NOT MEASUREMENT SENSITIVE

MIL-HDBK-501
15 April 1997

DEPARTMENT OF DEFENSE
HANDBOOK

PORTABLE INFORMATION CARRIER

This handbook is for guidance only. Do not cite this document as a requirement.

AMSC N/A AREA IPSC

FOREWORD

1. This handbook is approved for use by all Departments and Agencies of the Department of Defense (DoD).

2. A handbook is a guidance document that enhances user awareness by providing engineering information; lessons learned; possible options to address technical issues; classification of similar item, materials, or processes; interpretative direction and techniques; and any other type of guidance information that may help the Government or its contractors in the design, construction, selection, management, support, or operation of systems, products, processes, or services. This handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.

3. The guidance provides the common elements of a multi-technology, multi-application smart card. The identification of these common elements form a baseline for use of a cross-service, multi-application integrated circuit card across all functional areas of DoD having to deal with personal information transferral. The program relationships and interdependencies will be the responsibility of the DoD components that will implement this guidance. The intent is to assist in the planning and initiation of a single standard for smart card usage across DoD to prevent separate and incompatible implementation of smart card technologies.

4. The multi-technology aspect of the Portable Information Carrier (PIC) guidance provides an interface to existing applications using a variety of reader equipment. It also provides for selection of the most cost-effective reader technique for new applications, while allowing a single card to interface with multiple applications using different reader equipment. The uniqueness of the PIC is the ability to update and completely erase information contained on the chip of the card unlike the use of bar codes, embossing, and magnetic stripes.

5. PIC is a portable device which contains one or more technologies used to store information related to an individual and may be used in one or more applications. The PIC may contain both updatable and static technologies such as an integrated circuit chip, magnetic stripe, bar code, digitized photo, and other printed information. The major focus of the PIC is the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7816 (all parts) Integrated Circuit Card (ICC). Applications supporting PIC implementation must meet at least Level 5 compliancy with the Defense Information Infrastructure (DII) Common Operating Environment (COE) as defined in the *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS),* Preliminary Version 2.0, October 23, 1995.

6. A PIC is intended for information exchange with outside application(s). It is critical to realize the PIC is not intended to be exclusively a data storage device. The card delivers information and may modify its content based on the information exchange and the applications using the data. The actual storage location of data and structural information will be under the management of the DoD PIC management infrastructure. The key difference between the PIC and other types of information carrying cards is the ability to read from, add to, and completely erase the ICC data on the card.

7. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Defense Information Systems Agency, Center for Standards/JEBE, Attn: PIC Military Handbook, 10701 Parkridge Boulevard, Reston, VA 20191 by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

CONTENTS

1. SCOPE 1

1.1 Purpose of this document 1
1.2 Portable Information Carrier Standards Working Group (PICSWG) 1
1.3 Definition of PIC and the DoD PIC concept 2
1.4 Major findings 3
1.4.1 Infrastructure considerations 3
1.4.2 Technology assumptions 3
1.5 Document organization and introduction to next sections 4

2. APPLICABLE DOCUMENTS 5

2.1 General 5
2.2 Government documents 5
2.3 Non-Government publications 6
2.4 Order of precedence 7

3. DEFINITIONS 7

3.1 Acronyms used in this standard 7
3.2 Access control 9
3.3 Active 10
3.4 Algorithm 10
3.5 Answer to reset (ATR) file 10
3.6 Anti-tearing 10
3.7 Authenticate 10
3.8 Authentication 10
3.9 Authenticator 10
3.10 Authorization 10
3.11 Biometric 10
3.12 Cardholder 10
3.13 Card reader 10
3.14 Card version 10
3.15 Chip 10
3.16 Chip card 10
3.17 Chip or card operating system (COS) 10
3.18 Contact 10
3.19 Debit card 10
3.20 Dictionary 10
3.21 Digital signature 11
3.22 Digital signature algorithm 11
3.23 Exception 11
3.24 Hashing 11
3.25 International Organization for Standardization 11
3.26 Key 11
3.27 Key management 11
3.28 Nonvolatile memory 11
3.29 On-chip applications 11
3.30 Open Systems Environment (OSE) 11
3.31 Operating system (O/S) interface layer 11

3.32 Personal identification number (PIN) 11
3.33 Portable Information Carrier (PIC) 11
3.34 Private key cryptography 11
3.35 Public key cryptography 11
3.36 Reader/writer driver layer 11
3.37 Security 11
3.38 Smart card 12
3.39 Storage 12
3.40 Table 12
3.41 Tampering 12
3.42 User 12
3.43 Virtual card 12

4. DATA MANAGEMENT 12

4.1 Overview 12
4.2 Functional concepts for operational PIC program(s) 12
4.3 Data inclusion and categorization 13
4.4 Data modification/maintenance 13
4.5 External (outside DoD) application interfaces 13

5. PIC INTEGRATION INTERFACE (PI^2) 13

5.1 Overview 13
5.2 Workstation application layers 16
5.2.1 PIC user application software 16
5.2.2 Application programming layer 16
5.2.2.1 Security functions 16
5.2.2.2 Data operations 17
5.2.2.3 Control functions 17
5.2.3 Data index layer 17
5.2.3.1 Access control 18
5.2.3.2 Data addressing 18
5.2.3.3 Security functions 18
5.2.3.4 Calls from data index layer to host operating system layer 18
5.2.3.4.1 Structured card query language (SCQL) 19
5.2.3.4.2 Activation of on-chip applications 19
5.2.3.4.3 Data index layer extensions 19
5.2.4 Host operating system layer 19
5.2.4.1 Upper interface sublayer 19
5.2.4.2 Host operating system 19
5.2.4.3 Lower interface sublayer 19
5.2.4.4 Host operating system extensions 19
5.2.5 Reader/writer driver layer 20
5.2.6 Physical layer 20
5.2.6.1 Reader/writer 20
5.2.6.2 Interface electronics 20
5.3 PIC interface layer structure 20
5.3.1 Physical interface 20
5.3.2 Chip operating system layers 20
5.3.3 PIC on-chip applications 20

5.3.3.1 Security functions 20
5.3.3.2 Financial functions 21
5.3.3.3 Data operations 21

6. APPLICATION PROGRAMMING INTERFACE (API) 21

6.1 Overview 21
6.2 Application programming interface functions 21
6.3 Data index registration functions 21
6.4 Security/access control functions 21
6.5 Control functions 22
6.6 Operating system layer 22
6.7 Reader/writer driver layer 22
6.8 Year 2000 compliance 22
6.8.1 User layer 23
6.8.2 Logical layer 23
6.8.3 Interface layer 24
6.8.4 Data layer 24

7. SECURITY 24

7.1 Overview 24
7.2 General 25
7.2.1 Audit 25
7.2.2 Emergency destruction 25
7.3 PIC integrated circuit (IC) security profiles 25
7.3.1 PIC IC functions 25
7.3.1.1 Grant file access 26
7.3.1.1.1 Access types 26
7.3.1.1.2 File types 26
7.3.1.2 Hash 26
7.3.1.3 Digital signature 26
7.3.2 PIC access controls 26
7.3.2.1 Public request 27
7.3.2.2 Cardholder PIN 27
7.3.2.3 Password from application 27
7.3.2.4 Validity period check 27
7.3.2.5 Public key-based encryption protection 27
7.3.3 Profiles and scenarios 27
7.3.3.1 Basic PIC 27
7.3.3.1.1 Basic PIC applications 27
7.3.3.1.2 Basic PIC functions 27
7.3.3.1.3 Basic PIC access controls 28
7.3.3.2 Digital signature PIC 28
7.3.3.2.1 Digital signature PIC applications 29
7.3.3.2.2 Digital signature PIC functions 29
7.3.3.2.3 Digital signature PIC access controls 29
7.3.3.3 Cryptographically protected PIC 30
7.3.3.3.1 Cryptographically protected PIC applications 30
7.3.3.3.2 Cryptographically protected PIC functions 30
7.3.3.3.3 Cryptographically protected PIC access controls 30

7.3.3.4 Cryptographically protected digital signature PIC 31
7.3.3.4.1 Cryptographically protected digital signature PIC applications 32
7.3.3.4.2 Cryptographically protected digital signature PIC functions 32
7.3.3.4.3 Cryptographically protected digital signature PIC access controls 32
7.4 PIC data security 33
7.4.1 Confidentiality 33
7.4.2 Integrity 34
7.4.3 Availability (protection from denial of service) 34
7.5 PIC physical security 34
7.5.1 Overview 34
7.5.2 IC and card level 34
7.6 Application security 34
7.6.1 Overview 34
7.6.2 Security 34

8. PHYSICAL 35

8.1 Overview 35
8.2 Physical characteristics 35
8.2.1 Dimensions 35
8.2.2 Construction 35
8.2.3 Card materials 35
8.2.4 Card characteristics 35
8.2.4.1 Flammability 35
8.2.4.2 Resistance to chemicals 35
8.2.4.3 Reliability/durability 35
8.2.4.4 Environmental conditions 35
8.2.4.4.1 Temperature/humidity 36
8.2.4.4.2 Light 36
8.2.5 Magnetic stripe 36
8.2.6 Special characteristics 36
8.2.6.1 Holes in PIC 36
8.2.6.2 Decorations 36
8.2.6.3 Maintainability 36
8.3 Magnetic stripe 36
8.3.1 Location of magnetic stripe 36
8.3.2 Track encoding 36
8.4 Bar codes 36
8.4.1 One-dimensional bar code 36
8.4.1.1 Symbology 37
8.4.1.2 Code density and dimensions 37
8.4.1.2.1 Code density 37
8.4.1.2.2 Heights 37
8.4.1.2.3 Nominal width 37
8.4.1.2.4 Nominal wide-to-narrow ratio 37
8.4.1.3 Readability 37
8.4.1.4 Location 37
8.4.2 Two-dimensional bar code 38
8.4.2.1 Compaction modes 38
8.4.2.2 Symbol dimensions 38
8.4.2.3 Readability 38

8.4.2.4 Location 39
8.5 Integrated circuit chip 39
8.5.1 Location and dimensions of contacts 39
8.5.2 Contact assignment 39
8.5.3 Card session 39
8.5.4 Chip operating system 39

9. READER/WRITER 39

9.1 Overview 39
9.2 Card types/technologies 39
9.2.1 Magnetic stripe 39
9.2.2 Bar codes 40
9.2.3 Integrated circuit chip 40
9.2.3.1 Card feed speed 40
9.2.3.2 Transmission protocols 40
9.3 Reliability/durability 40
9.4 Environmental conditions 40
9.5 Power 40
9.6 Electronic design 40
9.7 External interface 40
9.8 Financial application capability 40

10. NOTES 40

10.1 Intended Use 40
10.2 Subject Word Listing 41

A. REFERENCES 42

A.1. SCOPE 42
A.1.1 Scope 42
A.2. APPLICABLE DOCUMENTS 42

B. ASSUMPTIONS 45

B.1. SCOPE 45
B.1.1 Scope 45
B.2. GENERAL 45
B.2.1 General 45
B.3. DATA MANAGEMENT 45
B.3.1 Data management 45
B.4. PIC INTEGRATION INTERFACE (PI^2) 46
B.4.1 PIC integration interface (PI^2) 46
B.5. SECURITY 46
B.5.1 Security 46
B.6. PHYSICAL 47
B.6.1 Physical 47

C. STRUCTURED CARD QUERY LANGUAGE (SCQL) CONSIDERATIONS 48

C.1. SCOPE 48

C.1.1 Scope 48
C.2. SCQL TABLES 48
C.2.1 SCQL tables 48
C.3. SCQL VIEWS 48
C.3.1 SCQL views 48
C.4. SCQL APPLICATION TABLES 48
C.4.1 SCQL application tables 48
C.4.1.1 SCQL dictionaries 49
C.5. USER APPLICATION RESTRICTIONS 49
C.5.1 User application restrictions 49
C.6. SCQL COMMANDS 49
C.6.1 General concepts 49
C.6.2 Grouping and encoding 50
C.6.3 Notation and special situations 50
C.6.4 Status bytes 51
C.6.5 Identifiers 52
C.6.6 Security attributes of tables 53

D. CHIP UTILIZATION BLUEPRINT 54

D.1. SCOPE 54
D.1.1 Scope 54
D.2. CHIP DATA LAYOUT BLUEPRINT OVERVIEW 54
D.2.1 Chip data layout blueprint overview 54
D.3. PI5 LAYER 54
D.3.1 PI5 layer 54
D.4. DEMOGRAPHICS LAYER 55
D.4.1 Demographics layer 55
D.5. AGENCY/COMPONENT GENERAL APPLICATION LAYER 55
D.5.1 Agency/component general application layer 55
D.6. OTHER POSSIBLE LAYERS 56
D.6.1 Other possible layers 56

CONCLUDING MATERIAL 58

FIGURES

1. Workstation interface structure....14
2. PIC interface structure....15
D-1. PI5 layer....54
D-2. Demographics layer....55
D-3. Component information on the PIC....56

TABLES

I. API security....22
II. Basic PIC profile....28
III. Digital signature PIC profile....29
IV. Cryptographically protected PIC profile....31
V. Cryptographically protected digital signature PIC profile....33
VI. Nominal wide-to-narrow ratio....37
VII. Symbol dimensions....38
VIII. Higher levels of error correction....38
IX. SCQL commands....50
X. General meaning of SW1-SW2....51

1. SCOPE

1.1 Purpose of this document. This handbook is written for the Department of Defense (DoD) through the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I). It was designed to build consensus on DoD standard guidance for a multi-technology smart card. This document was composed through a standards working group which was open to all DoD components and agencies and reformatted as a military handbook. The goal of this handbook is to establish a common DoD vision for the integration and implementation of smart card technology for DoD. This handbook is for guidance only. This handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.

The guidance provides the common elements of a multi-technology, multi-application smart card. The identification of these common elements form a baseline for use of a cross-service, multi-application integrated circuit card across all functional areas of DoD having to deal with personal information transferral. The program relationships and interdependencies will be the responsibility of DoD components that will implement this guidance. The intent is to assist in the planning and initiation of a single standard for smart card usage across DoD to prevent separate and incompatible implementation of smart card technologies.

The multi-technology aspect of the Portable Information Carrier (PIC) guidance provides an interface to existing applications using a variety of reader equipment. It also provides for selection of the most cost-effective reader technique for new applications, while allowing a single card to interface with multiple applications using different reader equipment. The uniqueness of the PIC is the ability to update and completely erase information contained on the chip of the card, unlike the use of barcodes, embossing, and magnetic stripes.

The guidance is a compilation of:

a. The Multi-Technology Automated Reader Card (MARC) test project.

b. Input from various vendors.

c. Examination of other technologies, such as the optical memory card, radio frequency identification (RFID), and PC cards.

d. Comments and discussions with and from industry.

e. Other Government agencies.

The guidance is built upon the lessons learned from the MARC Test Project, but is meant to be independent from MARC and the MARC Project. For purposes of this handbook, the DoD smart card program is identified as the PIC.

1.2 Portable Information Carrier Standards Working Group (PICSWG). In 1992, the former DoD Information Technology Policy Board (ITPB) recommended the development of an integrated architecture and standard for a MARC for the Director of Defense Information. In 1994, the focus shifted to developing standard guidance for a PIC reformatted to a military handbook. The handbook is envisioned to eventually contribute to a Federal Information Processing Standard Publication (FIPS Pub) or Government-wide standards.

The PIC Standards Working Group (PICSWG) was chartered under the sponsorship of the DoD Standards Coordinating Committee (SCC) and empowered to conduct its activities in accordance with the charter. The PICSWG was chaired by the Defense Information Systems Agency (DISA) Center for Standards (CFS), and meeting announcements and agendas were circulated to all services and DoD components. All DoD components

were invited to provide representatives. Active participation in PICSWG meetings varied over the 2 years of meetings. Representatives from the Office of the Secretary of Defense (OSD), DISA, the National Security Agency (NSA), and some of the services were represented at most of the meetings. Meeting announcements were distributed in the form of a memorandum from the CFS Information Processing Department, DISA.

