Configuration Management Plan
For the
Smart Card

Date

Agency

SECTION 1 ADMINISTRATION REMARKS AND VERSION CONTROL

1.1 Plan Maintenance

1.1.1 The Configuration Management Plan (CMP) is intended to be a "living document" and as changes occur to the smart card and the smart card platform they will be reflected in this document. This section will be used to maintain version control for the CMP. As changes are suggested and implemented, they will be reflected in chronological fashion. All changes and registered uses of the smart card will be recorded and tracked by the Agency.

Version	Date	Notes
1.0		
1.1		

1.1.2 Baseline: Final as of Date

1.1.3 Version 1.1: Final as of Date

1.1.3.1 *Changes:*

1.1.3.2 Corrections due to...

1.2 Plan Approval

1.2.1 Revisions to the CMP that are administrative in nature should be incorporated and annotated are required, but will not require formal vetting. Significant changes should be reviewed first in context, then, depending on the significance, reviewed in the entire CM process. The CMP will be evaluated on a bi-yearly or 2 year basis unless a significant change in the process occurs. Recommended changes to the CMP shall be reviewed by Agency/Governing Body for acceptance into the CMP.

Table of Contents

SECTION 1 ADMINISTRATION REMARKS AND VERSION CONTROL 2

1.1 Plan Maintenance 2

1.2 Plan Approval 2

SECTION 2 SUPPORTING DOCUMENTATION 5

2.1 References 5

2.2 Definitions 5

2.3 Acronyms and Terms 6

SECTION 3 INTRODUCTION 9

3.1 Purpose 9

3.2 Background 9

3.3 Scope 9

3.4 Objectives 10

SECTION 4 ORGANIZATION 11

4.1 Smart Card Management Organizational Structure 11

4.2 System Configuration Management (SCM) Organization Roles and Responsibilities 11

SECTION 5 CONFIGURATION MANAGEMENT ACTIVITIES 12

5.1 Configuration Identification 12

5.2 Configuration Control 12

5.3 Using Data and Functional Applets 21

5.4 Configuration Status Accounting 21

5.5 Audit/Review 22

APPENDICES A-1

APPENDIX A Organizational Charters A-1

APPENDIX B Federal Smart Card Working Groups B-1

APPENDIX C Applet Configuration Identification (ACI) Instruction and Datasheet C-1

APPENDIX D Change Request Proposal (CRP) Instruction and Form D-1

APPENDIX E Developers Support Request (DSR) Instruction and Form E-1

APPENDIX F Data Risk and Privacy Compliance Assessment F-1

APPENDIX G Configuration Management Stakeholders G-1

SECTION 2 SUPPORTING DOCUMENTATION

2.1 References

2.1.1 Documents that support the smart card configuration management process include:

2.1.1.1 MIL-HDBK-61A (SE), Configuration Management Guidance, February 7, 2001. The military handbook provides guidance and information to individuals responsible for Configuration Management.

2.1.1.2 National Institute of Standards and Technology (NIST) Specification, "Government Smart Card Interoperability Specification (GSC-IS) V2.1", July 16, 2003. The GSC-IS defines an architectural model for interoperable smart card service provider modules, compatible with both file system cards and virtual machine cards.

2.1.1.3 IEEE 12207 Series, Software Life Cycle Processes; Life Cycle Data; Implementation Consideration. Provides a comprehensive, concise description of each important software life cycle process, a total of seventeen processes in all.

2.1.2 Various individual systems using the smart card are widely distributed and must rely on their own CM processes to identify and integrate announced changes to smart card configurations. The smart card interfaces with several systems that have their own configuration management processes and supporting CM plans.

2.1.3 In an environment of emerging technologies, the smart card and standards that govern smart card technology are evolving. At any given time, several sets of standards may be applicable to a number of configurations of the smart card due to the shelf life of the card in circulation.

2.2 Definitions

a) Applet. A JAVA program module stored on the integrated circuit chip (ICC). It contains program code to store, retrieve, or manipulate different sets of data stored in or passed to it. Application programs running on a host computer or other applets stored on the ICC can access the data or call for services through the applet's program code. An applet is designed primarily to store data and is often referred to as a "container."

b) Application Program. A program that runs on a host computer and accesses the data and applets stored on the ICC of a smart card through a smart card reader/writer.

c) Configuration Audit. A process performed by either an internal or an independent system engineering group to ensure the process of configuration management can adequately answer questions regarding the management of change.

d) Configuration Item. Any hardware, software, or combination of both that satisfies an end use function and is designated for separate configuration management.
e) Container. An applet designed primarily to store data for retrieval by an application program running on a host computer or other applets co-located on the ICC.
f) Configuration Management. A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
g) Controlled Spaces. This relates to bases, buildings, and/or offices currently using some form of access control. This does not include higher-level security facilities dealing with classified information and processes above the unclassified level.
h) Interface Management. The management of the performance, functional and physical characteristics required to exist at a common boundary. In terms of the smart card, this involves the exchange of information between cards, card readers and other computerized equipment.
i) Legacy System. This term relates to information systems that have been in use for a significant period of time and therefore have some history. In most cases the application software was originally "stovepipe" or single purpose in nature. In many cases, it has been necessary to work out interface agreements between stovepipe applications when certain data are required either within the application or external to it.
j) Life Cycle Manager. The specific roles and responsibilities for the Life Cycle Managers (LCMs) are defined by the other Agencies that are responsible for the smart card at their organization.
k) Reader. An electromechanical device attached to a host computer that can read one of the machine-readable media imbedded or applied to a smart card, or other ID card. Media include smart card ICC (contact and contactless), magnetic stripe, and bar codes. Smart card and magnetic stripe readers often can also write to, or encode, the media.
l) Sponsoring Organization. The sponsoring organization for a change request can be…
m) System Configuration Management. System configuration management is the process of identifying and defining the items in the system, controlling the change of these items throughout their lifecycle, recording and reporting the status of items and change requests, and verifying the completeness and correctness of items.

