

**“BEYOND FLASH VALUE”
A USER’S QUICK GUIDE TO USING THE CAC**

DON eBusiness Operations Office

20 October 2003

“BEYOND FLASH VALUE” – A USER’S QUICK GUIDE TO USING THE CAC

1. PURPOSE: The purpose of this document is to provide a quick technology reference to the Department of Defense (DOD) Common Access Card (CAC) for customers who are considering using it for more than its basic “flash value” as an ID card.

The CAC is coming into widespread use throughout the Department of the Navy (DON) and the rest of DOD. The most obvious usage, at least initially, is a “Flash” ID card for access into most DOD installations and/or controlled areas. Because the CAC contains various technologies—also referred to as media—that can be used to simplify a wide range of business processes, the potential of the CAC is far greater than that of a simple “Flash” ID card.

This paper is intended to be a layman's document, to give to interested parties some basic CAC information. We will include pointers on where to go to get more detailed information if needed, for all the media on the CAC.

2. TARGET AUDIENCE: WHO ARE THE “CUSTOMERS?” By the term “customers”, we mean:

- People who currently have (or will be issued) the CAC. This population includes uniformed service members (to include Selected Reserve), civilian employees, and designated contractors.
- Vendors who are interested in selling to the Department commercial products that interface with the CAC, such as smart card readers, magnetic stripe readers for physical security or financial applications, bar code readers, Integrated Circuit Chips (ICC), etc.

3. WHAT IS THE CAC? The CAC is a DOD-level initiative. Dr. John Hamre, then Deputy Secretary of Defense, initially kicked it off in November 1999. Since then, DOD has published DOD Directive 8901.3, Smart Card Technology, 31 Aug 2002, to formally establish DOD policy and responsibilities for the CAC program. The key elements of the policy are that Smart Card technology will take the form of a Department-wide Common Access Card (CAC) that will be used in three key ways, as:

- The standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DOD civilian employees, eligible contractor personnel, and eligible foreign nationals.
- The Department's primary platform for the Public Key Infrastructure (PKI) authentication token used to access DOD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment.

- The principal card enabling physical access to buildings, facilities, installations, and controlled spaces.

NOTE: This policy does not require DOD Components to dismantle immediately current access systems, or preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC (e.g., such as entrance into a Sensitive Compartmentalized Information Facility (SCIF) or other high security space). However, the Heads of the DOD Components are to plan for migration to the CAC for general access control using the CAC's present or future access control capabilities.

So...the CAC is really three things: an ID card, a logical access token, and a physical access token.

4. WHAT'S ON THE CAC? The CAC is a Smart Card. That is, it is a credit card-size device, for carrying and use by personnel, which contains an integrated circuit chip, or ICC. The current ICC is read through contact with a card reader device and is used for the storage of information, applications, and Public Key Infrastructure (PKI) certificates. A summary of the various technologies and media on the CAC is as follows:

- Photograph and printed text (both sides of CAC)
- Integrated Circuit Chip (ICC) (front)
- Linear (Code 39) Bar Code (back)
- 2-dimensional (PDF 417) Bar Code (front)
- Magnetic Stripe (back)

During the issuance process specific data elements are printed on the CAC (Appendix A) and encoded on the ICC (Appendix B), Code 39 bar code (Appendix C), and PDF 417 bar code (Appendix D). These data elements are shown in tables at Appendices A thru E, respectively. The magnetic stripe is left blank at issuance but can be encoded using a generic magnetic stripe-encoding device, post issuance.

Paragraph 7 below explores each of these technologies in more detail: what is it, what information is contained in it, do you need a reader and where do you get one, how do you use it, where do you go to get more detailed information, etc.

NOTE: As with any technology, CAC technologies will evolve over time. Next-generation CACs **may** contain contactless ICCs and/or radio frequency (RF) transmitters (both of which can be read from a short distance without physical insertion in to a contact reader). In addition, biometric information (such as fingerprints) may be stored on the ICC in the future. Note that the fingerprint that is currently taken at time of CAC issuance is stored back in the master Defense Eligibility Enrollment Reporting System (DEERS) and is not stored on the CAC itself.