In developing this handbook, the PICSWG formed several working groups, each of which focused on a major area of the document. The PICSWG heard from a variety of sources familiar with actual (or potential) applications and programs where a PIC might be used. These included industry experts, DoD programs (including the MARC proof-of-principle test project), Federal programs outside DoD, and others. After gathering this information, each working group proceeded to develop the text for that particular section. The groups and chair components were:

GROUP	CHAIR COMPONENT
Application Programming Interface (API) (later changed to PIC Integration Interface (PI^2))	OSD (C3I-Information Technology)
Data Management	Air Force/OSD (Personnel and Readiness)
Security	NSA
Reader/Writer	Contractor Support
Physical	no chair - DISA and API group effort

While PICSWG participants actively contributed their expertise, the individuals who contributed most to this document's contents may not represent their component's or service's policy making authority. This document provides guidance and is not meant to be a Military Standard (MIL-STD) or Government specification. The PICSWG coordinated its efforts with the Federal Smart Card User Group (FSCUG), which is tasked to exchange information on smart card usage within the Federal Government. Input was received from various corporations and government agencies, many of whom are members of the Smart Card Forum (SCF).

1.3 Definition of PIC and the DoD PIC concept. PIC is a portable device which contains one or more technologies used to store information related to an individual and may be used in one or more applications. The PIC may contain both updatable and static technologies such as an integrated circuit chip, magnetic stripe, bar code, digitized photo, and other printed information. The major focus of the PIC is the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7816 (all parts) Integrated Circuit Card (ICC).

A PIC is intended for information exchange with outside application(s). It is critical to realize the PIC is not intended to be exclusively a data storage device. The card delivers information and may modify its content based on the information exchange and the applications using the data. This data exchange is accomplished through the PI^2. The actual storage location of data and structural information will be under the management of the DoD PIC management infrastructure. The key difference between the PIC and other types of information carrying cards is the ability to read from, add to, and completely erase the ICC data on the card.

Any DoD component implementing a PIC should review and take advantage of the documentation from the MARC test, including the final test report, functional economic analysis, and program integration report. Due to the limited storage space available, data management which eliminates redundancy and conserves storage capacity is central to effective implementation.

The PIC is to be a multi-service, multi-application card. Each application and each service may have an exclusive section of the ICC on which to implement service-, or mission-specific applications, but the overall card is meant to be used by all DoD services and components. This guidance strongly discourages the development of and use of PIC technologies as independent isolated service or mission cards. To prevent this from occurring, the PICSWG

strongly recommends that DoD establish a centralized management infrastructure, including a program office or executive agent, to centrally manage and coordinate the implementation of PIC across DoD. Commercial off-the-shelf (COTS) products are to be used wherever possible. The government off-the-shelf (GOTS) (DoD owned) Smart Card User Interface (SCUI) should be considered when developing and implementing PIC applications. All new application data should be integrated across the PIC to prevent any duplicate data fields or data entry.

Only Unclassified and Sensitive But Unclassified (SBU) content will be placed on the PIC as currently envisioned. Future advancements in the technology and encryption capabilities may justify future changes in this assumption. Applications have specific read/write permissions. A "unique identifier" is required for each card issued. A DoD PIC management infrastructure and a configuration control process will be in place to manage the process of standardizing security requirements. The PIC and its supporting infrastructure will provide the following security services: confidentiality, availability, and integrity of data stored on the chip. All applications will complete a security certification and accreditation process. Readers/writers will provide the level of security consistent with the PIC security guidance indicated in this document.

1.4 Major findings.

1.4.1 Infrastructure considerations. This handbook provides guidance which will enable DoD to field a viable PIC program. The handbook leads to an understanding of the type and role of infrastructure necessary for DoD to manage the program, but does not address policy or implementation procedures. The infrastructure applies to any entity seeking to standardize PIC technology to allow for interoperability, multiple applications using the same PIC, and reducing proliferation of multiple PICs.

The establishment and funding of a DoD PIC management infrastructure is critical to a successful DoD PIC implementation. This management infrastructure may include a program office or executive agent, a configuration control process, and the authority to mandate compliance with certain standard procedures and PIC processes across DoD. The following sections provide additional details about the infrastructure assumptions.

Section 4, "Data Management," documents the need for central data management. Configuration control and dissemination of software, policy, and information about all applications is needed to ensure use of common data elements, PI^2, and applications. PIC technology can allow for multiple functions/uses for the same PIC (rather than multiple "stove piped" PICs).

Section 5, "PIC Integration Interface (PI^2)," documents the guidance that will allow the PIC the flexibility to evolve as technology advances and to adapt to potential application interfaces. The ability to read past data structures should be maintained for at least two previous versions.

Section 6, "Application Programming Interface (API)," describes additional components of a PIC and a PIC program that depend on an infrastructure being in place. For example, the API narrative references the need to provide a resource kit comprised of specific API calls and other relevant data to application developers who are working on ways to use the PIC.

Section 7, "Security," assumes an infrastructure will be in place prior to fielding a DoD PIC program. As stated in the section, the security of an information system employing a PIC is dependent upon both the characteristics and capabilities of the PIC itself, and upon the infrastructures which issue, support, and use them. In general, the greatest threats and vulnerabilities are in the PIC infrastructure, rather than in a well-designed PIC.

1.4.2 Technology assumptions. This handbook serves as guidance and is not an implementation standard. The handbook takes into account the fact that smart card technology is rapidly evolving and expanding into new and as yet unimagined applications and capabilities. This guidance is not meant to confine the

implementation of the advances in the technology nor its uses as they become available. The PICSWG believes this guidance should evolve with the technology and continue to adjust and to incorporate the advances of technologies as they pertain to PIC when they become available.

This guidance is based on the assumption that the initial implementation of a PIC will use an 8K+ byte chip. The PICSWG is aware of the rapid development of chip technology and the potential future industry implementation of a 32K and larger chips. The size should be driven by the mission requirements and the information which will be contained in the chip, exclusive of the other storage devices on the card.

The PICSWG considered the use of biometrics for the PIC. The use of biometrics will be driven by the mission.

1.5 Document organization and introduction to next sections. The remainder of this document is divided into the following sections and appendixes:

a. 2. Applicable Documents

b. 3. Definitions and Acronyms

c. 4. Data Management

d. 5. PIC Integration Interface (PI^2)

e. 6. Application Programming Interface (API)

f. 7. Security

g. 8. Physical

h. 9. Reader/writer

i. 10. Notes

j. Appendix A. References

k. Appendix B. Assumptions

l. Appendix C. Chip Utilization Blueprint

m. Appendix D. Structured Card Query Language (SCQL) Considerations

Section 2, "Applicable Documents," lists documents needed in order to fully understand the information provided by this handbook.

Section 3, "Definitions and Acronyms," is self explanatory. Most concur with the definitions used in the SCF glossary and the ISO/IEC standards related to ICC. Some additional definitions and acronyms are from various DoD instructions, manuals, and guidance.

Section 4, "Data Management," provides fundamental assumptions underlying the data which the PIC is intended to carry and the management of that data. Two types of data management are acknowledged: (1) overall guidance for all DoD services and components, and (2) technical data management standards, processes, and design

parameters which enable the data from multiple applications to operate without interfering with security, data integrity, or the operation of applications in the field.

Section 5, "PIC Integration Interface (PI^2)," describes the subsystem required to allow a PIC user's application software, operating on a computer workstation, to access and maintain the PIC. The PI^2 layers are implemented as a collection of callable libraries.

Section 6, "Application Programming Interface (API)," contains specific calls and other relevant data provided for application developers. Where applicable, the ISO/IEC 7816 series should be used. The API calls will support static linking into an open systems programming language library, Windows 3.11 16-bit dynamic linked library (DLL), Windows 95 and NT 16-bit DLLs, Windows 95 and NT 32-bit DLLs, and a client/server architecture at a minimum.

Section 7, "Security," addresses the security implications of the sharing necessary for the PIC to support multiple applications. It is expected that the greatest threats and vulnerabilities lie in the PIC infrastructures, rather than in a well-designed PIC. PIC security involves a variety of services, characteristics, and capabilities, including at least data confidentiality, data integrity, and data availability.

Section 8, "Physical," addresses the physical characteristics of the PIC and the specific technologies optionally included on a PIC such as magnetic stripes, bar codes, and integrated circuit chips.

Section 9, "Reader/Writer," addresses the PIC readers/writers including card types, reliability, environmental, and power considerations. Reader/writer technologies needed include magnetic stripes, one-dimensional and two-dimensional bar codes, and integrated circuit chips.

Section 10, "Notes," contains information of a general or explanatory nature.

Appendix A, "References," lists all documents referenced herein.

Appendix B, "Assumptions," contains a summary of key assumptions used in developing this document.

Appendix C, "Chip Utilization Blueprint," provides a possible blueprint for data element layout on the integrated circuit.

Appendix D, "Structured Card Query Language (SCQL) Considerations," provides information for use when SCQL is implemented.

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed below are not necessarily all of the documents referenced herein, but are the ones that are needed in order to fully understand the information provided by this handbook. Appendix A lists all documents referenced herein.

2.2 Government documents. The following government documents form a part of this handbook to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the latest issue of the Department of Defense Index of Specifications and Standards (DoDISS) and supplement thereto.

a. Security Enterprise Integration Working Group (SEIWG), SEIWG-012, *Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC)*, February 28, 1994.

b. U.S. Department of Defense, DoD 8320.1-M-1, "DoD Data Element Standardization Procedures," January 1993.

c. U.S. Department of Defense, DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

d. U.S. Department of Defense, National Computer Security Center (NCSC), I-942-TR-003, *Information Systems Security Policy Guidelines*, July 1994.

(Unless otherwise indicated, copies of the above documents are available from the DISA/JIEO Center for Standards, ATTN: PIC Military Handbook, 10701 Parkridge Blvd., Reston, VA 20191-4398.)

2.3 Non-Government publications. The following document(s) form a part of this document to the extent specified herein. Unless otherwise specified, the issues of the documents which are DoD adopted are those listed in the latest issue of the DoDISS, and supplement thereto.

a. Automatic Identification Manufacturers (AIM) USA, ANSI/AIM BC-1-1995, *Uniform Symbology Specification Code 39*, June 1993.

b. Automatic Identification Manufacturers (AIM) USA, *PDF-417*, July 1994.

c. ISO/IEC 7810: 1995, *Identification Cards - Physical Characteristics*, August 15, 1995.

d. ISO/IEC 7811-2: 1994, *Identification Cards - Recording Techniques - Part 2: Magnetic Stripe*, August 15, 1995.

e. ISO/IEC 7811-4: 1994, *Identification Cards - Recording Techniques - Part 4: Location of Read-only Magnetic Tracks - Tracks 1 and 2*, August 15, 1995.

f. ISO/IEC 7811-5: 1994, *Identification Cards - Recording Techniques - Part 5: Location of Read-only Magnetic Track - Track 3*, August 15, 1995.

g. ISO/IEC 7811-6: 1995, *Identification Cards - Recording Technique - Part 6: Magnetic Stripe - High Coercivity*, August 15, 1995.

h. ISO/IEC 7816-1: 1987, *Identification Cards - Integrated Circuits(s) with Contacts - Part 1: Physical Characteristics*, July 1, 1987.

i. ISO/IEC 7816-2: 1988, *Identification Cards - Integrated Circuits(s) with Contacts - Part 2: Dimensions and Location of the Contacts*, May 15, 1988.

j. ISO/IEC 7816-3: 1989/Amd. 2: 1994, *Identification Cards - Integrated Circuits(s) with Contacts - Part 3: Electronic Signals and Transmission Protocols, Amendment 2: Revision of Protocol Type Selection*, December 1, 1994.

k. ISO/IEC 7816-4: 1995, *Identification Cards - Integrated Circuits(s) with Contacts - Part 4: Interindustry Commands for Interchange*, September 1, 1995.

(Unless otherwise indicated, copies of the above documents are available from ANSI (American National Standards Institute), 1430 Broadway, New York, NY 10018; Phone (212) 642-4900.)

2.4 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Acronyms used in this standard. The acronyms used in this standard are defined as follows:

AIM	-	Automatic Identification Manufacturers
AIS	-	Automated Information System
ANSI	-	American National Standards Institute
API	-	application programming interface
ASCII	-	American Standard Code for Information Interchange
ASD	-	Assistant Secretary of Defense
ASM	-	Application Security Module
ASN.1	-	Abstract Syntax Notation 1, as defined in ISO/IEC 8824
ATR	-	Answer to reset, as defined in ISO/IEC 7816-3
C3I	-	Command, Control, Communications, and Intelligence
CFS	-	Center for Standards
COS	-	Chip or Card Operating System
COTS	-	commercial off-the-shelf
DDDS	-	Defense Data Dictionary System
DISA	-	Defense Information Systems Agency
DLL	-	Dynamic Link Library
DoD	-	Department of Defense
DoDD	-	DoD Directive
DOS	-	disk operating system
EIA	-	Electronics Industries Association
EMV	-	Europay, MasterCard, and Visa

FIPS	-	Federal Information Processing Standard
FSCUG	-	Federal Smart Card User Group
GOTS	-	government off-the-shelf
HRI	-	Human Readable Interpretation
IC	-	integrated circuit(s)
ICC	-	integrated circuit card
IEC	-	International Electrotechnical Commission
IEEE	-	Institute for Electrical and Electronics Engineers
ISO	-	International Organization for Standardization
ISSP	-	Information System Security Policy
ITPB	-	Information Technology Policy Board
JEIDA	-	Japanese Electronic Industry Development Association
MARC	-	Multi-Technology Automated Reader Card
MIL-STD	-	Military Standard
MSC	-	Magnetic Stripe Credentials
NCSC	-	National Computer Security Center
NIST	-	National Institute of Standards and Technology
NSA	-	National Security Agency
OCX	-	OLE Control
ODBC	-	open database connectivity
OLE	-	object linking and embedding
O/S	-	operating system
OSD	-	Office of the Secretary of Defense
OSE	-	Open System Environment
PCMCIA	-	Personal Computer Memory Card International Association

PDF	-	Portable Data File
PI^2	-	PIC Integration Interface
PIC	-	Portable Information Carrier
PICSWG	-	PIC Standards Working Group
PIN	-	personal identification number
P&R	-	Personnel and Readiness
PROM	-	programmable read-only memory
PUB	-	Publication
PVC	-	polyvinyl chloride
PVCA	-	polyvinyl chloride acetate
RFID	-	radio frequency identification
SBU	-	Sensitive But Unclassified
SCC	-	Standards Coordinating Committee
SCF	-	Smart Card Forum
SCQL	-	Structured Card Query Language
SCUI	-	Smart Card User Interface
SQL	-	Structured Query Language
SSN	-	Social Security Number
STD	-	Standard
TAFIM	-	Technical Architecture Framework for Information Management
TLV	-	Tag, Length, Value
UL	-	Underwriters Laboratories
USS	-	Uniform Symbology Specification
VBX	-	Visual Basic Extensions

3.2 Access control. A process that moderates which data elements can be read, written, or erased by applications.

3.3 Active. An action that results in response to an outside stimulation such as providing a response to the signals entered into a PIC.

3.4 Algorithm. A computational procedure used for performing a set of tasks such as encryption/decryption processes.

3.5 Answer to reset (ATR) file. An optional elementary file, as defined in ISO/IEC 7816-4.

3.6 Anti-tearing. The process or processes that prevent data loss when a smart card is withdrawn from the contacts during a data operation.

3.7 Authenticate. To verify the identity of a user, user device, other entity, or the integrity of data stored, transmitted, or exposed to unauthorized modification in an information system.

3.8 Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

3.9 Authenticator. Means used to confirm the identity of a station, originator, or individual.

3.10 Authorization. The process by which a company guarantees an action made to a reader device by a PIC user, which involves taking appropriate steps to check the validity of the transaction. The guarantee is subject to certain procedures which will be carried out by the reader device, controlled by the particular application.

3.11 Biometric. A unique personal characteristic such as a signature, hand geometry, or fingerprint.

3.12 Cardholder. The person or entity to whom a PIC is issued.

3.13 Card reader. Equipment capable of reading the information on a PIC, such as that in the magnetic stripe or chip.

3.14 Card version. Refers to the specific Integrated Circuit (IC) model, IC size, and data model in use on a PIC.

3.15 Chip. A small piece of thin semiconductor material, such as silicon, that has been chemically processed to have a specific set of electrical characteristics such as circuits, storage, or logic elements.

3.16 Chip card. A card containing an integrated circuit. It can be a microprocessor or a simple memory chip.

3.17 Chip or card operating system (COS). A set of instructions permanently burned into the programmable read-only memory (PROM) of an ICC or built into the ICC during manufacture as mask PROM. The instructions usually constitute some primary security and memory management functions.