2.3 Acronyms and Terms

Term Abbreviation	Explanation
ACI	Applet Configuration Identification
AID	Application Identifier
API	Application Program Interface
BCA	Business Case Analysis

Term Abbreviation	Explanation
BPI	Business Process Improvement
BSP	Biometric Service Provider
CA	Certificate Authority
CAPI	Cryptographic Application Programming Interface
CI	Configuration Item
CIO	Chief Information Officer
CIO EB	Chief Information Officer Executive Board
CM	Configuration Management
CMP	Configuration Management Plan
CMS	Change Management System
CONOPS	Concept of Operations
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-The-Shelf
CRP	Change Request Proposal
CSP	Cryptography Service Provider
DEPSECDEF	Deputy Secretary of Defense
DHRA	Department of Defense Human Resources Activity
DoD	Department of Defense
DSR	Developer Support Request
EEPROM	Electrical Erasable Programmable Read Only Memory
FIPS	Federal Information Processing Standards
GCA	Generic Container Applet
GSA	Government Services Agency
GSC-IS	Government Smart Card Interoperability Specification
HSM	Hardware Security Module
IA	Information Assurance
ICC	Integrated Circuit Chip
ID	Identification
IP	Issuance Portal
IT	Information Technology
IV&V	Independent Verification and Validation
KB	Kilobyte
LCM	Life Cycle Manager
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSD	Office of Secretary of Defense
OUSD(C)	Office of Under Secretary of Defense, Comptroller
OUSD(P&R)	Office of Under Secretary of Defense, Personnel and Readiness
PA&E	Program Analysis & Evaluation
PDF	Portable Data File
PMO	Program/Project Management Office
POC	Point of contact

Term Abbreviation	Explanation
SCM	System Configuration Management
TOR	Task Order Request
VO/LRA	Verifying Official/Local Representative Issuing Agent
VM (JC 2.1)	Virtual Machine (Java Card, version 2.1)

SECTION 3 INTRODUCTION

3.1 Purpose

3.1.1 The purpose of the CMP is to describe the process for the management of the smart card platform configuration items. Items required for configuration management include: card stock, an ICC, specifications for interfacing (middleware, magnetic stripe, bar codes, and surface printing), changes to policy, cardholder recipient population, infrastructure requirements, development, integration, fielding and sustainment to the smart card. This CMP establishes the method for identifying, implementing, controlling, accounting for, and auditing changes to the approved smart card configuration baseline, as it exists at any point in time. Additionally, the CMP includes organizational roles and responsibilities, guidelines, detailed operating procedures, and data sheets to insure proper preparation, review, and approval of configuration control documentation.

3.2 Background

3.2.1 Provide program background….

3.3 Scope

3.3.1 The Configuration Management (CM) process defined in this plan applies to agencies using the smart card and various functional groups involved in defining and using the functionality and content of the smart card. Primary responsibility for implementation of the smart card CM process rests with the Agency.

3.3.2 The CMP defines the process by which developers of applications, who use the smart card, can access standard smart card platform resources and install their own unique data and functions. Functional proponents and system developers are required to register their applications with the Agency in the early stages of development to allow distribution of documentation and access keys and insure that announcements and warnings can be distributed to all organizations that may be impacted. All new functionality proposed for implementation on the smart card must be submitted for validation and/or testing prior to implementation to ensure that it is compatible with installed functions, smart card support infrastructure and does not undermine or interfere with the validated security of the smart card platform.

3.3.3 Components that may be interested in similar applications are encouraged to develop requirements jointly and, where possible, introduce new Department-wide applications. The CMP defines a process for establishing new groups or designating existing functional groups to facilitate this process.

3.3.4 This document defines processes and procedures for Agencies that are involved in the development of smart card applications and the smart card.

3.4 Objectives

3.4.1 The objectives of the CM process described within are to:

- Implement the configuration management policies established by the Agency.
- Compile consistent configuration data that defines baseline identification of smart card configuration items, their features, and their capabilities at any point in time.
- Provide consistent and unified status accounting of all baseline documents and changes thereto; and, provide a mechanism for requesting changes to the smart card baseline.
- Provide a method for obtaining a coordinated review of proposed changes to the smart card.
- Track configuration control decisions;
- Make configuration identification data available to communities needing data for designing and configuring applications using the smart card.
- Define a mechanism for obtaining certification of user-developed elements loaded onto the smart card.

3.4.2 The CM Process is the mechanism to evaluate proposed changes, notify impacted organizations in advance of forthcoming changes, and to insure an orderly and accurate integration of new capabilities and features. The smart card CM process focuses on card capabilities that support applications while tracking implementation of specific solutions approved for use within the designated space on the ICC.

3.4.3 The CM process and approach is flexible enough to provide applicability across multiple applications while ensuring a standard process for version control of the base platform.

.

SECTION 4 ORGANIZATION

4.1 Smart Card Management Organizational Structure

4.1.1 Figure 4.1.1 is the organizational structure of the CM process containing the identified organizations.

Figure 4.1.1 Organizations Supporting Smart Card CM

4.2 System Configuration Management (SCM) Organization Roles and Responsibilities

4.2.1 This CMP defines organizational roles and responsibilities to ensure that the smart card platform and applications developed for use in conjunction with the smart card are executed on time and remain consistent with stated requirements. In the following paragraphs, stakeholder roles and responsibilities are provided to help define how the coordination efforts are accomplished and to identify what levels and criteria are required to approve changes to the smart card. The primary organizations involved are the:

4.2.2 The above organizations must work collectively to ensure that configuration of the smart card platforms and approved applications are maintained and managed.

SECTION 5 CONFIGURATION MANAGEMENT ACTIVITIES

5.1 Configuration Identification

5.1.1 The smart card CM process encompasses three distinct areas: the baseline configuration of the smart card, the operational and functional utilization of the smart card, and the software associated with the smart card. Configuration Management (CM) outside the above areas will be handled on a case-by-case basis or as prescribed by the Agency.

5.1.2 The first area for CM is the baseline configuration of the smart card, including its physical properties and applicable standards, as presented in the Task Order Request (TOR) submitted for bids through the U.S. General Services Administration (GSA) award of Smart Access Common Identification Card contract. Any changes to this description will require a Change Request Proposal (CRPs are explained in Section 5.2.9). Figure 5.1.2 contains an illustration of the configuration items found on a smart card ICC in circulation. A more detailed list of the smart card configuration items is provided in Appendix X.