5. WHAT ABOUT NMCI AND PKI? NMCI is the Navy-Marine Corps Intranet, which “will establish a standardized end-to-end system for voice, video and data communications for all civilian and military personnel within the Department of the Navy.” For the user, the immediate change will be a new desktop computer, to include training, maintenance, operation and infrastructure, with access to standardized networks.

The CAC will be used to perform secure logon to the NMCI network using the DOD Public Key Infrastructure (PKI). By PKI we mean the framework and services that provide the generation, production, distribution, control, accounting, record keeping, and destruction of private key pairs for authentication, electronic signature, and encryption/decryption.

In a nutshell, the CAC is the hardware token that contains the member’s three Public Key Infrastructure (PKI) keys:

- Identity Certificate: Identifies you to network devices and applications such as web servers and system domains. The corresponding private key to your ID certificate is used to digitally sign DOD documents and verify your identity to networks and applications, which facilitates authentication, non-repudiation, and non e-mail digital signature.
- E-mail Signature Certificate: Contains your public key that is used to verify the digital signature on e-mail messages. Your corresponding private key is used to digitally sign your e-mail, which facilitates authentication, non-repudiation, and e-mail digital signatures.
- E-mail Encryption Certificate: Contains your public key, used by others to encrypt e-mail. Your corresponding private key is used to decrypt e-mail and any attachments, which facilitates greater security and confidentiality.

The Navy-wide CAC issuance schedule is designed to have mass issuance lead NMCI implementation at any given site. That way, users will already have their PKI token in hand, in the form of their CAC, when they get their new NMCI desktop workstation. That workstation will come equipped with a smart card reader (either integrated or stand-alone, and the middleware necessary to read the PKI certificates on the CAC.

Any command not participating in the NMCI cutover should contact CNO N614 to obtain guidance for card reader devices and middleware. Note that the term *middleware* is used to describe separate products that serve as the glue between two applications. Middleware, as it pertains to the CAC, is used to allow communication between the CAC and an application. It is, therefore, distinct from [import](#) and [export](#) features that may be built into one of the applications.

6. WHO IS IN CHARGE?

At the DOD level, the Access Card Office (DOD ACO) owns the CAC program. Their web site contains a wealth of information and can be reached at <http://www.dmdc.osd.mil/smartcard>

The Department of the Navy eBusiness Operations Office (eBUSOPSOFF), located at Mechanicsburg, PA, has been designated the responsible office for CAC implementation throughout the Department of the Navy. Our web site is <http://www.don-ebusiness.navsup.navy.mil>. We have two primary focus areas:

- Initial issuance of the CAC to all eligible service members, civilian employees, and eligible contractors.
- Facilitating and fostering expanded usage of the CAC as an enabling tool to improve business processes within the Department.

The eBUSOPSOFF website provides a wealth of CAC-related information, plus information about the rest of the eBUSOPSOFF mission. One key area allows the user to view information concerning pilot projects: we have some pilots relating to the CAC that are currently under consideration, already in the pilot process, or pilots completed.

7. BEYOND BASIC “FLASH VALUE”...A GUIDE TO USING EACH OF THE MEDIA ON THE CAC.

7.1. DON User wants to use the Magnetic Stripe.

- *Common applications:* Physical security is the most common application that uses the magnetic stripe, typically “swipe” readers used to unlock doors. This media was placed on the CAC to support legacy access control applications so that in certain instances the CAC could be used to replace a separate magnetic stripe badge. The magnetic stripe contains 3 tracks; the access control encoding is done on Track 2, which is the same track used by the banking industry for financial applications, such as your debit card or credit card. Presently the CAC is not being used for any financial applications, although there is nothing to physically preclude it—the magnetic stripe is physically the same as on a credit card. DOD policy, however, does not provide for the CAC to be used for financial applications at this time.
- *Reading the magnetic stripe:* Magnetic stripe “swipe” readers are commonly available to support access control applications. Consult your local security staff for further guidance.
- *Encoding the magnetic stripe:* The CAC is issued with the magnetic stripe blank. Encoding is usually done locally at your installation by your security staff.
- *Purchasing products that are compatible with the magnetic stripe:* Magnetic stripe “swipe” readers are commonly available to support access control applications. Consult your local security staff for further guidance.