3.18 Contact. An electrical connecting surface between an ICC and its interfacing device that permits a flow of current.

3.19 Debit card. A card used for drawing cash from machines or for paying for retail purchases. Unlike credit cards, debit cards are linked to currency in the form of checking or savings accounts.

3.20 Dictionary. View on a system table.

3.21 Digital signature. A unique binary number generated by a digital signature algorithm and appended to a file or data.

3.22 Digital signature algorithm. An algorithm which appends data to, or performs a cryptographic transformation of, a data unit. The appended data or cryptographic transformation protects against modification.

3.23 Exception. A transaction that does not receive authorization by the accepted rules and procedures.

3.24 Hashing. Iterative process which computes a value (hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable.

3.25 International Organization for Standardization. A worldwide federation of national standards bodies from some 100 countries, one from each country.

3.26 Key. A value that particularizes the use of a cryptographic system. See also private key cryptography and public key cryptography.

3.27 Key management. The process by which keys are generated, stored, protected, transferred, loaded, used, and destroyed.

3.28 Nonvolatile memory. Memory that retains its content when power is removed.

3.29 On-chip applications. DoD applications that reside on the ICC.

3.30 Open Systems Environment (OSE). A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

3.31 Operating system (O/S) interface layer. The layer that allows for the interconnection and interrelationship among the various operating systems in the form of two or more devices, applications, and the user interfacing with an application or device.

3.32 Personal identification number (PIN). Numbers used to identify a user. A PIN is normally four or more digits long.

3.33 Portable Information Carrier (PIC). A portable device which contains one or more technologies used to store information related to an individual and used in one or more applications. It may contain both updatable and static technologies such as an integrated circuit chip, magnetic stripe, bar code, and printed media.

3.34 Private key cryptography. Encryption methodology in which the encryptor and decryptor use the same key, which is kept secret.

3.35 Public key cryptography. Encryption system that uses a linked pair of keys; one key encrypts, the other key decrypts.

3.36 Reader/writer driver layer. The layer in various reader and writer devices that pulls information from, writes to, or erases segments or zones of a PIC.

3.37 Security. Features and procedures used to reduce the possibility of fraudulent use or subversion.

3.38 Smart card. A chip card containing a microprocessor, which therefore is capable of calculation as well as memory.

3.39 Storage. An electronic or mechanical-magnetic device that holds information for subsequent use or retrieval.

3.40 Table. Database object with a unique name and structured in columns and rows.

3.41 Tampering. Unauthorized modification that alters the proper functioning of the PIC.

3.42 User. The person presenting a PIC for a transaction or process. The user may or may not be the cardholder to whom the card was issued.

3.43 Virtual card. The data elements contained in the data indices without regard for physical addresses.

4. DATA MANAGEMENT

4.1 Overview. There are two types of data management: (1) overall guidance which ensures a DoD PIC is standard in its configuration across DoD so a PIC can be used throughout the services and the DoD; and (2) technical data management standards, processes, and design parameters which enable applications to operate while complying with security and data integrity. Appendix B lists assumptions made in the development of this and subsequent sections.

4.2 Functional concepts for operational PIC program(s). The operational concept presumes that DoD implements a PIC program that is supported by a DoD PIC management infrastructure and that a configuration control process is in place to manage the process of standardizing PIC technology, data modeling, and business processes. Such management is essential to prevent inefficiencies, waste, or even failures that would occur if PIC technology were implemented piecemeal.

Data management involves deciding what is approved to go on a PIC. It is presumed that DoD will set up oversight for policy on and fielding of PIC technology, including the following:

a. DoD PIC management infrastructure.

b. Requirements process.

c. Configuration control process.

- Joint-service in scope.
- Joint-functional area in scope.
- Topics such as allocation of "real estate" on the chip, data models.

d. Funding authority and funds.

Functional application managers responsible for designing, fielding, and implementing applications will be expected to plan and field each application in an operational mode. During development of the application, it will be important for the functional managers to integrate input from DoD and DoD proponents for that application and

work with the DoD PIC management infrastructure to ensure that their requirements can be implemented in the DoD PIC.

4.3 Data inclusion and categorization. Data available in a central database as part of an exclusive application would not normally be put on the carrier. This saves space and reduces redundancy. The data will be unclassified, but can be SBU, requiring access control; encryption would not normally be applied, but could be used if the application manager determines it necessary. For clarification of this and other security-related issues pertaining to the PIC, refer to section 7.

A data element will be stored only once on the chip. To be added to the PIC, a data element will be requested by at least one proponent. Data on the PIC will be a copy of data maintained elsewhere, with some exceptions such as field medical data. Data will be stored on the PIC as DoD standard elements and codes (DoD 8320.1-M-1, "DoD Data Element Standardization Procedures," January 1993).

When evaluating a data element for inclusion on the PIC, it should be noted that data elements which change frequently, in order to maintain the business process, will require a support infrastructure (equipment, staff). Appendix C provides information regarding the utilization of the chip.

4.4 Data modification/maintenance. Data management and modification are performed via the PI^2 described in detail in section 5. Assumptions underlying the data management process include several factors. For example, application operators may make modifications only to their functional areas. The data management process is expected to ensure PIC data can be locked when/if:

a. A card is shown to be no longer valid.

b. Non-approved applications attempt to modify data.

Data elements on the bar code or print media should also be on the chip. Data on the magnetic stripe may also be on the chip. Data on bar code and print media will be static (change very infrequently), which would be the case with data elements such as name and Social Security Number (SSN). To take advantage of the updatable chip technology, it would be counterproductive to place data elements that change in the printed media (bar code or text), because changes in the information would require total reissue of the PIC.

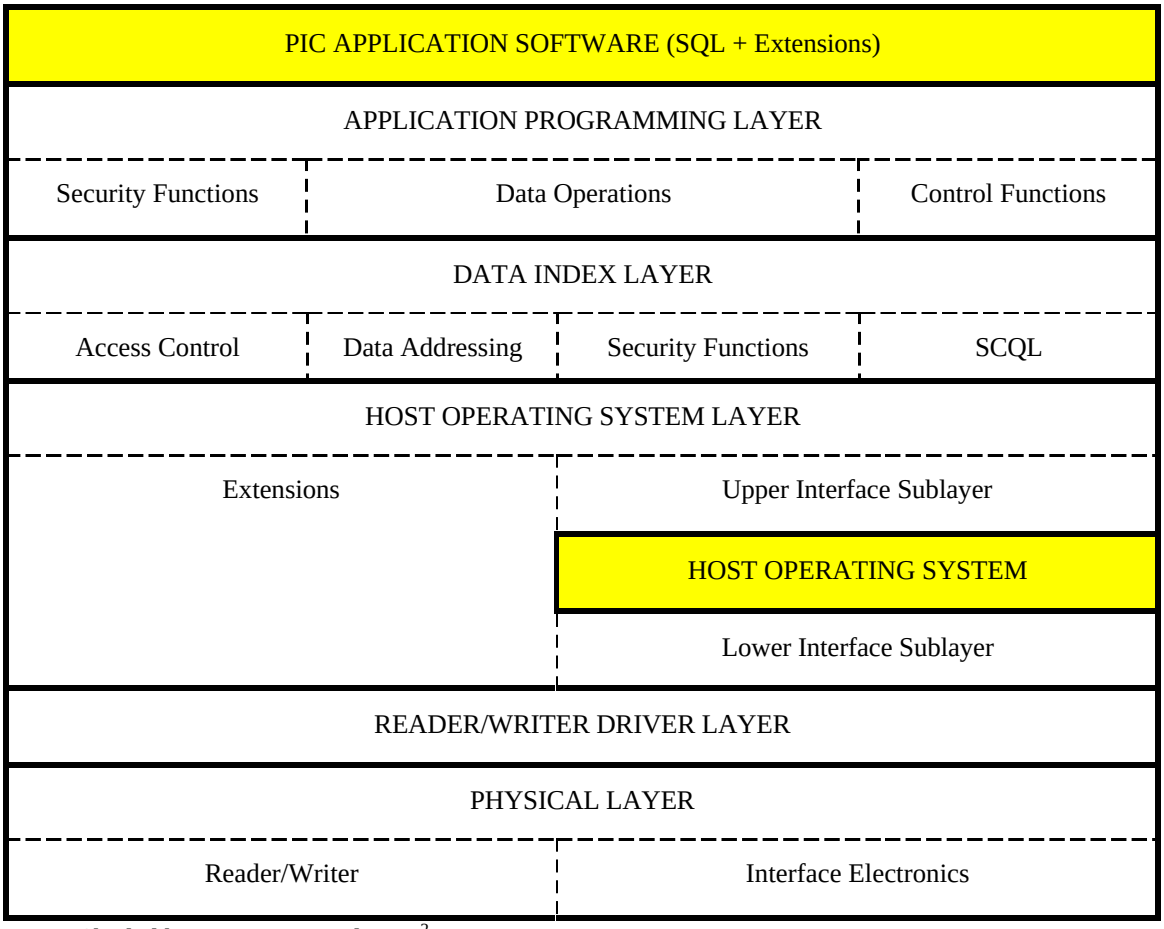
Data on the chip will be capable of being completely erased or overwritten and not merely deleted by changing a directory reference. This function will be controlled.

4.5 External (outside DoD) application interfaces. The overall DoD PIC management infrastructure and centrally managed configuration control process (see paragraph 4.2) are expected to set policy, procedures, and guidance to ensure DoD PIC devices can interface with other Federal card programs for which common functions are envisioned. If commercial credit/debit functions are used, they will be compliant with existing standards. If the PIC configuration control process determines there should be data areas for personal applications such as credit cards, civilian associations, ATMs, video rental, and library, the configuration control process would need to designate an area on the chip for such applications.

5. PIC INTEGRATION INTERFACE (PI^2)

5.1 Overview. The subsystem required to allow a PIC user's application software, operating on a computer workstation, to access and maintain the PIC is a layered structure as shown on figures 1 and 2. The shaded areas represent components outside the PI^2. These layers will be implemented as a collection of callable libraries provided by the Government and third party software vendors, drivers provided by smart card and smart

card reader/writer suppliers, reader/writer equipment, and smart card electronics and operating systems. The first five layers represent the workstation interface structure beginning with the application programming interface layer and extending down to the electrical, electronic, and mechanical reader/writer physical layer. The bottom three layers of the structure are the PIC interface structure that represents the electrical and electronic card physical layer that interfaces with the reader/writer extending into the PIC on-chip applications in which the data are stored on the PIC.



NOTE: 1. Shaded boxes are external to PI^2.

FIGURE 1. Workstation interface structure

A data index registry contains a data index (dictionary) for each card type and each version of data structure used, both currently and in the past. The workstation interface can determine which index to use when it identifies a card type and data structure version of the card in the reader/writer. The registry consists of several parts, each defined by the responsible development authority - DoD PIC management infrastructure, service PIC implementation offices, and local developers. These apply only to those open data areas allocated to those activities by higher authorities. Each data index shows the access privileges for each authorization type and data element or group of elements.

The PI^2 guidance provides sufficient flexibility to evolve along with the technology and the interfaces to the multiple programs and missions the PIC program is addressing in DoD.

The guidance encourages integration of advanced technology and software into the PIC program. The ability to read past data structures should be maintained for at least two previous versions. The PI^2 presented in this section is an attempt to provide such guidance as to allow for improved integration interfaces.

The basic PI^2 layers are presented on figures 1 and 2. These layers are not intended to be an extension of the seven layer model presented in the DoD Technical Architecture Framework for Information Management (TAFIM), but as guidance for the operation of PIC technology in DoD.

Every application, interface, report generator, API, data layer, and data call using a date format will demonstrate year 2000 compliance. Year 2000 compliance is defined, for purposes of this PIC guidance, as the ability to demonstrate that all date manipulations and date logic formats result in correct calculations when run under conditions that go past the year 2000.

The database access should comply with ISO/IEC 9075:1992, *Information Technology - Database Languages - SQL2*. Future applications may use object-oriented database access calls.

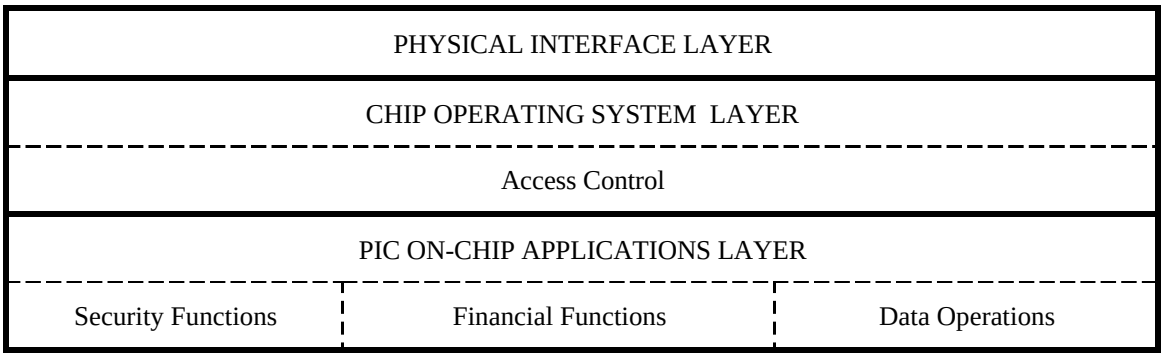


FIGURE 2. PIC interface structure

There are two layered structures that allow the workstations to access the PIC. The first is the workstation interface structure which contains five layers as shown on figure 1. The second structure is the PIC interface structure which contains three layers as shown on figure 2. The workstation interface structure will interface with the PIC interface structure to allow all requests and application interfaces to pass through the functions from the layer above and below in a way that is seamless and invisible to the user. The workstation interface structure layers are:

a. The PIC user application software is external to the PI^2 but will conform to the interface guidance presented in this document. The PIC user application software will be left to the individual mission and the supported software systems. The PIC user application software will conform to and interoperate with the PIC in a seamless manner allowing for existing functions to operate.

b. The application programming interface layer supports all the API system calls for PIC data and control functions made from PIC application(s) software.

c. The data index layer contains the registry information to determine the card type and version, verifies authorization for access, translates data operations functions into chip memory addresses, and manages data and control activities.

d. The host operating system layer includes the operating system (external to this guidance), routines to interface nonstandard operating systems with the upper layer, routines to interface nonstandard drivers with the operating system, and extensions for reader/writer functions not supported in the operating system.

e. The reader/writer driver layer consists of drivers provided by the device manufacturer and interoperable with major chip manufacturers.

f. The physical layer consists of the reader/writer, its electronic interface with the computer, and the PIC.

The PIC interface structure will interface with the workstation interface structure to allow all requests and application interfaces to pass through the functions from the layer above and below in a way that is seamless and invisible to the user. The layers of the PIC interface structure and their functions are, as follows:

a. The physical layer presents chip type identification information to the reader.

b. The chip operating system interprets commands sent by the application(s) workstation(s) and carries out the requested functions in accordance with the permissions and privileges of the application and requester.

c. The PIC on-chip applications consist of specific pre-packaged or user-developed functions performed on the chip.

Security functions will be implemented in all appropriate layers as well as in the various mission applications interfacing with the PIC.

Each data index contains a current data dictionary specific to the card version in effect. The indices will consist of several parts with each part containing indices defined by the responsible development authority. The service and local indices will only apply to those open data areas allocated to those activities by higher authorities. The indices are used to determine the authorization for access to a data element or group of elements.

The data indices identify the card type and data structure versions. The data indices will be used to address and access data.

5.2 Workstation application layers.

5.2.1 PIC user application software. The PIC user application software is external to the PI^2 but will conform to the interface guidance presented here.

5.2.2 Application programming layer. The application programming layer supports all the PIC user's application software calls for PIC data and control functions. This layer interprets the calls, verifies appropriateness relative to sequence of operations and availability of data indexing structures, and issues lower level calls to the data index layer. This layer includes the capability to pass a data index registry of user-provided data indexing, version, and authorization information to the data index layer. It also passes back a data index applicable to a specific transaction and includes the capability to pass event status and result messages to the user when the interface determines that a condition needs user response.

5.2.2.1 Security functions. PIC libraries provided to developers contain no information about where data is stored on the PIC or how to manipulate the data. An application sees only the data needed. Application data contains just enough information to access that data and information needed to decrypt the data if required.

Application programming layer participation in PIC security may include prompting for PINs. Other security functions are hidden from the PIC user inside the PI^2. Detailed security considerations are described in section 7.