Figure 5.1.2 Contents of the smart card Integrated Circuit Chip (ICC)

5.1.3 The second area of focus for CM activities is with the operational and functional utilization of the smart card. The core applets are provided with the initial issuance of the smart card for identification, physical access to buildings and controlled areas, and logical access to computers and networks. As the functionality of the smart card expands, access to additional data may be necessary. This may require possible engineering changes to the format of data on the smart card and/or interface activities with legacy application systems. Information assurance activities are included as a function of the CM process for adding or accessing additional data with the smart card. Standards developed and implemented for applications, middleware, and the smart card platform apply regardless of whether the application or platform is revised or changed for performance reasons. Application development includes building the necessary interfaces to other systems.

5.1.4 The third area of focus for the smart card CM process deals with the software that allows the smart card to function: card reader interface software, client/server based software, and functional applets or data containers that are placed on the card.

5.2 Configuration Control

5.2.1 Changes to smart card applications and the smart card platform are managed commensurate with the risk associated with implementing the change. Risk is

determined by the Agency submitting the change and verified throughout the CRP review process. Changes to the smart card are submitted via the CRP process described below. Depending on the scope of the change request, submission of a change request may reside at one (or more) of several levels. The Agency is the decision making body for CRPs and based on the type of change request, can either approve, concur or non-concur with the proposed change.

5.2.2 The most basic implementation of the smart card involves using the various media “as is” at the time of card issuance. Populating the magnetic stripe represents a higher level of complexity and is handled by the local organization responsible for the use of the magnetic stripe, in most cases a security organization dealing with physical access. The smart card magnetic stripe is not populated as a function of personalizing the card at the time of issuance.

5.2.3 A more complex level of implementation requires altering the information contained on the non-ICC media of the card. Any changes to the format or content of the barcodes require an advocate to document their via the CRP process.

5.2.4 Modifying the structure, functionality, or content of the ICC on the smart card represents an additional level of complexity. Content of the chip typically involves adding data to the chip in the form of expanded or additional storage applets to support retrieval or modification of the data on the ICC.

5.2.4.1 Any changes to the content of the ICC require an advocate to document their request via the CRP process.

5.2.4.2 Changes to the content in the specific area on the ICC only need to satisfy the Agency specific configuration management policies, but may require coordination of testing with the Smart Card Issuing Agency. Formal integration testing by the applet manager, in coordination with the Agency testing center, is performed to ensure that baseline smart card functionality is not affected by the new or modified applets.

5.2.5 Application managers are requested to ensure that descriptive details and contact information, pertaining to an application, are submitted for processing. At a minimum, each software application using the smart card should furnish the application data called for on the sample Developer Support Request (DSR) data sheet. A replica of this data sheet can be found at Appendix D, page D-1. Completing this data sheet registers an organization’s intentions to use the smart card in a particular application. Additionally, this data can be disseminated for informational purposes and also to reduce duplication of efforts.

5.2.6 In addition to a completed data sheet, applet/application managers may be required to submit for review a business case analysis (BCA), the testing to which the applet/application was subjected, the interfaced applications, fielding

methodology, and the requirements satisfied by the application. The fielding methodology must address the concerns related to placing applets or data containers on the smart card and populating the containers with the appropriate data. Through the Agency, this information is made available to accommodate future smart card development and provide an audit trail reference of changes made to any legacy system.

5.2.7 Data, either residing on the smart card or being accessed via the smart card, is a major issue from multiple perspectives. Tactical concerns for safety of the U. S. warfighter are paramount. Because of this, the data risk and privacy compliance assessment is a crucial part of the supporting documentation and provides the basis for identifying alternatives to mitigate any identified vulnerabilities. This guidance is for all Agencies requesting to place data on the smart card.

5.2.8 The Agency/Working Group recommends how much space should be allocated for specific use, generally consumed in the form of applets. The initial version of the smart card has a minimum of ## kilobytes (K) of area on the ICC for specific use. Applets can be added as long as there is room to add information. Instances where more than ## K of space is required are dealt with via the CRP process.

5.2.9 Change Request Proposals (CRPs)

5.2.9.1 Change Request Proposals (CRPs) are an official request to make a change to the smart card and are submitted to the Agency by a Sponsoring Organization.

5.2.9.2 Specific proposals will be evaluated primarily for adequacy of supporting infrastructure and funding, compliance with applicable standards and policies, and impacts outside the Agency. Additionally, proposals will be examined to include determination of the benefit across the Agency. All proposals will be reviewed within the context of smart card resource (primarily space) availability and proposed functionality. Proposals requiring major contributions, funding, and manpower from outside the sponsoring organization's purview can be expected to undergo detailed review by affected staffs.

5.2.9.3 There are three types of CRPs: Policy, Technology/Topology, and Technical Activity Notification. The process that the CRP follows coincides with the type of change that is being proposed. The following is a description of each CRP type:

- **Policy CRPs**: Address smart card policy changes.
- **Technology/Topology CRPs**: Address change requests to smart card technology, such as the ICC, and/or topology, such as the wording on the smart card.

- **Technical Activity Notification CRPs**: These are CRPs that represent an Agency action item to submit changes that impacts the smart card architecture in order to notify the technical community.