7.2. DON User wants to use the PDF 417 Bar Code.

The PDF 417 bar code contains a total compressed storage of 60 bytes of data. The PDF 417 bar code holds minimal personal data, benefits information (date of birth and entitlement conditions), organizational information, and some card management data tools. The data contained on both the PDF 417 and Code 39 bar codes is required for use in legacy (existing) applications.

- *Common applications:* Mustering (“head count”) type applications or individual identification applications are the most common applications that use the PDF 417 Bar Code (typical examples would be library book or equipment check-out). This media was placed on the CAC to support legacy applications.
- *Reading the bar code:* Bar code readers are commonly available to support these applications. Consult the DOD Automatic Identification Technology (AIT) Office at <http://www.dodait.com> or the General Services Agency (GSA) product schedules for further information on PDF 417 technology.
- *Encoding the bar code:* The CAC is issued with this bar code already printed; no post-issuance changes are permitted or possible.
- *Purchasing products that are compatible with the PDF 417 Bar Code:* Bar code readers are commonly available to support these applications. Consult the DOD AIT site or the General Services Agency (GSA) product schedules for further information on PDF 417 technology.

7.3. DON User wants to use the Code 39 Bar Code. The Code 39 or linear bar code contains a total compressed storage of 18 bytes of data. The Code 39 bar code contains the Electronic Data Interchange (EDI) personal identifier, a CAC holder’s social security number, Uniformed Service Branch, and some card management data tools. The data contained on both the Code 39 and PDF 417 bar codes is required for use in legacy (existing) applications.

- *Common applications:* Retail point-of sale, mustering (“head count”) type applications, or individual identification applications are the most common applications that use the Code 39 Bar Code (typical examples would be supermarket, library book or equipment check-out). This media was placed on the CAC to support legacy applications.
- *Reading the bar code:* Bar code readers are commonly available to support these applications. Consult the DOD AIT site or the General Services Agency (GSA) product schedules for further information on Code 39 Bar Code technology.
- *Encoding the bar code:* The CAC is issued with this bar code already printed; no post-issuance changes are permitted or possible.
- *Purchasing products that are compatible with the Code 39 Code:* Bar code readers are commonly available to support these applications. Consult the DOD AIT site or the General Services Agency (GSA) product schedules for further information on Code 39 Bar Code technology.

7.4. DON user wants to read data from the CAC Integrated Circuit Chip (ICC) for use in some local application.

- *Common applications:* Within the Navy, CACs issued at certain Navy locations have been encoded with a data container referred to as the “Joint Data Model,” or JDM. The JDM contains a variety of data elements; the JDM was developed to support any of the 5 applications: Food Service, Warrior Readiness, Manifest Tracking, Card Maintenance Utility and Weapons Issuance. These applications were originally developed for a predecessor smart card first used in Hawaii, and have now been made “backwards compatible” with the CAC—that is, both the CAC as well as the previous 8K smart card can be used to operate these applications.

- *Reading the ICC:* Any of the data elements on the CAC ICC may be read and subsequently used in a locally developed application. There are two conditions, however. First, the card owner must enter their PIN to “unlock” the card. Equally important is that the application that seeks to read data from the ICC most likely would use middleware, which is the software that enables an application to “talk” to the CAC. ActivCard Gold middleware is part of the suite of software that comes with an NMCI seat. Before a developer can write an application that reads the CAC, they must first go to the DOD ACO web site (at <http://www.dmdc.osd.mil/smartcard>) to obtain the CAC Developer’s Kit. This kit provides instructions for interfacing with the CAC. Note also that the provisions of the DON Configuration Management Plan must be conformed to, which requires that users register their “read only” applications with the eBusiness Operations Office.
- *Encoding the ICC:* The CAC is issued with the ICC already coded; no post-issuance changes are permitted for read-only applications.
- *Purchasing products that are compatible with the ICC:* Please refer to the DOD ACO web site for more information. Also, the Joint Interoperability Test Command (JITC) does product testing for compatibility with the CAC. Check out their web site at <http://ia.jitcwashops.disa.mil/cacindex.php>.