5.2.2.2 Data operations. There will be a minimum of five data operations to maintain and use data on a PIC. These data operations are as follows:

a. Review - Request retrieval of one or more data elements for display or use in an application.

b. Update - Request change of the data in one or more fixed data elements.

c. Add - Request storage of a new transaction as a set of data elements in a table structure.

d. Delete - Request removal of one or more transaction data sets from a table structure.

e. Modify - Request change of one or more data elements in a transaction data set stored previously in a table structure.

These data operations are for maintenance of data elements available for use in applications. This paradigm assumes there are two types of data - fixed data and transactions. Fixed data (e.g., name and date of birth) appears only once on the PIC and is stored and maintained in specific locations as defined by the data index. A transaction (e.g., type and date of shot or date and time of last PIC access) is stored as a data set in a row of a table and may result in multiple data sets depending how many times the card is used for the function. Transactions may be deleted after retrieval by an application or when "bumped" by a more recent transaction.

The data model is also defined by a set of data elements (e.g., version, data element name, data length, data characteristics, storage location, and access privileges) stored on the PIC. These data elements can be changed using the same set of data operations in the foregoing list but only by applications with data model access privileges. These applications can add and delete data elements, increase or decrease the size of a data element, or change its storage location. Deleting data elements results in contraction of the data model and elimination of obsolete data elements to free up space for other use. The data operations can be automatically invoked whenever a PIC with an out-of-date data model version is encountered.

5.2.2.3 Control functions. PIC control functions should be written in an open systems programming language to insure the vast majority of PI^2 functions are simply recompiled in different operating systems. The following operating systems' dependent function calls should be isolated to separate libraries to facilitate usage of PI^2 across operation systems:

a. clkticks() Get the number of clock ticks since midnight.
b. cleanup() Close the specified port and perform whatever house cleaning activities are necessary.
c. detain() Pause execution of program for a specified number of milliseconds.
d. openport() Open the specified port.
e. flushbuf() Reinitialize the port input (or output) buffers.
f. putblock() Send a block of data out the specified port.
g. rdchrtmd() Read a single character from the port input buffer.

Other modifications may be appropriate for the Windows-based operating system as those modifications deal with Dynamic Link Library (DLL) considerations.

5.2.3 Data index layer. The data index layer uses data indices to give applications seamless access to various data models. This is performed by taking the higher level data operations functions and implementing

these functions as the sequence of PIC operating system commands necessary to obtain the data for this application. Implicit in this layer is the management of passwords, encryption keys, data elements, and access privileges for each data element.

The data index layer determines the card type, card version, and applicable data indices. It contains tables specifying authorizations for access, translates data operations functions into chip memory addresses, and manages data and control activities. The calls from this layer to lower layers and the data structures passed are expected to comply with ISO/IEC 7816-4, 5, and 6. The data index layer provides a virtual card that is implemented across different card types. No portions of the PI^2 contain any PIC authorization passwords, encryption keys, data element information, or data element access data.

The PI^2 libraries should be the same for all applications. The differentiating aspect of these applications is the application data provided to the PI^2 and the structure the application uses to accept the PIC data.

5.2.3.1 Access control. Access control is a process that determines which data elements are read, written, or erased by applications. Access control allows retrieval of data via requests through the data index layer. The data index, combined with access control, will allow single data entry with multiple retrieval. The exception can be data utilizing the scratch pad portion of the PIC. Detailed security considerations are described in section 6.

Access control will include the following:

a. Identification/authentication (PIN, PIN verify).
b. Describe the PIC data formats (set data index registry, set appropriate data index).
c. Get appropriate card data format.

5.2.3.2 Data addressing. Data addressing will consist of the following:

a. Validate access privileges for data elements.
b. Pass data to/from the application interface and card.
   - Data element location.
   - Data element name.
c. Provide database indexing and data element authorization services.

5.2.3.3 Security functions. Security functions will consist of the following:

a. Opening of session.
b. PIC unique number transmission and validation.
c. PIN prompting (if required).
d. Application password(s) transmission to ICC for validation on the ICC.
e. Transmission of date to the ICC for validity period check.
f. Access to authorized data.
g. Closing of session.

Application owners using the PIC will be responsible for security functions at this level which may include auditing, logging, and history files. These files should be retained in the application database where possible, not on the PIC. The PIC will provide a card identification string to the application.

5.2.3.4 Calls from data index layer to host operating system layer. A PIC is intended for information exchange as negotiated between the outside application(s) and the integrated circuit in the card. As a result of an information exchange, the card may deliver information or modify its content. This is accomplished through the

PI^2. The actual storage location of data and structural information will be in accordance with the appropriate data model.

The PIC data index layer is independent of the host operating system. Operating systems will utilize PI^2 timing calls and serial port manipulation calls when either is required.

5.2.3.4.1 Structured card query language (SCQL). When SCQL is implemented, any database in an ICC is called an SCQL database. Currently all the commands for accessing structured databases in an ICC are a subset of structured query language (SQL). A database may be attached to a master file associated with one or more applications.

This does not restrict the use of object-oriented applications and the creation of objects, messages, and classes of objects which may replace the standard SQL-API solutions. Likewise, abstract data types and the construction of intelligent databases are encouraged, but at the time of the preparation of this document were not commonly used in ICC technology and the related PI^2 functions. Appendix D provides additional considerations regarding SCQL.

5.2.3.4.2 Activation of on-chip applications. On-chip applications will conform to ISO/IEC 7816-5.

5.2.3.4.3 Data index layer extensions. Examples of possible extensions include Get Scratchpad and Put Scratchpad.

5.2.4 Host operating system layer. The host operating system layer includes the upper interface sublayer routines to provide portability of the higher layers among host operating systems, lower interface sublayer routines to provide portability of the drivers among host operating systems, and extensions to support reader/writer functions that are not supportable through the host operating system. The host operating system, such as DOS, Windows, or UNIX, is considered external to the PI^2.

The host operating system layer includes the operating system, routines to interface nonstandard operating systems with the higher layers, routines to interface nonstandard drivers with the operating system, and extensions for reader/writer functions not supported in the operating system. This layer adapts user interface data, input/output, and service functions to specific reader drivers and vice versa.

Host operating systems will be POSIX compliant and will be able to interface with a reader/writer device if they are to use a PIC in an application.

5.2.4.1 Upper interface sublayer. The upper interface sublayer functions will consist of a mechanism that converts data strings to a format compatible with the host operating system port calls and reader/writer commands.

5.2.4.2 Host operating system. The host operating system is external to the PI^2 but will conform to the interface guidance presented here.

5.2.4.3 Lower interface sublayer. Lower interface functions will take the general reader/writer driver and adapt it to the host operating system specific to that device. Standard communications port drivers may satisfy the this function.

5.2.4.4 Host operating system extensions. All extensions fall back to the physical layers of the host operating system. Extensions support reader/writer functions not supportable through the host operating system. The host operating system, such as DOS, Windows, or UNIX, is considered external to the PI^2.

5.2.5 Reader/writer driver layer. The reader/writer driver layer consists of drivers to interface with the host operating system. Standard communications port drivers may satisfy this function. Data operations will consist of passing data streams between the workstation and the PIC. This software is expected to support control functions such as sensing insertion of the card and ejection at the end. Physical attributes of this layer are covered in section 8.

5.2.6 Physical layer. The physical layer consists of the reader/writer, its electronic interface with the computer, and the PIC.

5.2.6.1 Reader/writer. Reader/writer functions will be functionally and electronically compliant with specifications for a serial bus, such as RS 232 (*Electronic Industries Association (EIA) - 232-D*) or PC Card Type (*PCMCIA Standard Release 2.1/Japanese Electronic Industry Development Association (JEIDA) 4.2*) for all vendors and devices. Additional specifications are contained in section 9.

5.2.6.2 Interface electronics. Interface electronics functions will be consistent with ISO/IEC 7816-3, *Electronic Signals and Transmission Protocols*.

5.3 PIC interface layer structure. A PIC will be ISO/IEC 7816 compliant. This applies to all chip capacities and operating systems. A PIC should be fully interoperable in all the appropriate operating systems.

5.3.1 Physical interface. The PIC will comply with ISO/IEC 7816-3 with respect to the dialogue between the interface device and the card for all card stages. These stages range from insertion of the PIC into the interface device through the execution of the transaction to the removal of the PIC from the interface device. Card identification, contacts, and power will comply with the specifications in section 8.

5.3.2 Chip operating system layers[1]. The chip operating system interprets commands sent by the workstation and carries out the requested functions. The commands will be compliant with ISO/IEC 7816-4 and ISO/IEC 7816-5. This layer consists of access control.

Access control for the PIC should be performed with a minimum of application input. The applications should perform appropriate set-up functions which will utilize card security functions.

5.3.3 PIC on-chip applications. PIC on-chip applications are part of the chip operating system (COS) on the PIC and cannot be easily recalled for updates and maintenance.

5.3.3.1 Security functions. PIC on-chip security functions represent a potentially high level of data and system security. Many security algorithms have significant memory requirements and require a large number of operations to execute. Use of these applications provides increased security against "out of system" attacks on the data. These measures cannot defend against "in system" attacks where authorized personnel use the system to improperly update or access data. Security considerations are described in section 7.

[1] Due to the diversity of card operating systems available for use in a PIC, there is a substantial variation in the type of order-of-function calls made.

5.3.3.2 Financial functions. Credit/debit functions should be compliant with the Europay, MasterCard, and VISA (EMV) specifications.

Warning: Functions such as financial, banking, or purse/cache will require careful review before implementation on the PIC. Safeguarding data stored in the card may become more difficult due to the nature of these functions; however, defining the potential for these problems is beyond the scope of this document. Additionally, the value of the money that may be accessed with the card may make it a target for fraud, theft, or hacking.

5.3.3.3 Data operations. The PIC will be able to write data to its memory and data will be read out of the PIC memory.

6. APPLICATION PROGRAMMING INTERFACE (API)

6.1 Overview. When a requirement for a PIC is determined, based on the card profile, a resource kit comprised of specific API calls and other relevant data will be provided to application developers by the DoD PIC management infrastructure. Where applicable, the ISO/IEC 7816 series should be used as a guide. Applications supporting PIC implementation must meet at least Level 5 compliancy with the Defense Information Infrastructure (DII) Common Operating Environment (COE) as defined in the *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS),* Preliminary Version 2.0, October 23, 1995.

6.2 Application programming interface functions. The API calls will support static linking into an open systems programming language library, Windows 3.11 16-bit DLL, Windows 95 and NT 16-bit DLLs, Windows 95 and NT 32-bit DLLs, and a client/server architecture. Additionally, support of DLLs, Object Linking and Embedding (OLE) Controls (OCXs), and Visual Basic Extensions (VBXs) and access by Open Database Connectivity (ODBC) methods are desired. This additional support should not be cost prohibitive.

6.3 Data index registration functions. The PIC API will mask from the application the information about the management of the readers and the PIC. As an example, during setup, the PIN within the card is not reported to the application, but is passed by the PI^2. After this setup function is called, the application simply calls the data operation functions appropriate for this application. The internal workings of the PI^2 are hidden from the user just as the internal workings of a database or port handler are hidden from calling applications.

6.4 Security/access control functions. Security calls include registration and logging of authorization along with sign-on information if PIN entries are made through the console keyboard. Audit trail reports could also be obtained through these calls. A PIC should support the development of verification routines for a PIC to authenticate itself to a reader, and for a reader to authenticate itself to a PIC.

The PIC API does not provide registration and logging functions, although the capability is provided through the return of the application. The API security is set up as shown in table I.

Additional security may be provided by the application in a variety of ways.

Detailed security considerations are described in section 7.

TABLE I. API security

Entity	Physical Requirements	Logical Requirements
Application user	API, Application, Reader	Application PIN
PIC holder	PIC	PIC PIN
Application	API, Application, Reader	PIC design in API and application data

6.5 Control functions. Control functions, such as automatic eject, can be dependent upon the hardware. These calls would include status checks on the reader, card eject commands, and reset commands to clean up after aborted applications. Control functions should be compliant with ISO/IEC 7816 to the extent possible.

6.6 Operating system layer. The operating system layer allows portability of the higher layers to other operating systems, driver compatibility with various operating systems, and control of enhanced features (extensions) that cannot be exercised through the operating system.

6.7 Reader/writer driver layer. The reader/writer driver layer processes the data stream and will identify data to be passed to the PIC or reader. Compliance with ISO/IEC 7816 is desired.

6.8 Year 2000 compliance. PIC-related computer equipment, software, and systems delivered to the government by the offeror will perform as follows:

a. The contractor warrants fault-free performance in the processing of date and date-related data (including, but not limited to, calculating, comparing, and sequencing) by all hardware and software products delivered, individually and in combination, upon installation. Fault-free performance includes the manipulation of this data with dates prior to, through, and beyond January 1, 2000, and will be transparent to the user. Fault-free performance applies to the PIC deliverables and does not include integration and interfaces with data and applications developed externally to PIC. However, flags for other date error checking capability are strongly encouraged when interfacing with applications external to the PIC program.

b. All PIC system performance will also account for the allowance of the year 2000 being a leap year and therefore will include February 29, 2000 in the processing of the date and date-related data. (Traditional calculations of leap year skip years ending in "00," but 2000 is an exception to that rule.)

c. Hardware and software products, individually and in combination, will successfully transition into the year 2000 with the correct system date, without human intervention, including leap year calculations. Hardware and software products, individually and in combination, will also provide correct results when moving forward or backward in time across the year 2000.

Modifications of existing software/systems and computer equipment, software, and systems delivered to DoD but modified for the PIC implementation will perform as follows:

a. The contractor warrants proper processing performance in the processing of date and date-related data (including, but not limited to, calculating, comparing, and sequencing). Proper processing performance includes

the manipulation of this data with dates prior to, through, and beyond January 1, 2000, and will be transparent to the user.

b. Hardware and software products, individually and in combination, will successfully transition into the year 2000 with the correct system date, without human intervention, including leap year calculations. Hardware and software products, individually and in combination, will also provide correct results when moving forward or backward in time across the year 2000.

6.8.1 User layer. User interfaces and reports will account for the century in a manner acceptable to the end users. Date-related data will appear correctly in the DoD standard format (yyyy/mm/dd) or other application acceptable format. If date data is used in tables, it will appear in correctly sorted order (the date 2000 will come after 1999 in ascending order and before in descending order sorts). Any variant will be approved by the user community and the DoD PIC management infrastructure. All databases and applications interfacing to the PIC will use the DoD standard format. Compliance to this section of the PIC will include the following features and capabilities (at minimum):

a. All sorts are correct.

b. Four-digit year display fields.

c. Four-digit year report fields.

d. Data entry accommodates century where appropriate.

e. Formal approval from end users and DoD PIC management infrastructure for exceptions.

f. Optional: Date check for all incoming data and information from applications external to PIC development with appropriate flags for possible errors.

6.8.2 Logical layer. All PIC host operating systems and applications will show proof of properly processing date routine logic. This will apply to the processing time horizon (applications spanning the century boundary) as well as accurate processing of date-related fields and calculations involving those fields. If the date processing is routed through a common processing thread (subroutine), proof of the thread's compliance to the DoD PIC management infrastructure will suffice. Compliance will include the following features and capabilities (at minimum):

a. Correct date calculation.

b. Correct acceptance of dates from the operating system.

c. Correct calculation of resultant values based on dates.

d. Correct calculation of year 2000 as a leap year.

e. Correct direct and indirect data field sizes.

f. Optional: Logic check for all incoming data and information from applications external to PIC development.

6.8.3 Interface layer. All uploaded and downloaded (upstream and downstream) interfaces, ad hoc interfaces and queries, and APIs (either calling or called) will be certified for year 2000 PIC compliance. Both date field formats and calculations relying on dates passed through interfaces will be certified. If coordination is required with a different DoD component or other government application, the interfacing application will be compliant. Proof of compliance should be required from all processing partners to protect against transmission of faulty calculations through an interface. PIC compliance will include the following features and capabilities (at minimum):

a. Correct date format passing.
b. Correct value passing.
c. Partner date and report wording.
d. Identification of all interface points.
e. Correct leap year calculation for the year 2000.