5.2.10 CRP Process

5.2.10.1 As the smart card program evolves, so do the tools, technologies, and policies that govern the program. As such, a process for controlling and monitoring change must be in place and adhered to in order to effectively manage change. Over time, the process has been refined in order to provide high-quality service. The CRP starts with submission of a change request. The following sample change request flowchart and process flow defines the requirements for a submission of a Policy or Topology/Technology CRP to the smart card program and the progression of the CRP following the submission:

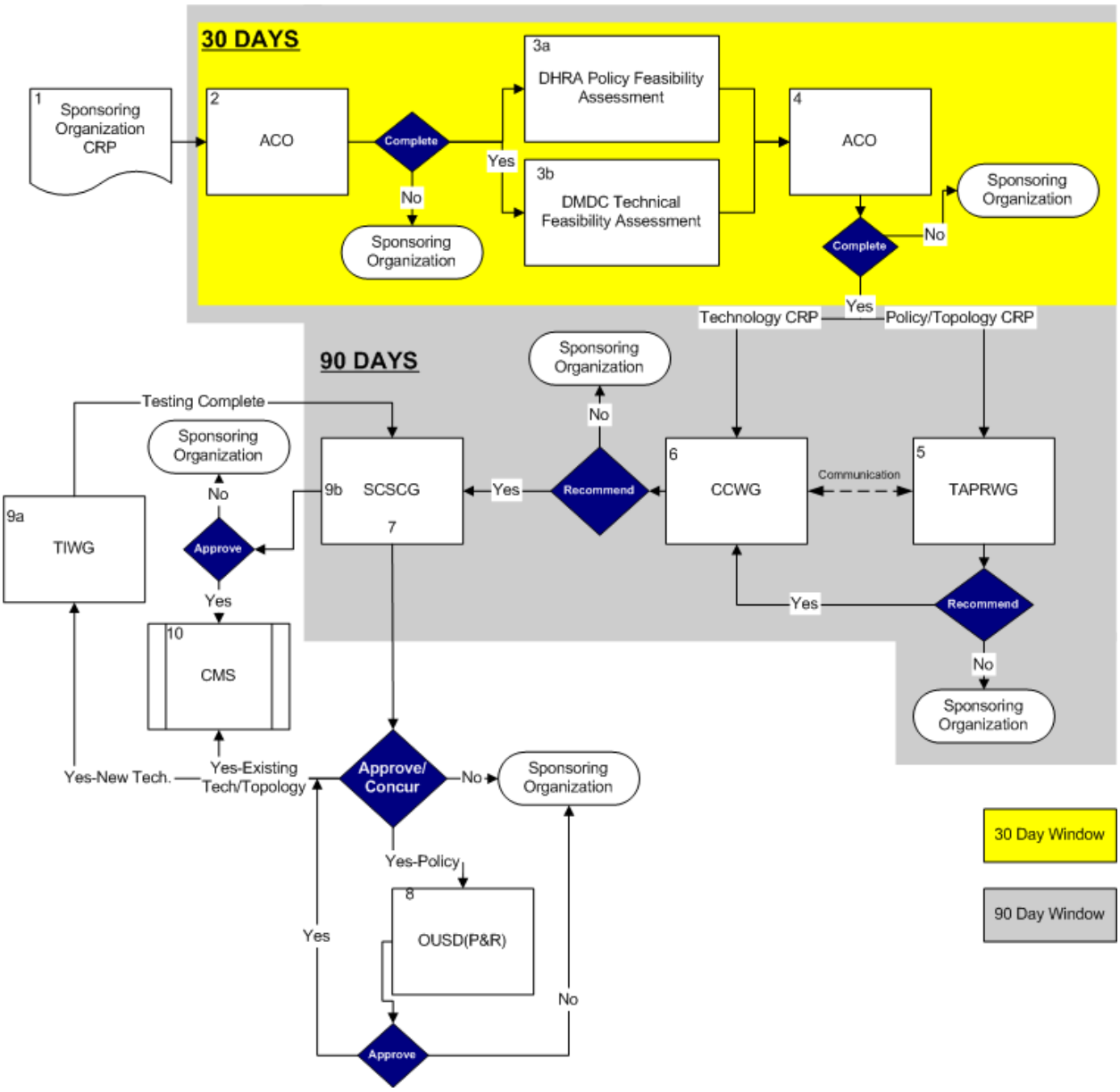

Figure 5.2.10.1 Sample CRP Submission Process

5.2.10.2 First, the sponsoring organization requesting a change must completely fill-out a CRP form according to the associated requirements on the form for the Policy or Technology/Topology change requested and the appropriate supporting documentation, outlined below, must be collected for submission to the Agency. The most current CRP form can be located on the Agency website. Supporting documentation requirements provided directly on the CRP form or as an attachment to the form for the respective CRP types may include:

- **Policy**
  - Memorandum/authority document
  - Data feed/source
  - Target population

- Proposed solution (i.e. symbol, seal, nomenclature, etc…)

- **Topology**
  - Proposed solution (i.e. symbol, seal, nomenclature, etc…)
  - Change to card face
  - Printing/placement
  - Technology placement
- **Technology**
  - Data Risk and Privacy Compliance Assessment
  - Developers Support Request (DSR) Datasheet
  - Data/Applet Management and Maintenance Plan
  - Security Assessment (NSA/FIPS Certification, etc)
  - Applet Configuration Identification (ACI) Datasheet
  - Business Case Analysis (BCA)

5.2.10.3 As soon as the Agency receives the CRP and supporting documentation from the sponsoring organization, the thirty-day and ninety-day period for review begins. Upon receipt of the CRP and supporting documentation, the Agency will make an initial assessment to ensure that all the necessary materials have been provided. The Agency may determine that the CRP and supporting documentation will require further details and will return the documentation to the sponsoring organization for coordination. *NOTE: If a CRP is returned to the sponsoring organization at any point in the CRP process the timeframe for review (i.e. 30/90 day period) starts over upon re-submission of the CRP.* Alternatively, if all documentation has been included and is complete , thus meeting the Agency's requirements, the Agency will assign a CRP number and, post the CRP to the website, submit the CRP and supporting documentation for a Policy Feasibility Assessment and a Technical Feasibility Assessment. These assessments are conducted in parallel.

5.2.10.4 Feasibility assessments are performed by the appropriate Agency. The following feasibility studies will be conducted on the CRP and supporting documentation:

5.2.10.4.1 **Policy Feasibility Assessment:** The policy Agendy will determine if the proposed recommendation:

- Has been previously addressed and rejected or adopted in another policy;
- Conflicts with current policy;
- Is a change/modification to current policy; and/or
- A new policy recommendation.