7.5. DON user wants to write data to the CAC Integrated Circuit Chip (ICC) for use in some local application.

- *Common applications:* Warrior Readiness, Manifest Tracking, Weapons Issuance, Card Maintenance Utility, and Food Service
- *Writing to the ICC:* Before any DON user can develop applications that propose to write to the ICC, all the requirements of the DON Configuration Management Plan (CMP) must be complied with. See this and other related CAC documentation on the [DON eBusiness Operations Office Web Portal](#). The DON CAC Configuration Management Plan is also maintained on the Web Portal. The main purpose of the CMP is to control the usage of the “limited” (Service Specific) space on the ICC and to institute a disciplined process for vetting proposed applications. Potential developers must also consult the DOD ACO web site for the CAC Developer’s Kit
- *Encoding the ICC:* This will be done via the application rather than at issuance.
- *Purchasing products that are compatible with the ICC:* Please refer to the DOD ACO web site for more information. In addition, the Joint Interoperability Test Command (JITC) does product testing for compatibility with the CAC. Check out their web site at [JITC](#).

7.6 Vendor wants to sell smart card products to DON.

Refer to the ACO web site for the Card Reader Specification and the Developer's Kit.

Interoperability and testing: Testing by the Joint Interoperability Test Command (JITC) is **not** a mandatory step...but the DOD ACO wants it to be **the** place that vendors will voluntarily choose to have their products tested at, so they can make the claim that their product has been passed by JTIC. Also see the Microsoft web site: <http://www.microsoft.com/hcl/default.asp> . Here is where vendors can get their product "branded" as being interoperable with the Microsoft world.

Appendix A: Printed Media Data Elements

<i>R E F #</i>	<i>CATEGORY</i>	<i>ALIAS</i>	<i>DATA ELEMENT</i>	<i>Size (Bytes)</i>	<i>DATA ELEMENT DEFINITION</i>	<i>DOD REFERENCE</i>
1	Identification	First Name	Person Forename Text	20	The text of a person forename.	DDDS ID # 49782
2	Identification	Last Name	Person Surname Text	26	The text of a person surname.	DDDS ID # 49789
3	Identification	Middle Name	Person Middle Name Text	20	The text of a person middle name.	DDDS ID # 49783
4	Identification	Social Security Number	Person Designator Identifier	15	The identifier that represents a person.	DDDS ID # 11185
5	Identification	Suffix	Person Cadency Name Text	4	The text of a person cadency name.	DDDS ID # 49780
6	Identification	Photograph	Person Photograph Image	N/A	Color photograph of cardholder	DDDS ID # 42242
7	Identification	Geneva Convention Category	Geneva Convention Category	1	Geneva convention category of cardholder	DDDS ID # 61310
8	Identification	Person Designator	Person Designator Type Code	1	The code that represents a person designator.	DDDS ID # 13680
9	Identification	Blood Type	Blood Type Code	2	The code that represents a person's blood type	DDDS ID # 28274
10	Identification	Organ Donor	Organ Donation Agreement Indicator Code	1	The code that indicates whether a person has agreed to donate their internal organs after death.	DDDS ID # 34591
11	Benefits	Date of Birth	Person Birth Calendar Date	8	The calendar date when a person was born.	DDDS ID # 11322
12	Benefits	Exchange Code	Exchange Benefit Status Code	1	The code that indicates the status of the person's exchange benefits.	DDDS ID # 50399