6.8.4 Data layer. Data fields will be year 2000 compliant or PIC mission applications will have to be modified to accept a noncompliant storage format. When a noncompliant storage format is being used, approval will be obtained from the DoD PIC management infrastructure. DoD PIC management infrastructure approval can only be obtained after procedures and standards are in place to ensure future maintenance accommodates the noncompliant date fields during the processing of the time horizon. Additional tests will be run to ensure no unintended modification of functionality has occurred because of the year 2000 compliance changes. PIC year 2000 compliance will include the following features and capabilities (at minimum):

a. Identification of all data access points.
b. Four-digit year format (field expansion).
c. Identification of logic filter (if no field expansion).
d. Verification of present and future use of processing filter (if no field expansion).

7. SECURITY

7.1 Overview. The security of an information system employing a PIC depends upon both the characteristics and capabilities of the PIC itself and the infrastructures which issue, support, and use them. Since the PIC is intended to support multiple applications, the security implications of this sharing have to be addressed. The PIC is intended to contain only unclassified information; however, if the PIC is used in a device interfaced to a classified system, provisions of Executive Order 12958 and other applicable security classification directives have to be met. In general, the greatest threats and vulnerabilities are in the PIC infrastructure.

PIC security involves a variety of services, characteristics, and capabilities, including at least data confidentiality, data integrity, and data availability. Development of a DoD PIC application will consider its requirements in all of these areas, not only during routine operations, but especially in times of stress when an adversary may attempt to disrupt PIC dependent operations.

The PIC infrastructures may include, but are not limited to, those involved with PIC design; analysis; fabrication; testing; initialization; distribution; encryption key and digital signature key material generation, distribution, and loading; issuance to cardholder; cardholder data loading; cardholder data retrieval; cardholder data modification; cardholder data uploading to operational systems and to repositories; cardholder data downloading from repositories to replace damaged or lost cards; audit collection and analysis; commercial system interactions such as point of sale terminals, vending machines, and automatic teller machines; and eventual card replacement, retirement, and disposal. These infrastructures will be geographically distributed and interconnected via an assortment of both electronic networks and physical data transport mechanisms such as magnetic tapes or disks, and optical disks. The infrastructures will potentially involve connectivity between DoD, and possibly other

Federal agencies, state and local governments, service members and dependents, other government personnel, the general public, allies, and both domestic and international commercial entities. They will range from central facilities and databases/repositories, to intermediate level systems, to gateways to convert between incompatibilities of various kinds, and to the end workstations, readers, and terminals which will actually interface with the PIC.

An Information System Security Policy (ISSP) should be generated, in accordance with the ISSP handbook, for each major PIC infrastructure, and for each PIC application to support the certification and accreditation requirements of DoDD 5200.28. An ISSP should be developed in the context of the system to be protected to identify the mission security objectives and the rationale for each. This entails description and analysis of the mission and specific threats to the mission, and considers generic threat guidance (covering natural threats, inadvertent human threats, and deliberate human threats) and umbrella security guidance (applicable policies and guidelines derived from national, intermediate, and local policies). The ISSP should then be used in development of the system's security requirements, evaluation of alternative system architectures, and assessment of the security effectiveness of the system design, and implementation. DoD PIC applications, as a subset of a DoD automated information system (AIS), should be accredited in accordance with existing certification and accreditation requirements. Successful application of the ISSP should provide adequate protection for the critical information which is transmitted, carried, stored, and processed by the PIC and its infrastructures. The PIC application ISSP will consider not just the particular application itself, but all of the infrastructure group ISSPs which will be involved, and the ISSPs of the other applications which will share the PIC. This last requirement may involve re-addressing each PIC application ISSP each time a new PIC application is to be developed and potentially added. A way will be found to deal with non-Government applications which may not be bound by formal, enforceable ISSPs, if interaction with such applications is to be allowed.

7.2 General. This section applies only to the PIC and to the application that authorizes use of data stored on the PIC. It does not apply to the security of the infrastructure. The purposes of security for the PIC are to provide confidentiality, integrity, and availability of the data. The highest level of data storable on the PIC, both as individual data elements and in the aggregate, will be SBU. Enhanced versions of the PIC may be required to provide or to verify a digital signature. The mission will drive the PIC security profile required. The PIC, at a minimum, will validate the cardholder and may require his participation for operation of an application. PIC security requirements increase substantially for any usage above the basic PIC requirements. Some potential applications may have security requirements that cannot be satisfied by the PIC. The PIC may migrate to higher security levels in the future.

7.2.1 Audit. A PIC may contain an audit trail generated and maintained internally to enhance security.

7.2.2 Emergency destruction. Emergency destruction of the data in the PIC is through physical destruction of the integrated circuit(s).

7.3 PIC integrated circuit (IC) security profiles. PIC IC functional capabilities and access controls are defined for a candidate set of increasingly complex profiles presented in this section. These profiles are arranged in generally ascending order of PIC IC functionality, security protection, complexity, and cost. Each profile is summarized by a table. In this section, a PIC IC is intended to mean either a single IC embedded in a PIC, or a small number of interconnected ICs embedded in the PIC. The profile characteristics and table entries should be interpreted as discussed in the following sections.

7.3.1 PIC IC functions. Every PIC IC is intended to carry data in protected nonvolatile memory. Some may also have the capability of hashing, signing, and verifying files. The generic PIC functions are: granting read or write access to files, hashing files, calculating digital signatures, and verifying digital signatures. More sophisticated versions of a PIC which would incorporate key-based cryptographic capabilities for key exchange and data encryption are addressed in this section and are not currently addressed in other sections.

7.3.1.1 Grant file access. The PIC will be capable of controlling at least two modes of file access: read and write.

7.3.1.1.1 Access types. Section 5 previously identified five logical data operations functions (add, delete, modify, update, and review). The PIC IC performs two physical types of access, read and write. Erasure of data will be accomplished via overwriting of data to be deleted. The erasure bit pattern(s) and number of overwrites will be determined as appropriate for the memory elements of the technology employed on a particular PIC IC.

Read -- grants an application the ability to read the data elements of a file in a PIC IC.

Write -- grants an application the ability to write the data elements of a file in a PIC IC.

7.3.1.1.2 File types.

Public -- A file which is intended to hold electronic copies of the static information printed on the PIC, together with an updatable validity date for the PIC. This file can be read by an application without provision of any access credentials, even if the current validity period of the PIC has been exceeded. It can be written to only after entry of a cardholder's PIN and satisfaction of additional access control requirements by the application desiring to write. The application writing to this type of file will be capable of providing a new validity date for the PIC.

Scratch pad -- A file which can be read or written without entry of the cardholder's PIN, but which requires satisfaction of additional access control requirements by the application needing to write. This type of file may neither be accessed for reading nor for writing if the current validity period of the PIC has been exceeded.

Emergency scratch pad -- Emergency scratch pad is the same as a scratch pad with the exception that it may be accessed for reading and writing even if the current validity period of the card has been exceeded.

Private -- A file which can be read or written after entry of the cardholder's PIN and satisfaction of additional access control requirements by the application requesting authorization to write. This type of file may neither be accessed for reading nor for writing if the current validity period of the card has been exceeded. Access will be limited to a single application.

Shared private -- Shared private is the same as private with the exception that it is intended to be shared by two or more applications which require access to some of the same standard data elements.

7.3.1.2 Hash. If a PIC is capable of performing a hash function, the hash function will only be enabled after the cardholder has entered the PIN, and the application which requires the hashing to be performed has satisfied additional access control requirements. This function will not be enabled if the current validity period of the PIC has been exceeded.

7.3.1.3 Digital signature. If a PIC is capable of performing a digital signature function, the digital signature function will only be enabled after the cardholder has performed a validation operation, such as entering a PIN or performing a biometric scan, and the application which requires the hashing to be performed has satisfied additional access control requirements. This function will not be enabled if the validity period of the PIC has been exceeded.

7.3.2 PIC access controls. Read and write access to the various types of PIC files are to be protected via a graded set of access control security mechanisms. The common mechanisms used in the PIC profiles are defined in this section.

7.3.2.1 Public request. This access control mechanism enables any card reader which recognizes the PIC, and which can properly format a request, to obtain read access to "public information." Public information consists of the electronic copies of the data printed on the PIC. The expiration date of the validity period of the PIC will not be revealed in response to this type of request. The request is to supply the current date to the PIC for comparison with the limit of its validity period.

7.3.2.2 Cardholder PIN. This access control mechanism enables the cardholder to control read and write access to a file in the PIC, as appropriate to an application. The cardholder grants access to the file associated with the current application running in a computer associated with the card reader in which the cardholder's PIC is inserted by entering the PIN into the PIC reader or computer. The PIN is then supplied to the PIC IC for verification.

7.3.2.3 Password from application. This access control mechanism enables a PIC IC to limit access to a file of a password protected type by the application program associated with the PI^2. The application is required to provide the appropriate password or series of passwords, which are verified inside the PIC IC.

7.3.2.4 Validity period check. This access control mechanism enables a PIC IC to limit access to a file of a validity period protected type by the application program by requiring the application to provide the current date to the PIC IC. The PIC IC grants access to the file if the date supplied is prior to or equal to the date stored on the IC as of the end of the validity period.

7.3.2.5 Public key based encryption protection. Public key-based key exchange and encryption may be used to provide additional confidentiality, integrity, and availability protection to the data stored in a PIC IC, but definition of the requirements for such capabilities are presently beyond the scope of this document. This is because specification of such capabilities cannot reasonably be done without concurrent specification of the infrastructures which are to support them, and in which they are to be used. Two of the PIC profiles which follow, however, do address likely applications of such technology in the future by indicating the types of files which may benefit from this additional protection. Specification of algorithms should be done concurrently with the specification of the infrastructures to be involved. In general, it would be expected that the algorithms to be used would be selected from those specified in FIPS Pubs.

7.3.3 Profiles and scenarios. Four general types of PIC profiles are defined in this section. The first profile, Basic PIC, reflects current technology. The other profiles project the future growth path. Each profile is summarized via a table. In each table, access to a file, in the mode specified (either read or write), and ability to use the hash, digital signature, and digital signature verification algorithms, requires satisfaction of all of the access control requirements specified by an "X" in its row.

7.3.3.1 Basic PIC. The Basic PIC is defined in a way intended to allow economical implementation based upon readily available COTS smart card technology. It provides a minimal level of protection for the data it carries. Its security is based almost entirely upon protection of the PI^2 software, the card user's PIN, and the application passwords used.

7.3.3.1.1 Basic PIC applications. The Basic PIC is intended to carry Unclassified information, which in the aggregation over a single PIC, could reveal no more than SBU information. Single data elements should rarely, if ever, be allowed to reach the SBU level.

7.3.3.1.2 Basic PIC functions. The Basic PIC simply stores data and protects access to it via a variety of mechanisms. There are no cryptographic functions implemented on the Basic PIC. If encryption is required for additional protection of some or all of its data, the encryption is done by the application, and the PIC only stores the encrypted data. If some biometric verification is desired for an application, the biometric measurements and

comparisons would be tasks of the host system and the particular application. The Basic PIC would simply store and protect the biometric template of the cardholder, and provide it to the application (via the PI^2) upon satisfaction of the access controls required for the file type holding them.

7.3.3.1.3 Basic PIC access controls. The access controls for the Basic PIC are shown in table II. These access controls establish its protection profile.

TABLE II. Basic PIC profile

PIC Functions		PIC Access Controls				
		Public Request	PIN	Application Password	Validity Period O.K.	Enc/Dec Single File
Grant File Access	Public Read	X			Flag if Expired	
	Public Write		X	X		
	Scratch Pad Read			X	X	
	Scratch Pad Write			X	X	
	Emergency Scratch Pad Read			X	Flag if Expired	
	Emergency Scratch Pad Write			X	Flag if Expired	
	Private Read		X	X	X	
	Private Write		X	X	X	
	Shared Private Read		X	X	X	
	Shared Private Write		X	X	X	
Hash	Hash					
Digital Signature	Sign					
	Verify					

7.3.3.2 Digital signature PIC. The use of digital signature on a PIC should be driven by the mission. The Digital Signature PIC is defined as essentially a Basic PIC with the additional capabilities to perform hashing of data to be signed or verified, digital signature generation, and digital signature verification. It provides a minimal level of protection for the data it carries. Its security is based almost entirely upon protection of the PI^2 software, the user's PIN, and the application passwords used. Digital signature schemes introduce complex infrastructure requirements, such as signature hierarchies and systems to alert PIC holders of lost or compromised cards in a timely manner. Algorithms to be used for such purposes should be specified at the time the program is established.

7.3.3.2.1 Digital signature PIC applications. A Digital Signature PIC is intended to be backward compatible with the Basic PIC, and to operate correctly in all of its applications. It would not necessarily provide any greater level of protection for the data carried.

7.3.3.2.2 Digital signature PIC functions. A Digital Signature PIC performs the Basic PIC functions plus hashing, digital signature generation, and digital signature verification. It should support protected caching of at least the private signature material of the cardholder. It may hold the cardholder's public digital signature keying material. If used to verify the signatures of others, it will be provided with a trusted way to obtain their public digital signature keys.

7.3.3.2.3 Digital signature PIC access controls. Access to the hashing and the digital signature algorithms and the public and private digital signature keying material would require:

a. Verification of the cardholder's PIN.
b. Verification of the application password.
c. Verification that the PIC has not exceeded its validity period.
d. Verification that the digital signature keying material contained within the PIC has not expired.
e. Satisfaction of possible additional digital signature-based access controls.
f. Satisfaction of possible additional biometric-based access controls.

TABLE III. Digital signature PIC profile

PIC Functions		PIC Access Controls				
		Public Request	PIN	Application Password	Validity Period O.K.	Enc/Dec Single File
Grant File Access	Public Read	X			Flag if Expired	
	Public Write		X	X		
	Scratch Pad Read			X	X	
	Scratch Pad Write			X	X	
	Emergency Scratch Pad Read			X	Flag if Expired	
	Emergency Scratch Pad Write			X	Flag if Expired	
	Private Read		X	X	X	
	Private Write		X	X	X	
	Shared Private Read		X	X	X	
	Shared Private Write		X	X	X	
Hash	Hash		X	X	X	
Digital Signature	Sign		X	X	X	
	Verify		X	X	X	

Access to the Digital Signature PIC functions is as for the Basic PIC, with the possible addition of some digital signature-based controls.

The access controls for the Digital Signature PIC are shown in table III. These access controls establish its minimum protection profile.

7.3.3.3 Cryptographically protected PIC. The use of cryptographic protection on a PIC should be driven by the mission. The Cryptographically Protected PIC is defined as a Basic PIC with the additional on-board capabilities to perform encryption and decryption of its most sensitive files to better protect them from compromise or unauthorized modification. It provides an increased level of protection for some of the data it carries. Its security depends upon protection of the cardholder's PIN. Keying and key management become major issues.

7.3.3.3.1 Cryptographically protected PIC applications. The Cryptographically Protected PIC is intended to be backward compatible with the Basic PIC for non-critical applications. Representative applications would include performing those enumerated for the Basic PIC with more data integrity and confidentiality and possibly carrying more sensitive data.

7.3.3.3.2 Cryptographically protected PIC functions. In addition to the Basic PIC functions, the Cryptographically Protected PIC would also encrypt its more sensitive data files for storage, and decrypt them for use. It would need to incorporate key management functions and key exchange functions if it incorporated public key cryptography. It may encrypt/decrypt data being exchanged with an application program to protect it while in transit between the PIC and some trusted workstation. If this is done, it would be preferable for a hardware-based security module to be used with the host system to encapsulate its algorithms and keying material. It may dispense with application passwords for data files which are cryptographically protected.

7.3.3.3.3 Cryptographically protected PIC access controls. Access to the Cryptographically Protected PIC functions is as for the Basic PIC, with the addition of encryption protection for the more sensitive files. Biometric based access requirements could also be imposed and implemented by an application, using the PIC to provide a cardholder's biometric data to the PI^2.

The minimum access controls for the Cryptographically Protected PIC are shown in table IV. These access controls establish its minimum protection profile.

Additional access controls would be desirable at this level of PIC protection. They could be based upon challenge and response mechanisms to:

a. Validate the cardholder to the PIC.
b. Validate the PIC to the reader.
c. Validate the reader to the PIC.
d. Validate the reader to the application.
e. Validate the application to the reader.
f. Validate the PIC to the application.
g. Validate the applications to the PIC.