5.2.10.4.2 **Agency Technical Feasibility Assessment:** The Technical Activity will determine if the recommendation:

- Is Commercial-off-the-shelf (COTS) technology that is technically achievable;

- Can be achieved on the current smart card configuration or if a configuration change is required;
- If the change will necessitate a new applet or can utilize the existing applet;
- Ensure that it will not conflict with other containers or elements currently residing on the smart card; and/or
- Ensure that the change will not violate the security integrity of the smart card.

5.2.10.5 After the required feasibility assessments have been completed, policy and Agency technical resource will return the CRP and supporting documentation along with a report documenting the results of the assessment to the Agency.

5.2.10.6 *NOTE: This step must be completed within 30 days of the CRP submission.* At this point, the Agency determines, based on the feasibility assessments, if the CRP requires additional revisions by the sponsoring organization. Additionally, this step marks the end of the thirty-day timeframe. If revisions are necessary, the CRP and supporting documentation will be returned to the sponsoring organization for revision or termination. Providing the CRP, supporting documentation, and assessments are acceptable, the Agency will forward the CRP to the appropriate working group for coordination.

5.2.11 Configuration Change Approval Guidelines

5.2.11.1 Request for changes to smart card policy, topology, or technology are initiated with a Change Request Proposal (CRP). Such requests include changes to: cardstock body, ICC, data transfer and pin management protocols, compression and cryptographic algorithms, security domains, architecture, data elements, inventory control processes and nomenclature on the smart card. Furthermore, changes to the card recommended by the vendor/manufacturer requiring applet additions/modifications or other modifications that affect the use or appearance of the card must be exposed to the CRP process.

5.2.11.2 Implementing policy changes should be staffed through all affected policy offices and approved by the policy proponent prior to formal submission of the smart card CRP.

5.2.11.3 Vendors and contractors do not have the authority to direct other vendors or contractors to make a change to the approved smart card specifications; therefore, all requests for proposed changes by vendors/contractors must go through the CRP process defined herein.

5.2.11.4 The timeframe for CRP review and approval and/or concurrence/non-concurrence of all completed and signed CRPs is 90 days from the date of submission. However, from the point of approval or concurrence to actual implementation the timeframe will vary depending upon:

- Number of approvals required (e.g., GSA interoperability specification, FIPS certification).
- Time required to accommodate the changes (e.g., middleware, applications using the smart card).
- Time required to accommodate the logistical issues (e.g., card production lines).
- Time required to distribute information on the changes in card appearance through State Department channels.
- Time required to consume existing card stock.

5.2.12 CRP Priority and Processing

5.2.12.1 CRPs are prioritized as Statutory (mandated by law), Urgent (impacts the warfighter), or Routine, depending on the impact of the proposed change. Initially, the sponsoring organization will identify the CRP priority and the Agency will review the CRP and come to mutual agreement on the priority classification. CRPs prioritized as Statutory will receive an expedited review and coordination. CRPs prioritized as Urgent will also receive expedited review and coordination in order to be entered into the CMS as soon as possible. As referenced above, the timeframe for the review and approval of all completed and signed CRPs is 90 days. Approved changes will be incorporated into normal periodic developmental releases.

5.2.13 Supporting Documentation

5.2.13.1 An explanation of why the change is required or desired should be provided and is required with each CRP submission. Rationale should present the benefit, risk reduction, or other effect of implementing or not implementing the proposed change. If applicable, indicate alternatives that were rejected and the reason for rejection. In addition to the rationale or reason for the change, the required supporting documentation based on the type of change requested should accompany all CRPs.

5.2.13.2 To expedite the change request process, it is imperative that the appropriate supporting documentation is included with the submission of the CRP. The type of CRP will determine the required documentation.

5.2.13.3 Policy change requests, such as including a new community of cardholder recipients or changing the wording on the smart card may contain the following supporting documentation:

- Memorandum
- Data feed/source data supply
- Target population
- Proposed solution (i.e. symbol, seal, nomenclature, etc…)

5.2.13.4 Additionally, changes to policy must account for anticipated changes in the cards topology, architecture, and technology to accommodate the change.

For example, a new community of smart card recipients may be required by policy and the change will have an impact on the topology of the card since the new community will require their own seal. Therefore, the CRP must recommend a solution to address the change to the seal as part of the Policy CRP submission.

5.2.13.5 Topology change requests, such as a change to the ICC size by an increase to the chips foil size, may require the following supporting documentation:

- Proposed solution (i.e. symbol, seal, nomenclature, etc…)
- Change to card face
  - Printing/placement
  - Technology placement

5.2.13.6 Additionally, if a change in the smart card's topology impacts the technology on the card then the CRP must include a discussion addressing the impact and proposing a solution.

5.2.13.7 Technology change requests address new technology, such as a contactless card or introduction of a new ICC, and also existing changes to the technology on the card such as the ICC, barcode, and/or magnetic stripe. Additionally, changes to technology may impact the data on the smart card in the form of a change to an applet.

5.2.13.8 Change requests affecting the data on the smart card must be accompanied by an Applet Configuration Identification (ACI) sheet, a data/applet management and maintenance plan, and a data privacy and risk assessment. In order to add data to the smart card or to change functions on the card, an existing applet must be modified or a new applet must be added. Additional information must be provided to support configuration management, smart card space accounting, validate continued compliance with the FIPS 140 certification, and package the applet for loading onto the smart card. This information is submitted on an ACI data sheet. A sample copy of the ACI and instructions are provided in Appendix B, page B-1.

5.2.13.9 Additionally, a data/applet management and maintenance Plan should be provided to the Agency. The plan should describe the management structure and responsibilities, how joint operations will be coordinated, the data sources and applications that will update the card in a timely manner, the applications or classes of applications that will use the data, how use will be controlled, and data backup/recovery procedures.

5.2.13.10 Lastly, a data risk and privacy compliance assessment must be provided to determine if the data imposes any new risks on the cardholder in terms of increased physical vulnerability in a combative tactical and non-tactical environment. Appendix F, page F-1 provides further clarification and a sample assessment format.

5.3 Using Data and Functional Applets

5.3.1 Agency-wide Applications

5.3.1.1 Department-wide applications are defined as the software applications supporting the business processes and functionality performed in a joint environment and/or a shared capacity.

