 79 03 00 00 00 00 00 00 00 00 00 00
CARD APDUs	0xF7	00	
Redirection Tag	0xFA	00	
Capability Tuples (CTs)	0xFB	00	
Status Tuples (STs)	0xFC	00	
Next CCC	0xFD	00	
Error Detection Code	0xFE	00	

4.0 Impact of the Data Model Change

- For CAC enabled applications that leverage the NIST GSC-IS 2.1 CCC, there is no impact. Additional, for CAC enabled applications that send raw APDU commands to the CAC and are compliant with NIST GSC-IS 2.1, there is no impact.

- For CAC enabled applications that interface with the CAC using BSI (NIST GSC-IS 2.1), Microsoft CSP, PIV (NIST SP800-73-1) or PKCS#11 using NIST GSC-IS 2.1/PIV EP strictly compliant middleware, there is no impact. (ActivIdentity ActivClient 6.x is GSC-IS 2.1 compliant)

- If your application continues to read the containers the same way as on a CAC v1, the following containers are impacted in the "New Consolidated PIV+CACv2 Data Model":

- DoD Demographic Containers
    - Person
    - Personnel
- JDM
    - BCMedical
- CAC PKI Keys
    - CAC PKI Digital Signature Key
    - CAC PKI Key Management Key

NOTE: *The containers above will require two selects to access the specific container for all non-compliant NIST GSC-IS 2.1 applications using raw APDU commands to communicate to the CAC (refer to procedures below for details).*

- For CAC enabled applications that use NIST GSC-IS v2.1 **NOT** strictly compliant middleware **OR** CAC enabled applications that are **NOT** compliant with NIST GSC-IS v2.1 (e.g. applications that sends raw APDU commands and do not follow GSC-IS v2.1 to discover applications in the CAC), there is an impact. The following procedure demonstrates how to mitigate this impact:

  To access a container in the "New Consolidated PIV+CACv2 Data Model" (e.g. DoD Person container):

    1. **Select and read the CCC applet instance (0xA0.00.00.01.16.DB.00) after smartcard power-on *(new)***
    2. **Read the "Applications CardURL" in the CCC to locate the AID and OID of the container, such as the DoD Person Container *(new)***
    3. **Select the AID of the Applet Instance (0xA0.00.00.00.79.01.00) containing the DoD Person Container *(new)***
    4. **Select the OID of the container, such as the DoD Person Container (02.00) *(new)***
    5. Read the Applet Properties
    6. Extract T-Buffer and V-Buffer Max Length
    7. Read content of T-Buffer
    8. Read content of V-Buffer

  NOTE: *The example above applies to accessing any container that is grouped within a single applet instance.*

5.0 Impact of EOL of the CACv1 Card Edge

- For CAC enabled application that use NIST GSC-IS v1.7 (CACv1), the following APDU commands have changed in NIST GSC-IS v2.1:

- GET PROPERTIES APDU

  - In GSC-IS v1.7 (CACv1), P1 value is 0x00. In GSC-IS v2.1, P1=0x00 is rejected since P1 can be either 0x01 or 0x02.

- GET CERTIFICATE APDU is no longer supported in GSC-IS v2.1; thus, READ BUFFER should be used.