TABLE IV. Cryptographically protected PIC profile

PIC Functions		PIC Access Controls				
		Public Request	PIN	Application Password	Validity Period O.K.	Enc/Dec Single File
Grant File Access	Public Read	X			Flag if Expired	
	Public Write		X	X		
	Scratch Pad Read			X	X	
	Scratch Pad Write			X	X	
	Emergency Scratch Pad Read			X	Flag if Expired	
	Emergency Scratch Pad Write			X	Flag if Expired	
	Private Read		X	TBD	X	X
	Private Write		X	TBD	X	X
	Shared Private Read		X	TBD	X	X
	Shared Private Write		X	TBD	X	X
Hash	Hash					
Digital Signature	Sign					
	Verify					

7.3.3.4 Cryptographically protected digital signature PIC. The use of both cryptographic protection and digital signature on a PIC should be driven by the mission. A Cryptographically Protected Digital Signature PIC is essentially the combination of all three previous PIC types. At this level of integration and sophistication, it would be desirable to increase the security capability of the PIC by adding some or all of the following additional requirements that:

a. ICC and its components be designed in the U.S. to provide enhanced security.

- The developer fully analyze and document its security features.
- Its full details be divulged to the Government for confirmation of the analysis.
- The resulting design be placed under configuration control, with the Government in the approval cycle for any changes.

b. A PIC trusted operating system be developed in the U.S. to provide enhanced security.

- The developer fully analyze and document its security features.
- Its full details be divulged to the Government for confirmation of the analysis.
- The resulting design be placed under configuration control, with the Government in the approval cycle for any changes.

c. The PIC trusted operating system be installed on the PIC IC via mask programmable ROM.

d. A conformance test suite be developed and provided to the Government to fully test the PIC IC and its trusted operating system for all required functionality, and to verify that no "undocumented features" exist which could compromise security.

e. The IC die be manufactured and packaged in the U.S.

f. The full conformance test suite be run on periodic and randomly chosen samples of the IC die, if not on 100 percent of the die, and on randomly selected new cards, to detect any non-standard IC which may have been introduced.

g. Biometric comparison capability be added to the PIC.

h. Enhanced audit trail capabilities be added to the PIC.

7.3.3.4.1 Cryptographically protected digital signature PIC applications. This PIC profile would be capable of performing all of the functions in the three previously defined PIC profiles, but it may sacrifice backward compatibility for all but the "public read" type of "file access."

7.3.3.4.2 Cryptographically protected digital signature PIC functions. The functions of this PIC profile would be a composite of all the functions of the three previously defined PIC profiles, with probable security enhancements such as biometric data comparison and verification on the PIC IC.

7.3.3.4.3 Cryptographically protected digital signature PIC access controls. Access to the Cryptographically Protected Digital Signature PIC functions would be similar to the Basic PIC, with the addition of encryption protection for at least the more sensitive files and the possible addition of some digital signature based controls. Biometric based access requirements could also be imposed. The role of the PI^2 would be greatly reduced at this point due to much greater PIC standardization and on-chip access control decision capability.

The minimum access controls for the Cryptographically Protected Digital Signature PIC are shown in table V. These access controls establish its minimum protection profile.

The additional access controls introduced as desirable at the Cryptographically Protected PIC level should be almost mandatory at this level. They could be based upon challenge and response mechanisms to:

a. Validate the cardholder to the PIC.
b. Validate the PIC to the reader.
c. Validate the reader to the PIC.
d. Validate the reader to the application.
e. Validate the application to the reader.

f. Validate the PIC to the application.
g. Validate the applications to the PIC.

TABLE V. Cryptographically protected digital signature PIC profile

PIC Functions		PIC Access Controls				
		Public Request	PIN	Application Password	Validity Period O.K.	Enc/Dec Single File
Grant File Access	Public Read	X			Flag if Expired	
	Public Write		X	X		
	Scratch Pad Read			X	X	
	Scratch Pad Write			X	X	
	Emergency Scratch Pad Read			X	Flag if Expired	
	Emergency Scratch Pad Write			X	Flag if Expired	
	Private Read		X	TBD	X	X
	Private Write		X	TBD	X	X
	Shared Private Read		X	TBD	X	X
	Shared Private Write		X	TBD	X	X
Hash	Hash		X	TBD	X	
Digital Signature	Sign		X	TBD	X	Opt ?
	Verify		X	TBD	X	Opt ?

7.4 PIC data security. The security services necessary to be provided to PIC data fall into at least three categories: confidentiality, integrity, and availability.

7.4.1 Confidentiality. The confidentiality requirements on an individual's Basic PIC are generally considered to be low, and primarily required to protect "privacy" type information.

As the need to store more sensitive information on a PIC arises, a more advanced and sophisticated type of PIC than profiled here may be needed.

For an application security module (if implemented as a PIC), the confidentiality requirements are significantly higher, and should be established based on the need to protect the application passwords and possibly the keying material contained, since it can give access to many PIC applications.

7.4.2 Integrity. The integrity of the data on a PIC is quite important since real time decisions will be based upon it, potentially in crisis situations. The data will be protected from unauthorized erasure, tampering, and manipulation.

7.4.3 Availability (protection from denial of service). Availability of PIC data is supported primarily through the integrity protection mechanisms. Present technology cannot prevent loss of a PIC, but it can and will protect PIC data from corruption by hackers and potential Trojan horse readers, particularly those which may reside in the commercial sector, if a PIC is provided with commercial financial applications.

7.5 PIC physical security.

7.5.1 Overview. Information may be stored on a PIC in various ways. For example, photographic images, printed alphanumeric characters, and bar codes are just some of the ways information may be stored on the front and back surfaces of a PIC. Information may also be stored digitally in the integrated circuit chip(s). To protect this information from inadvertent or adversarial modification and to verify the authenticity of the information, designers of PIC technologies should design physical security protection features into a PIC, based on the security requirement(s) of the PIC application.

Physical security protection refers to those features, mechanisms, and technologies that can be physically applied during or after production. These features may be apparent or hidden and may be interrogated at a later time to check the authenticity and integrity of the information in question.

7.5.2 IC and card level. A PIC will provide the following IC and physical card level security protection:

a. Tamper deterrent: technologies that may prevent tampering with the integrated circuit(s) and information stored on the surface of the card.

b. Tamper resistant: technologies that resist tampering with the integrated circuit(s) and information stored on the surface of the card.

c. Tamper indicator(s): technologies that indicate tampering with the integrated circuit(s) and information stored on the surface of the card.

d. Authenticator(s): technologies that authenticate the integrated circuit(s) and information stored on the surface of the card.

7.6 Application security.

7.6.1 Overview. An application requests to retrieve or to deposit specific data from or to a PIC after authentication of the application, reader/writer, and PIC. The application may use an application security module (ASM) to contain and protect its application passwords and possibly algorithms and keys. If an ASM is used, it may be in the form of a PIC.

7.6.2 Security. In addition to the security requirements for the PIC, the following requirements may apply to the application:

a. Digital signature either for validating data on the application or the PIC.
b. Capable of cryptographic processing.
c. Accessed at least by a PIN or other authentication process.
d. Maintaining strict controls over distribution and the use of application.

e. An audit trail of all uses.
f. Periodic validation of all data on application and usage.

8. PHYSICAL

8.1 Overview. This section addresses the physical characteristics of the carrier and the specific technologies optionally included on a PIC such as magnetic stripes, bar codes, and integrated circuit chips.

8.2 Physical characteristics. This section specifies physical characteristics for a PIC including card dimensions, construction, materials, and characteristics. It considers both human and machine aspects and states minimum requirements.

8.2.1 Dimensions. The PIC will comply with the dimensions for unembossed ID-1 cards (credit card sized cards) given in ISO/IEC 7810 for card width and height, thickness, corners, and edges. As stated in ISO/IEC 7816-1, the ISO/IEC 7810 specification for card thickness will apply to a non-embossed card including contacts and integrated circuits.

8.2.2 Construction. Construction of the PIC will be in accordance with ISO/IEC 7810.

8.2.3 Card materials. The PIC will be made of abrasion resistant materials such as polyvinyl chloride (PVC), polyvinyl chloride acetate (PVCA), or other materials having equal or better performance. Card insert material may be used. Any material used in the PIC, including insert material, will conform to and not interfere with other requirements specified in this handbook. This material will support the printing/graphics of specific DoD mission requirements and will remain intact and readable for the life of the card. Also, the material will not soften, harden, or deform if kept in contact with flexible plastics. The use of environmentally friendly material is encouraged if the material meets the above requirements.

8.2.4 Card characteristics. The requirements for bending stiffness, toxicity, delamination, adhesion or blocking, light transmittance, and overall card warpage for unembossed cards specified in ISO/IEC 7810 will apply to the PIC. The additional characteristics in ISO/IEC 7816-1 for ultraviolet light, X-rays, surface profile of contacts, mechanical strength (of cards and contacts), electrical resistance (of contacts), electromagnetic interference (between magnetic stripe and integrated circuit(s)), electromagnetic fields, static electricity, and heat dissipation also apply. In addition, the following characteristics will apply.

8.2.4.1 Flammability. The PIC will conform to the flammability requirements given in ISO/IEC 7813:1995, *Identification Cards - Financial Transaction Cards*.

8.2.4.2 Resistance to chemicals. In addition to the solutions specified in ISO/IEC 10373, the PIC will be resistant to chemical effects present in a DoD environment such as gasoline, oil, hydraulic fluid, or paint solvents. Card issuers should be aware that information held on a magnetic stripe or an integrated circuit may be rendered ineffective as a result of contamination (see ISO/IEC 7816-1).

8.2.4.3 Reliability/durability. The PIC will have a minimum usable life of 5 years. The magnetic stripe will last for a minimum of 25,000 reads. The integrated circuit chip will last for a minimum of 75,000 card insertions and will be capable of retaining data for the life of the card. These requirements will be met under the full range of environmental conditions described below.

8.2.4.4 Environmental conditions. In addition to meeting or exceeding the environmental requirements specified in ISO/IEC 7810, the PIC will not crack, peel, delaminate, warp, permanently deform, or become

unreadable either visually (printed text and digitized photograph) or by a card reader (magnetic stripe, bar code, and integrated circuit chip) when subjected to the conditions below.

8.2.4.4.1 Temperature/humidity. The PIC will operate in environments ranging from -35°C to +50°C (-31°F to +122°F) with a relative humidity of 30 to 80 percent noncondensing. In addition, the PIC will allow for storage in environments ranging from -62°C to +65°C (-80°F to 149°F) with a relative humidity of 5 to 95 percent noncondensing.

8.2.4.4.2 Light. The PIC and its printed text and digitized photograph will not deteriorate from exposure to light encountered in DoD environments.

8.2.5 Magnetic stripe. The special characteristics for cards with magnetic stripe, magnetic stripe area warpage, surface distortions, and contamination specified in ISO/IEC 7810 will apply to the PIC. The physical characteristics of the magnetic stripe specified in ISO/IEC 7811-2, including height and surface profiles, surface roughness, adhesion of the stripe to card, wear from read/write head, and resistance to chemicals, will apply to the PIC, unless a high coercivity magnetic stripe is used, in which case the characteristics in ISO/IEC 7811-6 will apply.

8.2.6 Special characteristics. The following special characteristics will also apply to the PIC.

8.2.6.1 Holes in PIC. Some readers/writers will perform a surface integrity check of the PIC. Unless mission considerations outweigh potential loss of functionality, holes should not be punched in a PIC.

8.2.6.2 Decorations. Any printing or screening placed on the PIC will not impair the function of the magnetic stripe, bar code, or integrated circuit chip. Decals or logos placed on the PIC will not interfere with the readability of the PIC either visually (printed text and digitized photograph) or with a card reader (magnetic stripe, bar code, and integrated circuit chip).

8.2.6.3 Maintainability. Maintenance consideration will be limited to the cleansing of exterior dirt with a clean cloth, soap, and water. This cleansing will not cause the PIC to crack, peel, delaminate, warp, permanently deform, or become unreadable either visually or by a card reader.

8.3 Magnetic stripe. The requirements for magnetic stripes in ISO/IEC 7811-2, 7811-4, and 7811-5 will apply to the PIC. If a high coercivity magnetic stripe is used, the requirements in ISO/IEC 7811-6 will take precedence.

8.3.1 Location of magnetic stripe. The magnetic stripe will be located on the back of the card. The actual location of the magnetic stripe will be in accordance with ISO/IEC 7811-2 or 7811-6 for high coercivity magnetic stripes.

8.3.2 Track encoding. The encoding of each magnetic stripe track depends on the application. For example, track 2 is used by the financial community for financial transaction cards in accordance with ISO/IEC 7813 and by the security community to carry security credentials in accordance with SEIWG-02. The encoding used for these two applications is different and therefore will not interoperate.

8.4 Bar codes.

8.4.1 One-dimensional bar code. Any one-dimensional bar codes used on the PIC will comply with the requirements in ANSI/AIM BC-1-1995 Uniform Symbology Specification (USS) Code 39 (USS-39), and ANSI

X3.182-1990. These documents are listed in hierarchical order of precedence if any conflict between these documents exists.

8.4.1.1 Symbology. The one-dimensional bar code will conform to the 3-of-9 bar code specified in USS-39. A human readable interpretation (HRI) as defined in USS-39 will not be used on the PIC. The following application-specific optional code formats and special requirements will not apply to the PIC:

a. Optional code formats.
- Check characters.
- Broken messages.
- Full ASCII.

b. Special requirements.
- Code format and density.
- HRI location and size.

8.4.1.2 Code density and dimensions. The dimensions given in USS-39 for intercharacter gaps and quiet zones will apply to the PIC. The requirements for code density and other dimensions and tolerances are given below.

8.4.1.2.1 Code density. Since the space on a PIC is at a premium, a code density of 3.7 characters per centimeter (9.4 characters per inch) will be used. No ultra-high densities are allowed.

8.4.1.2.2 Heights. The bar code height may range from a minimum of 6.35 mm (0.25 in.) to a maximum of 12.7 mm (0.5 in.).

8.4.1.2.3 Nominal width. The nominal width of the narrow element of the bar code will range from a minimum of 0.19 mm (0.0075 in.) to a maximum of 0.508 mm (0.02 in.).

8.4.1.2.4 Nominal wide-to-narrow ratio. The nominal ratio of wide-to-narrow elements varies according to the size of the narrow element. These values are given in table VI.

In all cases, the preferred nominal wide-to-narrow ratio is 3.0:1 and will remain constant throughout the symbol. The actual wide-to-narrow ratio will not exceed 3.3:1.

TABLE VI. Nominal wide-to-narrow ratio

UNIT SIZE (X)		RATIO
(in millimeters)	(in inches)	
0.381>X≥0.1905	0.015>X≥0.0075	2.2:1 to 3.0:1
0.598≥X≥0.381	0.02≥X≥0.015	2.0:1 to 3.0:1

8.4.1.3 Readability. The bar code will be readable over the lifetime of the PIC.

8.4.1.4 Location. The bar code may be located on the front or the back of the card and will not interfere with the readability of the PIC either visually (printed text and digitized photograph) or with a card reader

(magnetic stripe, bar code, and integrated circuit chip). The center line of the 3-of-9 bar code will be located 12.7 mm (0.5 in) from the edge of the PIC.

8.4.2 Two-dimensional bar code. Any two-dimensional bar codes used on a PIC will comply with the requirements in Uniform Symbology Specification (USS) Portable Data File (PDF) 417. Neither truncated USS PDF-417 nor Macro PDF-417 will be used on the PIC.

8.4.2.1 Compaction modes. The PIC will support text, byte, and numeric data compaction modes and the associated mode shifts and latches. It is recommended that the numeric compaction mode be used for more than 13 consecutive digits.

8.4.2.2 Symbol dimensions. The largest nominal width of each narrow element (X) practical should be used. If the minimum error correction levels shown in table VII are used, the minimum row height will be 3X; otherwise, the minimum row height will be 4X. Greater levels of error correction may also be used; these higher levels of error correction are given in table VIII.

TABLE VII. Symbol dimensions

Number of Data Codewords	Minimum Error Correction Level	Number of Error Correction Codewords (for this Error Correction Level)
1-40	2	8
41-160	3	16
161-320	4	32
321-863	5	64

TABLE VIII. Higher levels of error correction

Error Correction Level	Number of Error Correction Codewords (for this Error Correction Level)
6	128
7	256
8	512

8.4.2.3 Readability. The bar code will be readable over the lifetime of the PIC. It is recommended a matte (non-glossy) finish be used to minimize the interference of shiny surfaces with PDF-417 readers. Overlays or irregularities such as curvatures in the surface will not interfere with the readability of the USS PDF-417.