5.3.1.2 These initial Department-wide applications may be expanded to include: medical/dental, personal finance, exchange/commissary activities, logistics (manifesting, deployment, equipment issue, weapons accountability), vending, door locks, food service, and Morale, Welfare, & Recreation (MWR) Activities.

5.3.1.3 Any application that can be beneficial across the Agency, enhance business processes, or effectively utilize resources, is considered for inclusion in the shared area of the chip. User communities, vendors, applet/application managers, or industry representatives can suggest a modification or change to an application on the smart card. To initiate a change, the change request process defined herein must be followed.

5.3.2 Specific Applications

5.3.2.1 An allocated amount of space on the chip (i.e., a designated amount of Electrical Erasable Programmable Read Only Memory (EEPROM)) used for functionality, as deemed appropriate may be allocated. The overall management of specific application is the responsibility of the designated LCM. The development of the application is coordinated with the Agency technical office to validate (through testing) that the application does not affect or interfere with core smart card functionality. In order for an application to be placed on the ICC of the smart card, it must be registered with the Agency technical office, which allows the application to be utilized in a production environment.

5.3.3 Commercial-off-the-Shelf (COTS) Applications

5.3.3.1 Strongly encouraged to identify COTS products that may be utilized as part of a proposed application. Formal integration testing, by the Agency technical office, will be performed to ensure that the baseline smart card functionality is not affected by the new COTS application.

5.4 Configuration Status Accounting

5.4.1 The ability to effectively communicate change and the impact of implementing change is vital in the CM process. The Agency is responsible for tracking, managing, and maintaining an archive of the changes to the smart card's

configuration and platform. The Agency will communicate changes in the status of CRPs by means of the Agency website.

5.5 Audit/Review

5.5.1 Conduct an audit of smart card functions and print testing associated with the issuance process. Concurrently, a physical testing laboratory conducts IV&V tests to confirm compliance with standards and specifications called for in the acquisition. Independent laboratories, arranged by each card manufacturer, conduct FIPS 140 certification testing of cryptographic functions and the smart card platform as a cryptographic device. If modifications to the smart card platform architecture are made, re-certification testing may be required. Similarly, when the standard software components are modified, a battery of tests will be conducted. The Agency technical office performs or reviews the results of tests of the applet on the smart card platform to insure that the applet code does not violate any smart card rules or compromise any aspect of card security.

APPENDICES

APPENDIX A Organizational Charters

APPENDIX B Federal Smart Card Working Groups

APPENDIX C Applet Configuration Identification (ACI) Instruction and Datasheet

The Applet Configuration Identification (ACI) template is used to describe user-defined applets and request applet tests and validations that must be completed for all applets before they can be installed on smart cards. All user-defined applets must be managed by a Life-cycle Manager (LCM) and all ACIs pertaining to that applet should be submitted by, or through, the LCM. The Agency's Test Lab will conduct the validations and tests and coordinate any testing required by outside certification labs.

Persons wishing to add an applet should refer to the Configuration Management Plan (CMP) for a description of the LCM role and the steps through which this ACI and the CRP will be processed. The ACI must be submitted with a Change Request Proposal (CRP).

All ACIs for specific applets must be coordinated through the submitting Agency's smart card office. Changes involving policy changes should be submitted through the relevant policy office. Any questions about completing this form should be directed to the Agency smart card office. All communications with the Agency on ACIs and CRPs, including submission of ACIs, should be with this e-mail address:

The following instructions are provided to assist the person completing the ACI in providing all the required information. Use continuation sheets to extend sections that do not provide sufficient space. Add attachments if necessary. Check boxes are set by double clicking and clicking the "Checked" radio button in the pop-up window.

1. **ACI Number.** This tracking number will be assigned by the Agency upon receipt of the ACI, draft or signed. If submitting a revision, enter the original ACI Number and check the Revision box. The number will be of the form YYYYMM-nnr. "YYYYMM" is the year and month when the ACI Number is assigned and "nn" is a sequentially assigned number within the month. The "r", if present, is an alphabetic character indicating the revision.

2. **Date Prepared.** Enter the date that the form is submitted for review. Update the date as changes to the data are submitted, until signed.

3. **Applet Name.** Enter the name of the applet being submitted. Include an acronym if you wish. Suggest that the name be kept to 60 characters.

4. **CRP Number.** Enter the CRP Number of the CRP to which this ACI supports. Leave blank, if the CRP Number has not yet been assigned, and describe the CRP if not submitting together. The number will be of the form YYYYMM-nnr. "YYYYMM" is the year and month when the CRP Number is assigned and "nn" **is a sequentially** assigned number within the month. The "r", if present, is an alphabetic character indicating the revision.

5. **Applet ID.** The Technical Authority/Test Lab will assign this tracking number upon successful completion of the validation.

6. **Sponsoring Office.** Enter the Government organization name, office symbol, mailing address, office phone number(s) of the sponsoring office, and role of the office as it relates to this change. If another entity, such as a Life Cycle Manager (LCM), enter the name of the entity and the office information for the head of that entity.

7. **Primary Point of Contact -- Sponsor.** Enter the name, phone number(s), and e-mail address of the person who will handle management questions and is to receive periodic status reports.

8. **Developer Office.** Enter the Government organization name of the office, office symbol, mailing address, office phone number(s), and role of the office configuring or developing the applet. Indicate relationships among technical, functional, Government, contractor and product vendor POCs.

9. **Primary Point of Contact -- Developer.** Enter the name, phone number(s), and e-mail address of the person who will handle management questions and is to receive periodic status reports.

10. **Other POC(s).** Enter the name, organization name/office symbol, mailing address, phone number(s), e-mail address, and role in this change for one, or more, individuals. Enter at least one to serve as backup for the primary POC.

11. **Applet Type.** Indicate if this is a request to use an existing general container applet (GCA), implement a new instance of the general container applet, a user-developed applet, or a commercial applet. Also, indicate whether it is to reside in Department-wide or Component-specific space.

12. **Applet Size.** Indicate the compiled size of the applet in bytes.