- EXTERNAL AUTHENTICATE command format has changed in GSC-IS v2.1

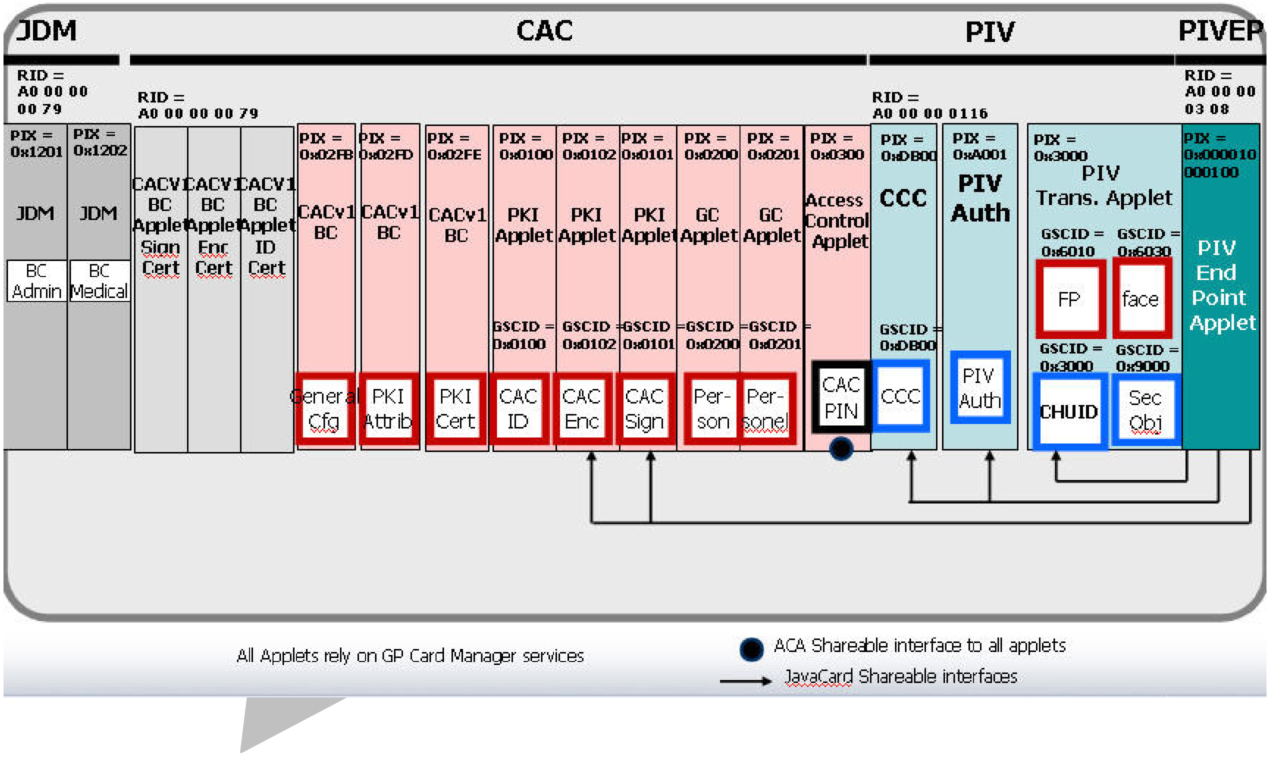
  - INS=0x42 for GSC-IS v1.7 (CACv1)

  - INS= 0x82 for GSC-IS v2.1

Appendix A – Existing CAC PIV EP Data Model

The following diagram and table describe the “Existing CAC PIV EP Data Model” which is deployed in the following card platforms:

- Gemalto (GemCombiXpresso R4) 72K dual interface card
- Oberthur ID-One Cosmo 64K v5.2D dual interface card



Application Name	AID	OID	Description
ACA	A0000000790300	0300	Access Control Applet
CCC	A000000116DB00	DB00	Card Capability Container
PIV	A0000001163000	3000	CHUID
		6010	Fingerprints
		6030	Facial Image
		9000	Security Object
PIV Authentication Key	A000000116A001	A001	PIV Authentication Key

CACv2 PKI Identity Key	A0000000790100	0100	Identity Key
CACv2 PKI Digital Signature Key	A0000000790101	0101	Digital Signature Key
CACv2 PKI Key Management Key	A0000000790102	0102	Key Management Key
CACv1 PKI Attributes	A00000007902FD	02FD	CACv1 PKI Certificate Attributes
CACv1 PKI Certificates	A00000007902FE	02FE	CACv1 PKI Certificates
CACv1 General Configuration	A00000007902FB	02FB	CACv1 General Configuration
CACv1 PKI Identity Key	A00000007901F0	01F0	Re-directs to CACv2 PKI Identity Key
CACv1 PKI Digital Signature Key	A00000007901F1	01F1	Re-directs to CACv2 PKI Digital Signature Key
CACv1 PKI Key Management Key	A00000007901F2	01F2	Re-directs to CACv2 PKI Key Management Key
DoD Demographic	A0000000790200	0200	DoD Person
DoD Demographic	A0000000790201	0201	DoD Personnel
JDM	A0000000791201	1201	BCAdmin
JDM	A0000000791202	1202	BCMedical
PIV EP	A000000308000010000100		PIV EP

Question or comment

Please submit any questions or comments to cacsupport@osd.pentagon.mil