8.4.2.4 Location. The USS PDF-417 may be located on the front or the back of the card and will not interfere with the readability of the PIC either visually (printed text and digitized photograph) or with a card reader (magnetic stripe, bar code, and integrated circuit chip).

8.5 Integrated circuit chip.

8.5.1 Location and dimensions of contacts. The location and dimensions of each of the contacts will comply with ISO/IEC 7816-2, with the contacts on the front of the card.

8.5.2 Contact assignment. The assignment of the ICC contacts will be as defined in ISO/IEC 7816-2. Unused contact areas do not need to be physically present. If unused contacts are present, they will be either nonconductive or electrically isolated from the ICC and the other contacts.

8.5.3 Card session. The PIC will comply with ISO/IEC 7816-3 with respect to the dialogue between the interface device and the card for all card stages ranging from insertion of the PIC into the interface device through the execution of the transaction to the removal of the PIC from the interface device. The PIC will answer to reset (ATR) asynchronously using active low reset. Although the PIC may use either the asynchronous half duplex character transmission protocol (T=0) or asynchronous half duplex block transmission protocol (T=1), T=0 is preferred and will be the default protocol. An external clock will be used. The default clock rate conversion factor will be F=372 and the bit rate adjustment factor will be D=1. The preferred mode of operations will be the negotiable mode, although the PIC will be able to handle the specific mode of operations. If the ICC is prematurely removed from the interface device during the execution, no electrical or mechanical damage will be caused to the ICC.

8.5.4 Chip operating system. At least two approaches to the chip operating system (COS) may be used. The first is to develop in the PI^2 a driver or equivalent that is able to recognize and utilize any COS provided by the card manufacturer. Another is that the infrastructure organizations for the PIC will specify a COS the manufacturers will have to implement on the card. The approach taken should be specified prior to acquisition of the system.

9. READER/WRITER

9.1 Overview. This section addresses PIC readers/writers, including the card types and the reliability, environmental, and power requirements.

9.2 Card types/technologies. PIC readers/writers will read and write non-embossed ID-1 cards (credit card sized cards) in accordance with ISO/IEC 7810 and ISO/IEC 7816-1 for non-embossed cards including contacts and integrated circuits, ISO/IEC 7811 for magnetic stripes, USS-39 for one-dimensional bar codes, and PDF-417 for two-dimensional bar codes. It is not expected to have one reader to read all possible technologies which can be on a PIC. Section 8, Physical, provides additional information on the PIC types and the potential technologies which can be included on a PIC, including the applicable standards references. In no case will a PIC reader/writer interfere with the readability either visually (printed text and digitized photograph) or with a card reader (magnetic stripe, bar code, and integrated circuit chip). This requirement applies to combined technology readers/writers such as a combined magnetic stripe/integrated circuit chip reader.

9.2.1 Magnetic stripe. A reader/writer for magnetic stripe will conform to the requirements of SEIWG-02, ISO/IEC 7811-2, 7811-4, and 7811-5. If a high coercivity magnetic stripe is used, the requirements in ISO/IEC 7811-6 will take precedence.

9.2.2 Bar codes. For one-dimensional bar codes, the reader will comply with the requirements in USS-39 (ANSI/AIM BC-1-1995) and ANSI X3.182-1990. For two-dimensional bar codes, the reader will comply with the requirements for USS PDF-417.

9.2.3 Integrated circuit chip. The ICC contacts and interconnect on a reader/writer will be in accordance with ISO/IEC 7816-1, 7816-2, and 7816-3.

9.2.3.1 Card feed speed. The minimum card feed speed for motorized PIC readers/writers will be 10 cm/sec. Non-motorized readers/writers are preferred due to reliability and cost considerations.

9.2.3.2 Transmission protocols. The PIC readers/writers will support both T=1 and T=0 transmission protocols.

9.3 Reliability/durability. Readers/writers will have a minimum usable life of 5 years. Magnetic stripe readers/writers will allow a minimum of 1,000,000 reads/writes. ICC readers/writers will allow a minimum of 1,000,000 card insertions. These requirements will be met under the full range of environmental conditions specified in 8.4.

9.4 Environmental conditions. PIC readers/writers will be capable of meeting the operating and storage environment conditions for temperature and humidity specified for a PIC in section 8.

9.5 Power. The power requirements for a PIC reader/writer will depend upon the specific application based on worldwide DoD requirements. The operating voltage applied to a PIC will be 5V ± 5 percent. Future consideration of alternative voltage such as 3.5V will depend upon changes in commercial devices.

9.6 Electronic design. A PIC reader/writer will comply with Underwriters Laboratories (UL) requirements.

9.7 External interface. A PIC reader/writer will provide a serial bus or PC Card Type interface.

9.8 Financial application capability. If a PIC is used in commercial stored value, credit card, or debit card applications, the reader/writer will comply with the EMV terminal specification.

Warning: Functions such as financial, banking, or purse/cache will require careful review before implementation on the PIC. Safeguarding data stored in the card may become more difficult due to the nature of these functions; however, defining the potential for these problems lies beyond the scope of this document. Additionally, the value of the money that may be accessed with the card may make it a target for fraud, theft, or hacking.

10. NOTES

10.1 Intended Use. This handbook is for guidance only. The intended use of the handbook is to assist in the planning and initiation of a single standard for smart card usage across DoD to prevent separate and incompatible implementation of smart card technologies.

10.2 Subject Word Listing.

Portable Information Carrier (PIC)
smart card
Integrated Circuit Chip (ICC)
PIC Integration Interface (PI^2)
Multi-Technology Automated Reader Card (MARC)
bar coding
magnetic stripe

APPENDIX A

REFERENCES

A.1. SCOPE

A.1.1 Scope. This appendix lists all documents referenced in this handbook. Section 2 lists the documents needed in order to fully understand the information provided by this handbook.

A.2. APPLICABLE DOCUMENTS

American National Standards Institute (ANSI), ANSI X3.182-1990, *Bar Code Print Quality - Guideline*, 1990.

Automatic Identification Manufacturers (AIM) USA, ANSI/AIM BC-1-1995, *Uniform Symbology Specification Code 39*, June 1993.

Automatic Identification Manufacturers (AIM) USA, *PDF-417*, July 1994.

Electronic Industries Association (EIA) - 232-D, *Interface Between Data Terminal Equipment and Data Circuit-Termination Equipment Employing Serial Binary Data Interchange*.

Europay, MasterCard, and VISA (EMV), *Integrated Circuit Card Application Specification for Payment Systems*, Version 3.0, June 1996.

Europay, MasterCard, and VISA (EMV), *Integrated Circuit Card Specification for Payment Systems*, Version 3.0, June 1996.

Europay, MasterCard, and VISA (EMV), *Integrated Circuit Card Terminal Specification for Payment Systems*, Version 3.0, June 1996.

Executive Order 12958, "Classified National Security Information," April 17, 1995.

ISO/IEC 4287: 1984, *Surface Roughness Terminology - Part 1: Surface and Its Parameters.*

ISO/IEC 7810: 1995, *Identification Cards - Physical Characteristics*, August 15, 1995.

ISO/IEC 7811-1: 1995, *Identification Cards - Recording Techniques - Part 1: Embossing*, August 15, 1995.

ISO/IEC 7811-2: 1994, *Identification Cards - Recording Techniques - Part 2: Magnetic Stripe*, August 15, 1995.

ISO/IEC 7811-3: 1995, *Identification Cards - Recording Techniques - Part 3: Location of Embossed Characters on ID-1 Cards*, August 15, 1995.

ISO/IEC 7811-4: 1994, *Identification Cards - Recording Techniques - Part 4: Location of Read-only Magnetic Tracks - Tracks 1 and 2*, August 15, 1995.

ISO/IEC 7811-5: 1994, *Identification Cards - Recording Techniques - Part 5: Location of Read-only Magnetic Track - Track 3*, August 15, 1995.

APPENDIX A

ISO/IEC 7811-6: 1995, *Identification Cards - Recording Technique - Part 6: Magnetic Stripe - High Coercivity*, August 15, 1995.

ISO/IEC 7812-1: 1993, *Identification Cards - Identification of Issuers - Part 1: Numbering System*, December 1, 1993.

ISO/IEC 7812-2: 1993, *Identification Cards - Identification of Issuers - Part 2: Allocation and Registration Procedures*, December 1, 1993.

ISO/IEC 7813: 1995, *Identification Cards - Financial Transaction Cards*, August 15, 1995.

ISO/IEC 7816-1: 1987, *Identification Cards - Integrated Circuits(s) with Contacts - Part 1: Physical Characteristics*, July 1, 1987.

ISO/IEC 7816-2: 1988, *Identification Cards - Integrated Circuits(s) with Contacts - Part 2: Dimensions and Location of the Contacts*, May 15, 1988.

ISO/IEC 7816-3: 1989/Amd. 2: 1994, *Identification Cards - Integrated Circuits(s) with Contacts - Part 3: Electronic Signals and Transmission Protocols, Amendment 2: Revision of Protocol Type Selection*, December 1, 1994.

ISO/IEC 7816-4: 1995, *Identification Cards - Integrated Circuits(s) with Contacts - Part 4: Interindustry Commands for Interchange*, September 1, 1995.

ISO/IEC 7816-5: 1994, *Identification Cards - Integrated Circuits(s) with Contacts - Part 5: Numbering System and Registration Procedure for Application Identifiers*, June 15, 1994.

ISO/IEC 7816-6: 1995, *Identification Cards - Integrated Circuits(s) with Contacts - Part 6: Inter-industry Data Elements*, 1995.

ISO/IEC 7816-7: when it becomes available, *Identification Cards - Integrated Circuits(s) with Contacts - Part 7: Interindustry Commands for Structured Card Query Language (SCQL).*

ISO/IEC 7618-8 and 7618-9 when they become available.

ISO/IEC 8824-1: 1996/Amd. 1: 1996, *Information Technology - Open Systems Interconnection - Abstract Syntax Notation One (ASN.1) - Part 1: Specification of Basic Notation First Edition, Amendment 1*, 1996.

ISO/IEC 9075: 1992, *Information Technology - Database Languages - SQL2.*

ISO/IEC 10373: 1993, *Identification Cards - Test Methods.*

Personal Computer Memory Card International Association (PCMCIA), *PCMCIA Standard Release 2.1/Japanese Electronic Industry Development Association (JEIDA) 4.2*, July 1993.

Security Enterprise Integration Working Group (SEIWG), SEIWG-012, *Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC)*, February 28, 1994.

APPENDIX A

U.S. Department of Defense, Defense Information Systems Agency, *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)*, Preliminary Version 2.0, October 23, 1995.

U.S. Department of Defense, DoD 8320.1-M-1, "DoD Data Element Standardization Procedures," January 1993.

U.S. Department of Defense, DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

U.S. Department of Defense, National Computer Security Center (NCSC), I-942-TR-003, *Information Systems Security Policy Guidelines*, July 1994.

APPENDIX B

ASSUMPTIONS

B.1. SCOPE

B.1.1 Scope. In developing this DoD PIC standard guidance, the PICSWG formed several working groups, each of which focused on a major area of the document. The PICSWG heard from a variety of sources familiar with actual (or potential) applications and programs where a PIC might be used. These included industry experts, DoD programs (including the MARC proof-of-principle test), Federal programs outside DoD, and others. After gathering this information, each working group proceeded to develop its findings.

This appendix presents a summary of the key assumptions used by four of the working groups: Data Management, PI^2, Security, and Physical. As the working groups made decisions about elements to include in the document, they kept track of their assumptions. Readers of this document will find the assumptions presented in this appendix helpful in understanding the perspectives from which each of the sections was written.

B.2. GENERAL

B.2.1 General.

- Error recovery for problems caused by a card being prematurely removed from the reader/writer or other interruption of the data transfer process should be addressed by techniques such as "anti-tearing" or an equivalent.

B.3. DATA MANAGEMENT

B.3.1 Data management.

- A DoD PIC management infrastructure and a configuration control process will be in place to standardize the process of managing PIC technology.

- A separate DoD policy group will be formed with each DoD component and functional owner represented to support the PIC infrastructure and the configuration control process.

- A data element will be stored only once on the chip. To be added to a PIC, a data element will be requested by at least one proponent.

- Data will be unclassified but can be Sensitive But Unclassified (SBU), requiring access control; encryption would not normally be used but could be used if the application manager determines it is necessary.

- Data stored on the PIC will be DoD standard elements and codes in accordance with the Defense Data Dictionary System (DDDS) and DoD 8320.1-M-1; exceptions may be authorized by the PIC infrastructure.

- Data stored on the PIC will be a copy of data maintained elsewhere (with the exception of scratchpad or emergency scratchpad data).

- Application operators may make modifications only to data in their functional areas.

- The data management process is expected to ensure the PIC data can be locked when/if:
  - A card is shown to be no longer valid.
  - Non-approved applications attempt to modify data.

- Any data element on the bar code or print media should also be on the chip.

- Data on the bar code(s) and print media will be static (change very infrequently), such as name and SSN.

- Data will be capable of being erased, not merely by changing a directory reference. This function should be controlled.

- Commercial stored value chip functions, if used, will be compliant with existing standards such as Europay, MasterCard, and Visa (EMV).

B.4. PIC INTEGRATION INTERFACE (PI^2)

B.4.1 PIC integration interface (PI^2).

- The API will address any POSIX-compliant, commercially available, host operating system.

- When a new device is added to the configuration, the vendor will provide 100 percent of the details about the operating system. The vendor will provide the required driver(s).

- Where ISO/IEC standards are not applicable or are incomplete, the PIC PI^2 will conform as much as possible to the IEEE, ANSI, and FIPS standards concerning smart card technology. All system applications and technology associated with the PIC will conform to the guidelines set forth in the DoD TAFIM as it applies to the PIC technology.

B.5. SECURITY

B.5.1 Security.

- Applications have specific read/write permissions.

- A unique identifier is required for each card.

- The DoD PIC management infrastructure will control which applications are to be implemented.

- A DoD PIC management infrastructure and a configuration control process will be in place to manage the process of standardizing security requirements.

- Application sensitivity drives card security requirements.

- Only unclassified and SBU data will be stored on the PIC.

- The PIC and its supporting infrastructure will provide the following security services: confidentiality, availability, and integrity of data stored on the chip.

APPENDIX B

- Emergency destruction of the data in the PIC is achieved by physically destroying the IC(s).
- All applications will complete the appropriate certification and accreditation process.
- Readers/writers will provide the level of security consistent with the PIC security requirements indicated in this document.

B.6. PHYSICAL

B.6.1 Physical.

- The following application-specific optional code formats and special requirements will not apply to the PIC:
    - Optional code formats.
        - Check characters.
        - Broken messages.
        - Full ASCII.
    - Special requirements.
        - Code format and density.
        - HRI location and size.
- No ultra-high code densities are allowed, to ensure interoperability.
- The bar code will be readable over the lifetime of the PIC.
- Only one PDF-417 bar code may be used on a PIC. MACRO PDF-417 will not be used.
- Only one 3-of-9 bar code may be used on a PIC.

APPENDIX C

STRUCTURED CARD QUERY LANGUAGE (SCQL) CONSIDERATIONS

C.1. SCOPE

C.1.1 Scope. This appendix addresses considerations regarding the use of structured card query language.

C.2. SCQL TABLES

C.2.1 SCQL tables. An SCQL database contains objects called tables, views, and dictionaries. Each object can be referenced with a unique identifier. A table is a structured data object with a unique name within a database. It consists of named columns and a sequence of rows. The number of rows may be conceptually unlimited (limited only by the memory space available on the chip) or limited by the space allocation for that particular application.

After creation, the table structure is persistent. In other words, neither an existing column can be withdrawn nor a new column can be inserted. On a table the following actions can be performed:

a. Read (select).
b. Insert.
c. Update.
d. Delete.

C.3. SCQL VIEWS

C.3.1 SCQL views. A view is a logical subset of a table, which defines the part of the table accessible. Two types of views are to be distinguished:

a. A view which by definition fixes the accessible columns, called a static view.

b. A view which restricts the access to those rows whose contents match defined conditions, called a dynamic view.

A combination of static and dynamic views in the same definition is possible. A view and a table have a unique name in an SCQL database. Several views may be defined on the same table. On a view the following actions can be performed:

a. Read (select).
b. Update.

C.4. SCQL APPLICATION TABLES

C.4.1 SCQL application tables. A system table is maintained by the card and contains information necessary to manage the database structure and access. There are three basic system tables:

a. The object description table.
b. The user description table.
c. The privilege description table.