13. **Target Implementation Date.** Enter date when deployment of the applet to smart card is expected to begin.

14. **User Community.** Identify the functional areas that will maintain or use the applet, indicating the number of workstations accessing the applet, frequency of access, and number of smart cards on which the applet will be installed. Indicate versions of the card on which the applet will be installed and any versions that will be excluded from implementation. Identify any unique hardware of operating system platform requirements for the applications.

15. **Applet Description.** Describe purpose and functions of the applet, including keywords (e.g., logical access, physical access, manifesting, and ordinance management). Identify the role of the applet in a deployed or ship-board environment

16. **Interfaces.** Identify workstation host-side applications and card-side applets with which the applet will interact.

17. **Data.** Identify the data that will be stored in the applet. Indicate the access rules (read only vs. read/write and PIN protection requirements). Identify backup and transfer procedures that will be used to transfer data from one card to another when a card is lost, or otherwise, reissued in either fixed installation or deployed environments. Identifying data that will be used when deployed and any data that should be removed before deployment. The following information should be provided

for each data element: data element name, data element description, alphanumeric type, length or range of data field, and access rules.

18. **Testing:** Identify the smart card platform(s) that will be used during development and test of the applet. Platform testing involves testing against the smart card system as a whole including card specifications (manufacturer, operating system) and terminal specifications (manufacturer of card acceptance device, desktop platform, and middleware).

19. **Supporting Documentation.** Listed documentation is required to begin testing. Check the boxes that correspond with the documents submitted in support of the ACI at this time. List any other attachments included.

20. **Sponsor Signature.** The head of the submitting organization is expected to sign the CRP when formally submitting it. Enter name, organization, and date. Once signed, the CRP and all attachments should be transmitted via a single e-mail to the Agency, or the next node of the submission chain. A wet signature is not normally required, however, there are exceptions. The Agency will inform the submitter if a wet signature is required.

Applet Configuration Identification	1. ACI NUMBER (*Assigned by Agency*) ☐ Revision	2. DATE PREPARED
	3. APPLET NAME	
	4. REFERENCE CRP NUMBER	5. APPLET ID (*Assigned by TA*)

6. SPONSORING OFFICE	7. PRIMARY POINT OF CONTACT -- SPONSOR
	A. NAME
	B. TELEPHONE NUMBERS COML: DSN:
	C. E-MAIL ADDRESS

8. DEVELOPER OFFICE	9. PRIMARY POINT OF CONTACT -- DEVELOPER
	A. NAME
	B. TELEPHONE NUMBERS COML: DSN:
	C. E-MAIL ADDRESS

10. OTHER POINTS OF CONTACT		
11. APPLET TYPE	12. APPLET SIZE *(bytes)*	13. TARGET IMPLEMENTATION DATE
14. USER COMMUNITY *(Description & Size)*		
15. APPLET DESCRIPTION		
16. INTERFACES *(List all host-side applications & card-side applets)*		
17. DATA (*List all data fields defined in applet*)		
18. TESTING (*Identify smart card platforms on which each was tested*)		

D. 19. SUPPORTING DOCUMENTATION

☐ Requirements Specification	☐ Source Code	☐ System Test Results
☐ Functional Design Specification	☐ System Test Design Specification	Other:
☐ Card-edge Specification	☐ System Test Scripts	

20 SPONSOR SIGNATURE *(Name, Organization, Date)*

Applet Configuration Identification
13 MAY 2002

Applet Configuration Identification	CRP NUMBER
21. CONTINUATIONS	

Applet Configuration Identification
13 MAY 2002

APPENDIX D Change Request Proposal (CRP) Instruction and Form

The Agency Change Request Proposal (CRP) must be used to request any changes to the smart card configuration. The CRP configuration includes the composition of the card stock and any technology embedded in it, the content and format of machine-readable information stored in or printed on the smart card, and the content and layout of any human-readable text and graphics printed on the card. Machine-readable information includes the integrated circuit chip, the magnetic stripe, and the bar codes.

All CRPs must be endorsed by the submitting organization. Any questions about completing this form should be directed to the Agency. All communications with the Agency on CRPs, including submission of CRPs, should be with this e-mail address: XXXX@XXXX.mil, Subject: “Change Request Proposal.”

Persons wishing to request a change should refer to the Configuration Management Plan (CMP) for a description of the steps through which a CRP is processed. A copy of the CMP can be found on the Agency home page at: <www.>. Originators are required to formally submit CRPs in final form with the fulfilled requirements for completion to include Business Case Analysis (BCA), LCM, and Service Secretary Memo (policy CRP) as appropriate.

The following instructions are provided to assist the originator submitting this worksheet in providing all the required information. The originator should be as complete and accurate as possible, adding attachments as required.

Section I - Tracking Information (1)

1. CRP Tracking Number: Select the appropriate box that indicates whether this is a new Change Request Proposal (CRP) or a revision to a previously submitted CRP. If this is a revision to an existing CRP, enter the original CRP tracking number in the space provided. New CRPs will be assigned a CRP tracking number by the Agency. This number will serve as a unique identifier for future reference. Enter the date the CRP is submitted to the Agency.

Section II - Change Request Proposal Information (Boxes 2 - 7)

2. CRP Title: Enter a short title for the change being requested.

3. CRP Priority: The CRP originator assigns priority of urgent or routine to indicate the urgency with which the CRP is to be reviewed, evaluated, and approved.

- Statutory CRPs that implement a new or changed regulatory requirement with stringent completion date requirements issued by an authority higher than that of the functional proponent and/or reflect changes in information technology (IT) policy are considered urgent

- CRPs affecting the Warfighter are considered urgent
- Urgent priority is used to make substantial changes in baseline configuration, have an immediate implementation need, and affect war fighting readiness such as making a significant and measurable effectiveness change in the operational capabilities or logistics supportability
- An urgent priority is defined as a CRP needing the review and evaluation to be completed within 30 days
- Routine matters include anything of a minor nature that do not affect readiness such as correcting technical deficiencies, effecting substantial life cycle cost savings, and/or adding new or modifying existing functional requirements
- Routine priority should complete the review and evaluation cycle within a 60-day period

4. Smart Card Change Impact: Identify the smart card and supporting system configuration items that will be impacted by this change request. More than one area can be impacted.