13	Benefits	Commissary Code	Commissary Benefit Status Code	1	The code that indicates the status of the person's commissary benefits.	DDDS ID # 50399
14	Benefits	MWR Code	MWR Benefit Status Code	1	The code that indicates the status of the person morale, welfare, and recreation benefits.	DDDS ID # 50399
15	Benefits	Entitlement Code	Civilian Health Care Entitlement Type Code	1	The code that represents what type of civilian health care privileges a person has.	DDDS ID # 61294
16	Benefits	Type Code	Direct Care Benefit Type Code	1	The code that represents what type of direct care benefits the person has.	DDDS ID # 61293
17	Organization	Branch	Uniformed Service Branch Classification Code	1	The code that represents a Uniformed Service branch classification.	DDDS ID # 52292
18	Organization	Pay Grade	Uniformed Service Member Pay Grade Code	3	The code that represents the level of pay or enumerates a member's status in a pay hierarchy and consists of both a flag denoting officer/enlisted status as well as rank order within that status.	DDDS ID # 53488
19	Organization	Rank	Uniformed Service Rank Short Name	6	The abbreviated name of a Uniformed Service rank.	DDDS ID # 23514
20	Organization	DOD or Branch Seal	DOD or Branch Seal	N/A		DDDS ID # 12695
21	Card Management	Card Issue Date	Identification Card Issue Calendar Date	8	The date when the person's current or former ID card was issued.	DDDS ID # 18085
22	Card Management	Card Expiration Date	Identification Card Expiration Calendar Date	8	The date when the person's current ID card is expected to expire.	DDDS ID # 18085
<p>Note 1: There are multiple iterations of the CAC (military, civilian, civilian with benefits, and civilian with emergency entitlements)</p> <p>Note 2: Entitlement information for Active and Reserve will NOT be printed on the card.</p>						

Appendix B: Integrated Circuit Chip (ICC) Data Elements

<i>R E F #</i>	<i>CATEGORY</i>	<i>ALIAS</i>	<i>DATA ELEMENT</i>	<i>Size (Bytes)</i>	<i>DATA ELEMENT DEFINITION</i>	<i>DOD REFERENCE</i>
1	Identification	First Name	Person Forename Text	20	The text of a person forename.	DDDS ID # 49782
2	Identification	Gender	Sex Category Code	1	The code that represents a sex category.	DDDS ID # 11697
3	Identification	Person Designator	Person Designator Type Code	1	The code that represents a specific kind of person designator.	DDDS ID # 13680
4	Identification	Last Name	Person Surname Text	26	The text of a person surname.	DDDS ID # 49789
5	Identification	Middle Name	Person Middle Name Text	20	The text of a person middle name.	DDDS ID # 49783
6	Identification	Social Security Number	Person Designator Identifier	15	The identifier that represents a person designator.	DDDS ID # 11185
7	Identification	Suffix	Person Cadency Name Text	4	The text of a person cadency name.	DDDS ID # 49780
8	Identification	Person Identifier	DOD Electronic Data Interchange (EDI) Person Identifier	10	The identifier that represents a person within the Department of Defense Electronic Data Interchange.	DDDS ID# 61041
9	Identification	Blood Type	Blood Type Code	2	The code that represents a person's blood type	DDDS ID # 28274
10	Identification	Organ Donor	Organ Donation Agreement Indicator Code	1	The code that indicates whether a person has agreed to donate their internal organs after death.	DDDS ID # 34591
11	PKI	Identity Certificate	DOD PKI Authentication Certificate Data	2000	The data contained in a person's authentication certificate used for the DOD private key infrastructure.	8320.1.B.8.5
12	PKI	Signature E-Mail Certificate	S/MIME Certificate Signature Data	2000	The data contained in a person's public signature key for the secure multipurpose Internet mail extension certificate.	8320.1.B.8
13	PKI	Encryption E-Mail Certificate	S/MIME Certificate Encryption Data	2000	The data contained in a person's public encryption key for the secure multipurpose Internet mail extension certificate.	8320.1.B.8
14	PKI	Private Key Identifier	DOD PKI Authentication Private Key Identifier	768	The identifier for a person's authentication used for the DOD private key infrastructure.	8320.1.B.8