APPENDIX C

The object description table contains information about the tables and views stored in the database. The user description table contains basic information about the user(s) which have access to the database(s). The privilege description table contains information about the privileges to the database tables and views for each. Privileges describe which tables and views can be accessed by which users, and which actions can be performed by those users on the respective table, application, or view.

C.4.1.1 SCQL dictionaries. For access to the information contained in the system tables, views on these system tables can be created. A view on a system table is called an SCQL dictionary. The only action which a user can perform on a dictionary is reading.

C.5. USER APPLICATION RESTRICTIONS

C.5.1 User application restrictions. SCQL user profiles are characterized by special permissions. A user profile is attached to a user identifier stored in the user description table. Permissions may be attached to the database, the database object owner, the database basic user (which may be the application owner) with specific user identification, or the application owner. The types of user profiles and permissions include, but are not restricted to, the following:

a. Database owner - permissions:
- Adding/dropping of user with profile database object owner or database basic user.
- Creation/deletion of objects.
- Granting/revoking of privileges for objects owned.
- Creation/deletion of dictionaries with access to all rows in the system tables.
- Access to objects not owned according to the privileges granted.

b. Database object owner:
- Adding/dropping of users with profile database basic user.
- Creation/deletion of objects (tables/views).
- Granting/revoking of privileges for objects owned.
- Creation/deletion of dictionaries with access to rows where the database object owner is registered.
- Access to objects not owned according to the privileges granted.

c. Database basic user with specific user id or the general user id:
- Access to objects according to the privileges granted within the application.

d. Application database owner - permissions:
- Adding/dropping of user(s) with application profile database object owner or database.
- Creation/deletion of objects in the application.
- Granting/revoking of privileges for objects owned within a particular application.
- Creation/deletion of dictionaries with access to all rows in the system tables associated with that application.
- Access to objects not owned according to the privileges granted to the application.

C.6. SCQL COMMANDS

C.6.1 General concepts. The SCQL represents an ICC-related subset of the standard SQL. SQL statements are mapped onto SCQL operations within the PERFORM SCQL OPERATION command. See table IX.

APPENDIX C

The mandatory parameters of a command occur always in the sequence defined in the related command table; their tag is therefore not present. The optional parameters are presented in the tag, length, value (TLV) format if not indicated otherwise.

Two additional commands belong to the SCQL environment, but may also be used outside an SCQL environment:

a. The PERFORM TRANSACTION OPERATION command.
b. The PERFORM USER OPERATION command.

C.6.2 Grouping and encoding. The SCQL related commands can be grouped as shown in table IX.

TABLE IX. SCQL commands

SCQL Related Commands		
Perform SCQL Operation	**Perform Transaction Operation**	**Perform User Operation**
create table	begin	present user
create view	commit	create user
drop table	rollback	delete user
drop view		
create dictionary		
grant		
revoke		
declare cursor		
open		
next		
fetch		
fetch nest		
insert		
update		
delete		

C.6.3 Notation and special situations. The following notation is used for describing SCQL statements:

a. Words in capital letters are SQL words (fixed expressions of the SQL language).
b. {} means optional.
c. <...> means attribute string.
d. ::= means consists of.
e. | means or.
f. * means all.

APPENDIX C

For command description, the following notation is used:

a. Lp = Length (coded in one byte) of the subsequent parameter.
b. <...> = parameter string of bytes with the length LP and the meaning given in <...>.
c. Ln = "01" = Length of the subsequent number N.
d. <N> = Integer number codes in one byte.

Comparison operators which occur in search conditions follow the normal meanings.

C.6.4 Status bytes. The status bytes SW1-SW2 of a response denote the processing state in the card. Table X shows the general meaning of the values of SW1-SW2. For each command or performed operation, an appropriate clause provides more detailed meanings. The meaning of status bytes are defined in table X.

TABLE X. General meaning of SW1-SW2

SW1-SW2	Meaning
Normal processing	
9000	Command successful
61xx	Command successful, xx codes the number of data bytes to be fetched by GET RESPONSE
Warning processing	
6282	End of table reached
Execution errors	
6500	No information given
6581	Memory failure
Checking errors	
6700	Wrong length
Command not allowed	
6900	No information given
6982	Security status not satisfied
6985	Necessary commands or operations not performed before
Wrong parameters	
6A00	No information given
6A80	Incorrect parameter in data field
6A81	Operation not supported
6A84	Not enough memory space
6A88	Referenced object not found
6A89	Object exists already
6D00	Instruction code not supported

APPENDIX C

C.6.5 Identifiers. The following conventions for identifiers are defined:

a. <identifier> ::= <capital letter> [<capital letter> |<digit> |<_>...]

b. <capital letter> ::= A|B|C|...|Z

c. <digit> ::= 0|1|2|3|4|5|6|7|8|9|

d. <table name> ::= <identifier, maximum 8 bytes>

e. <view name> ::= <specifiable part of dictionary name><_><OIUIP>

f. <column name> ::= <identifier, maximum 8 bytes>

g. <specifiable part of dictionary name> ::= <identifier, maximum 6 bytes>

h. <user id> ::=
- <individual id>|
- <group id> <delimiter> <individual id>|
- <group id> <delimiter> <subgroup id> <delimiter> <individual id>|
- <group id> <delimiter> <asterisk>|
- <group id> <delimiter> <subgroup id> <delimiter> <asterisk>|
- <group id> <delimiter> <asterisk><delimiter> <asterisk>

i. <group id> ::= <identifier, maximum 8 bytes>

j. <subgroup id>::= <identifier, maximum 8 bytes>

k. <individual id>::= <identifier, maximum 8 bytes>

l. <delimiter> ::= .

m. <asterisk>::= *

The meaning of an asterisk is "don't care," therefore, the coding of this part is not compared.

For checking a user id, the following cases have to be distinguished:

a. If the user id is an individual, then the user id has to be identical with the registered user id.

b. If the user id consists of a group id in combination with an individual id, then the following steps have to be performed:
- Check whether the full user id is registered.
- If not, check whether <group id>.* is registered.

c. If the use id consists of a group id in combination with subgroup id and individual id, then the following steps have to be performed:

- Check whether the full user id is registered.
- If not, check whether <group id>.<subgroup id>.* is registered.
- If not, check whether <group id>.*.* is registered.

The user id verification is performed if a PRESENT USER operation is performed, but also in situations where access control to applications, tables, views and dictionaries is required.

C.6.6 Security attributes of tables. The following convention for security attributes is defined:

<security attribute>::= <security related data object as defined in other parts of this standard guidance, e.g., for authentication or access control>

Security attributes associated to tables and views may be related to authentication procedures to be performed before access or may describe secure messaging mechanisms to be applied, if data manipulation operations such as reading and writing in confidential mode are performed.

A security attribute attached to a user is related to user authentication.

APPENDIX D

CHIP UTILIZATION BLUEPRINT

D.1. SCOPE

D.1.1 Scope. This appendix provides guidance for utilizing the storage capacity of the IC.

D.2. CHIP DATA LAYOUT BLUEPRINT OVERVIEW

D.2.1 Chip data layout blueprint overview. To maximize the space on the PIC, data on the IC has to be carefully laid out. Sharing of data elements and elimination of duplicate data elements is critical. There will be basically two types of data: (1) data used by more than one application/mission which needs to be shared, and (2) data unique to any particular mission which is not to be shared. The non-shared data may also be isolated and not accessed by other missions and applications. This appendix describes a possible blueprint to assist in data element layout on the IC.

At least four layers will be considered. The basic four layers can be described as follows:

a. PI5 layer.
b. Demographics layer.
c. Agency/component general application layer.
d. Mission specific application layer.

The need for additional layers will depend upon the nature and objectives of the mission and the applications being developed. Additional layers may include a scratch pad area for temporary information storage and other information critical to the mission using the PIC.

D.3. PI5 LAYER

D.3.1 PI5 layer. If the PI5 concept guidance is utilized, the first layer will be devoted to the storage of the PI5 software necessary for basic operation. See figure D-1.

The use of embedded indices in the application(s) enabled by the IC will allow minimum amounts of coding and conserve IC space. As IC sizes increase, this may become less important. Until IC sizes increase, it is strongly urged the PI5 continue to embed the index in the applications. The PIC should only enable the application when inserted into the reader/writer device being used by the mission managing that application.

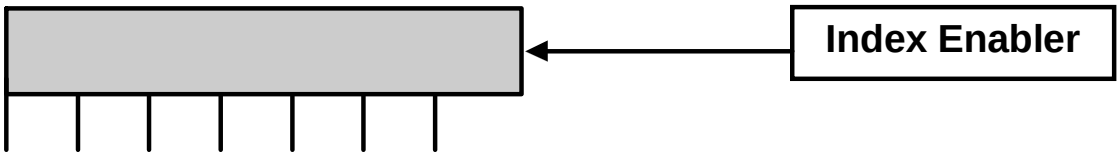


FIGURE D-1. PI^2 layer

APPENDIX D

D.4. DEMOGRAPHICS LAYER

D.4.1 Demographics layer. The demographics layer should contain basic information to identify the PIC user. This would include the user's name, identification number, and additional information determined necessary by the DoD PIC management infrastructure. Only information agreed to by the PIC management infrastructure should be loaded in this layer. See figure D-2.

If biometrics identification is loaded on the PIC, the demographics layer would be the most likely place for this information to be stored. This is because several mission applications may need to use the data to provide additional security to the PIC and to the particular mission of the mission application.

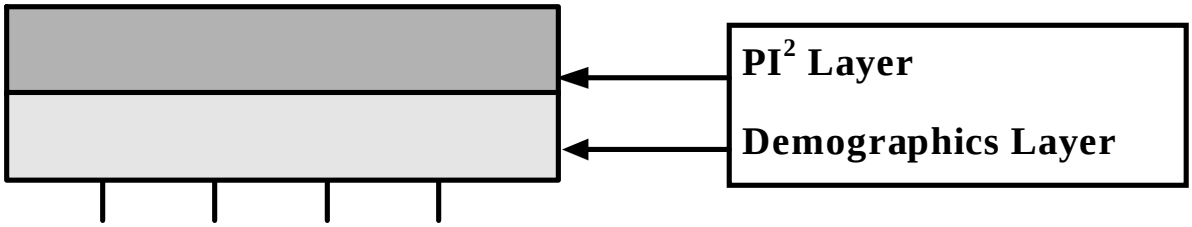


FIGURE D-2. Demographics layer

D.5. AGENCY/COMPONENT GENERAL APPLICATION LAYER

D.5.1 Agency/component general application layer. This layer holds the information related to the general functions common to all components. The layer would be able to use the data contained in the demographic layer and share data elements among the various applications within the agency/component general application layer.

DoD information that is identical for the various services, but has its own unique identifying convention, would be contained in this layer. The data would be stored following the data standardization requirements in the DoD data standardization dictionary. The specific application should translate the data to the format of that particular mission or component.

Examples of the types of information which could be placed in this layer include, but are not limited to, the following:

a. Financial.
b. Medical.
c. Medical allergy.
d. Personnel.
e. Readiness.
f. Personal qualifications.

Other agencies in contact with the user, such as the State Department, Veterans Administration, Department of Health and Human Services, and other Federal Agencies, may want to use data contained in this layer for their

applications if and when they implement the use of a PIC style card for their programs. When this occurs, the PIC should not have to be replaced or supplemented by an additional card, but should be able to accommodate the additional requirements in this layer by utilizing shared data elements. The goal of "enter once, retrieve many" should be realized in this layer by all the applications which can share information. See figure D-3.

As the various missions identify universal data elements, consideration should be given to moving those particular elements to the demographics section. This will minimize the number of unique data elements.

For purposes of the PIC, these application(s) would be the service-, or component-unique mission applications with unique data elements. The applications would still access the information in the higher layers to prevent duplicate data entry and usage. However, the read/write capabilities would be restricted to the mission and the application(s) supporting that mission. There may be elements in the mission-specific applications that should be shared across the services in joint operations. The PIC mission management should reflect those requirements.

Within this layer, a function-specific requirement could be added as needed. Deployment information is a possible example. For a particular deployment, the information on personnel from several DoD components could be accessed in a common area on the PIC. Once units are deployed, mission critical data elements encoded in the card could be retrieved from the command database used to manage the deployment. When completed, this area could be erased.

As needed, unit applications could be placed at this layer if the applications are not prone to continual change. If the applications are temporary, they could be placed in this level or lower levels of the PIC.

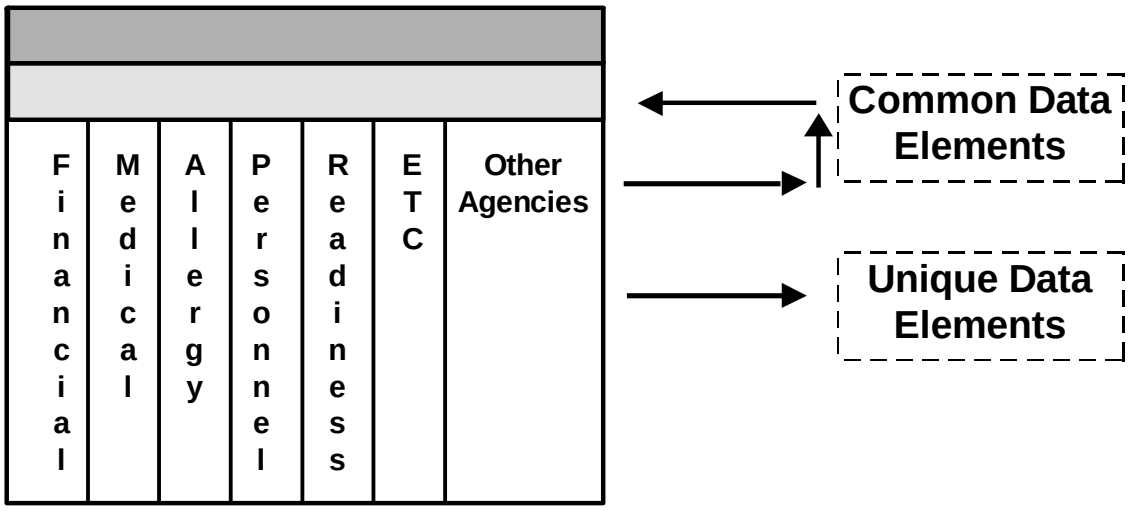


FIGURE D-3. Component information on the PIC

D.6. OTHER POSSIBLE LAYERS

D.6.1 Other possible layers. The most common "other" function would consist of a "scratch pad" function contained in this layer. The scratch pad would be for the temporary storage of data that could be retrieved

in another database application once the PIC is inserted into the proper reader/writer for use by the application in that particular layer.

Section 6 of this document identifies the need for a medical emergency scratch pad. This scratch pad would be contained at this level of the PIC. Other possible temporary applications would use the scratch pad.

Other potential layers depend on the mission or component/service requirements. Unit-specific applications are an example of other layers.

CONCLUDING MATERIAL

Custodians:
DISA-DC
Army-AC
Navy-NM
Air Force-02
DLA-DH
DMA-MP

Preparing activity:
DISA-DC
(Project IPSC 0348)

Review activities:
OSD - DO, IQ, IR
DISA - DC1, DC5, DC7
Army - AM, PT, TM1, TM3, SC1, SC2, SC3
Navy - AS, CG, CH, EC, MC, NC, ND, OM, TD
Air Force - 13, 16, 17, 19, 29, 33, 84, 90, 93, 99
DIA - DI
MISC.- CB, CI,DI, NS, OST, US

Industry associations:
SCF

Civil agency coordinating activities:

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1,2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER **MIL-HDBK-501**	2. DOCUMENT DATE (YYMMDD) 97 04 15

3. DOCUMENT TITLE
DEPARTMENT OF DEFENSE HANDBOOK PORTABLE INFORMATION CARRIER

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include Zip Code)*	d. TELEPHONE *(Include Area Code)* (1) Commercial (2) AUTOVON *(If applicable)*	7. DATE SUBMITTED *(YYMMDD)*

8. PREPARING ACTIVITY DISA/JIEO CENTER FOR STANDARDS

a. NAME JAMES BARNETTE	b. TELEPHONE *(Include Area Code)* (1) Commercial: (703) 735-3557 (2) AUTOVON: 653-3557
c. ADDRESS *(Include Zip Code)* **ATTN: JEBEB** **10701 PARKRIDGE BLVD.** **RESTON, VA 20191-4398**	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340