15	PKI	Encryption Key Identifier	S/MIME Encryption Private Key Identifier	768	The identifier used for a person for the secure multipurpose Internet mail extension private encryption key.	8320.1.B.8
16	PKI	Signature Key Identifier	S/MIME Signature Private Key Identifier	768	The identifier used for a person for the secure multipurpose Internet mail extension private signature key.	8320.1.B.8
17	Benefits	Date of Birth	Person Birth Calendar Date	8	The calendar date when a person was born.	DDDS ID # 11322
18	Benefits	Contractor Code	DOD Contractor Function Code	1	A code that indicates the type of work a DOD contractor does or agency they work for.	DDDS ID # 13877
19	Benefits	Meal Entitlement Code	Meal Plan Type Code	2	The code that represents what meal plan a person is eligible for.	DDDS ID # 61309
20	Benefits	Exchange Code	Exchange Benefit Status Code	1	The code that indicates the status of the person's exchange benefits.	DDDS ID # 50399
21	Benefits	Commissary Code	Commissary Benefit Status Code	1	The code that indicates the status of the person's commissary benefits.	DDDS ID # 50399
22	Benefits	MWR Code	MWR Benefit Status Code	1	The code that indicates the status of the person morale, welfare, and recreation benefits.	DDDS ID # 50399
23	Benefits	End Date	CAC Non-Medical Benefits Eligibility End Calendar Date	8	The end date of a person's DOD non-medical personnel programs on the CAC.	DDDS ID # 29259
24	Benefits	Entitlement Code	Civilian Health Care Entitlement Type Code	1	The code that represents what type of civilian health care privileges a person has.	DDDS ID # 61294
25	Benefits	Type Code	Direct Care Health Benefit Type Code	1	The code that represents a specific kind of direct care benefits program.	DDDS ID # 61293
26	Benefits	End Date	Direct Care End Date	8	The end date a person's direct care benefit programs on the CAC.	DDDS ID # 29259
27	Benefits	Medical Benefits End Date	CAC Medical Benefits End Calendar Date	8	The end date a person's DOD medical benefit programs on the CAC.	DDDS ID # 29259
28	Benefits	Entitlement Condition	Personnel Entitlement Condition Type Code	2	The code that represents the type of condition that occurred while a sponsor was in a personnel category and organization that affects the entitlements of the sponsor and/or the sponsor's dependents.	Multiple 6
29	Organization	Branch	Uniformed Service Branch Classification Code	1	The code that represents a Uniformed Service branch classification.	DDDS ID # 52292

30	Organization	Personnel Category	Personnel Category Code	1	The code that represents how the DOD personnel and/or finance center views the sponsor based on accountability and reporting strengths.	DDDS ID # 12715 DDDS ID # 39834 DDDS ID # 17049
31	Organization	Government Agency	US Government Agency/Sub-agency Code	4	The code that indicates the government agency a "Non-DOD civil services employee, except Presidential appointee", works for.	DDDS ID # 17141
32	Organization	Non-Government Agency	US Non-Government Agency Code	2	The code that indicates the non-government agency a "Non-government agency personnel" works for.	DDDS ID # 7875
33	Organization	Pay Category	Pay Plan Code	2	The code that represents a category or a schedule for monetary compensation.	DDDS ID # 20374
34	Organization	Pay Grade	Pay Plan Grade Code	2	The code that represents a pay category or schedule for monetary compensation.	DDDS ID # 20369
35	Organization	Rank	Uniformed Service Rank Short Name	6	The abbreviated name of a Uniformed Service rank.	DDDS ID # 23514
36	Card Management	Date Demographic Data was Loaded on Chip	CAC Demographic Data Update Calendar Date	8	The date when the last update was made to the demographic data; is independent of benefit dates.	DDDS ID # 61300
37	Card Management	Date Demographic Data on Chip Expires	CAC Demographic Data Expiration Calendar Date	8	The date when demographic data is expected to expire; is independent of benefit dates.	DDDS ID # 61301
38	Card Management	Card Security Code	Card Instance Identifier	3	The identifier used to uniquely identify each card issued to a person	DDDS ID # 9643
39	Card Management	Card Issue Date	Identification Card Issue Calendar Date	8	The date when the person's current or former ID card was issued.	DDDS ID # 18085
40	Card Management	Card Expiration Date	Identification Card Expiration Calendar Date	8	The date when the person's current ID card is expected to expire.	DDDS ID # 18085
Total Uncompressed Storage, not including overhead (Bytes)				8,499		
Non-PKI storage space, not including overhead (Bytes)				195		
PKI storage space, not including overhead (Bytes)				8,304		

Appendix C: “Code 39” Bar Code Data Elements

<i>R E F #</i>	<i>CATEGORY</i>	<i>ALIAS</i>	<i>DATA ELEMENT</i>	<i>Size (Bytes)</i>	<i>DATA ELEMENT DEFINITION</i>	<i>DOD REFERENCE</i>
1	Identification	Person Designator	Person Designator Type Code	1	The code that represents a specific kind of person designator.	DDDS ID # 13680
2	Identification	Social Security Number	Person Designator Identifier	9	The identifier that represents a person designator.	DDDS ID # 11185
3	Identification	Person Identifier	DOD Electronic Data Interchange (EDI) Person Identifier	10	The identifier that represents a person within the Department of Defense Electronic Data Interchange.	DDDS ID# 61041
4	Organization	Personnel Category	Personnel Category Code	1	The code that represents how the DOD personnel and/or finance center views the sponsor based on accountability and reporting strengths.	DDDS ID # 12715 DDDS ID # 39834 DDDS ID # 17049
5	Organization	Branch	Uniformed Service Branch Classification Code	1	The code that represents a Uniformed Service branch classification.	DDDS ID # 52292
6	Card Management	Card Security Code	Card Instance Identifier	1	The identifier used to uniquely identify each card issued to a person	DDDS ID # 9643
7	Card Management	Bar Code Version	Bar Code Version Number Code	1	The code that represents the bar code type and version number.	N/A 7
		Total Uncompressed Storage (Bytes)		24	Total Compressed Storage (Bytes)	
		Media Limit: 24 Bytes Uncompressed, 18 Bytes Compressed				

Appendix D: PDF 417 Bar Code Data Elements

<i>R E F #</i>	<i>CATEGORY</i>	<i>ALIAS</i>	<i>DATA ELEMENT</i>	<i>SIZE (Bytes)</i>	<i>DATA ELEMENT DEFINITION</i>	<i>DOD REFERENCE</i>
1	Identification	Person Designator	Person Designator Type Code	1	The code that represents a specific kind of person designator.	DDDS ID # 13680
2	Identification	Last Name	Person Surname Text	26	The text of a person surname.	DDDS ID # 49789
3	Identification	First Name	Person Forename	20	The text of a person forename.	DDDS ID # 49782
4	Identification	Social Security Number	Person Designator Identifier	9	The identifier that represents a person designator.	DDDS ID # 11185
5	Identification	Person Identifier	DOD Electronic Data Interchange (EDI) Person Identifier	10	The identifier that represents a person within the Department of Defense Electronic Data Interchange.	DDDS ID# 61041
6	Benefits	Date of Birth	Person Birth Calendar Date	8	The calendar date when a person was born.	DDDS ID # 11322
7	Benefits	Entitlement Condition	Personnel Entitlement Condition Type Code	2	The code that represents the type of condition that occurred while a sponsor was in a personnel category and organization that affects the entitlements of the sponsor and/or the sponsor's dependents.	Multiple 6
8	Organization	Personnel Category	Personnel Category Code	1	The code that represents how the DOD personnel and/or finance center views the sponsor based on accountability and reporting strengths.	DDDS ID # 12715 DDDS ID # 39834 DDDS ID # 17049
9	Organization	Branch	Uniformed Service Branch Classification Code	1	The code that represents a Uniformed Service branch classification.	DDDS ID # 52292
10	Organization	Pay Category	Pay Plan Code	2	The code that represents a pay category or schedule for monetary compensation.	DDDS ID # 20374

11	Organization	Pay Grade	Pay Plan Grade Code	2	The code that represents a sequential level of pay within a Pay Plan.	DDDS ID # 20369
12	Organization	Rank	Uniformed Service Rank Short Name	6	The abbreviated name of the Uniformed Service Rank	DDDS ID # 23514
13	Card Management	Bar Code Version	Bar Code Version Number Code	1	The code that represents the bar code type and version number.	N/A 7
14	Card Management	Card Issue Date	Identification Card Issue Calendar Date	8	The date when the person's current or former ID card was issued.	DDDS ID # 18085
15	Card Management	Card Expiration Date	Identification Card Expiration Calendar Date	8	The date when the person's current ID card will expire.	DDDS ID # 18085
16	Card Management	Card Security Code	Card Instance Identifier	3	The identifier used to uniquely identify each card issued to a person.	DDDS ID # 9643
		Total Uncompressed Storage (Bytes)		108	Total Compressed Storage (Bytes)	
			Media Limit:	140	Bytes Compressed	