5. Configuration Items Impacted: Identify smart card elements and supporting systems that will be impacted by the change.

6. Description of Change: Completely describe the proposed change. This description should address the specific features, content, behavior, or appearance that is to be changed. It should be complete as possible and include references to policy documents, technical documents, and lists of data elements and codes. Provide illustrations, if necessary, for changes involving printing. Add attachments, as necessary.

7. Supporting Rationale: Identify improvements in effectiveness and operational savings in dollars and manpower that would result from this change. Identify the entities or populations that would benefit from the change. Build a business case for implementing this change. Identify negative impacts that would result or continue if the change were not implemented. Provide background to aid in understanding the significance of the change. Cite policy documents that are generating the need for the change.

Section III - Supporting Documentation (8)

8. Attachments: List documents that are submitted in support of the CRP. Documents must include a Business Case Analysis (BCA), a Life Cycle Manager (LCM), Funding Status (FS), a Data Risk and Privacy Compliance Assessment (PA), and Applet Configuration Identification (ACI) datasheet. A Service Secretary Memo must accompany any Policy-related CRPs. If “other,” please be specific.

Section IV – Sponsoring Organization Information (9 - 18)

9 -14. Sponsoring Organization Affiliation and Address: Enter the name and address (Street Number & Name, City, State and Zip Code) of the sponsoring organization.

15 - 16. Sponsoring Officer Information: Enter the name of the individual who is sponsoring the change request. This individual will serve as the main point of contact (POC) for the Agency and is responsible for answering questions regarding the change request.

17. Telephone Number: Enter the commercial and DSN telephone numbers for the POC specified in boxes 14 -15.

18. E-Mail Address: Enter the work e-mail address of the individual specified in boxes 15 - 16.

Section V - Signature Block (19 - 20)

19. Signature & Office: Enter the name and organization submitting the request. CRPs should be signed by executives with authority over impacted functional activities.

20. Date: Enter the date on which the CRP is signed and submitted for formal processing.

CHANGE REQUEST PROPOSAL (CRP)

SECTION I TRACKING INFORMATION

1. CRP TRACKING NUMBER

☐ New Request *(Tracking number assigned by Agency):* Tracker Number *(assigned by Agency)*

☐ Revision to Existing Request *(Provide CRP Tracking Number):* Date Draft CRP Submitted to Agency

SECTION II CPR INFORMATION

2. CRP TITLE

3. CRP PRIORITY

☐ Statutory (mandated by law)

☐ Urgent (impacts warfighter—provide justification)

☐ Routine

4. **SMART CARD CHANGE IMPACT** ***(Can be more than one)***

☐ Policy ☐ Topology ☐ Technology ☐ Technical Activy Notification Only

5. CONFIRGURATION ITEMS IMPACTED

6. DESCRIPTION OF CHANGE

7. SUPPORTING RATIONALE

SECTION III SUPPORTING DOCUMENTATIO

8. ATTACHMENTS *(must be included when submitting a completed and signed CRP)*

☐ Business Case Analysis ☐ Life Cycle Manager ☐ Funding Status

☐ Data Privacy & Risk Assessment ☐ Service Secretary/PSA Memo (Policy CRP) ☐ ACI

☐ Other (Specify)

SECTION IV SPONSORING ORGANIZATION INFORMATION

9. SPONSORING ORGANIZATION

10. STREET ADDRESS 1	**11. STREET ADDRESS 2**	
12. CITY	**13. STATE**	**14. ZIP CODE**
15. POC FIRST NAME	**16. POC LAST NAME**	
17. COMMERCIAL TELEPHONE NUMBER	**18. WORK E-MAIL ADDRESS**	

SECTION V SIGNATURE BLOCK

19. SIGNATURE & ORGANIZATION	**20. DATE**

Change Request Proposal, March 2003

APPENDIX E Developers Support Request (DSR) Instruction and Form

The Developer Support Request (DSR) is used to request documentation, test cards, and sample software to assist in the development of applications, using the smart card, and the development of applets to be installed on the card. The documentation and sample software is available for downloaded as the smart card Development Kit (SCDK) from the Agency's web site at <www>. The SCDK is also available in the form of a compact disk (CD) which can be obtained by completing this request This request should also be used to obtain test cards. Requests for test encoded-ICC test cards also require submission of a smart card (ICC) Test Card Request. All communications with the Agency on the SCDK, test cards, or other developer support matters should be with this e-mail address: <XXXX@XXXX.mil>.

The information on points of contact and the applications and applets is for the Agency developer database which is used to contact you in the event that change or alert information needs to be disseminated. The information is also posted on the Agency web site to assist developers in sharing information about similar applications.

The following instructions are provided to assist the person completing the DSR in providing all the required information. Use continuation sheets to extend sections that do not provide sufficient space. Add attachments (such as brief system descriptions), if available. Check boxes are set by double-clicking and clicking the "Checked" radio button in the pop-up window.

1. **Application Tracking No.** This tracking number will be assigned by the Agency. Requests for SCDKs and test cards can be tracked with this number.

2. **Request Date.** Enter the date that the request is submitted

3. **SCDK Tracking No.** This tracking number will be assigned by the Agency.

4. **Requesting Office.** Enter the Government organization, office symbol, mailing address, office phone number(s) of the requestor, and role of the office in the development/testing effort. Contractors and vendors normally would complete the developers section.

5. **Primary Point of Contact (POC) - Requestor.** Enter the name, phone number(s), and e-mail address of the person who will handle management questions and is to receive periodic status reports. This may be a Government employee or a contractor.

6. **Application/Applet Developer Office.** Enter the Government organization/office symbol or company name, mailing address, office phone number(s), and role of the office in the development/testing effort

7. **Primary Point of Contact - Developer.** Enter the name, phone number(s), and e-mail address of the person who will handle technical questions and is to receive periodic status reports. This may be a Government employee or a contractor.

8. **Other Points of Contact.** Enter the name, organization name/office symbol, mailing address, phone number(s), e-mail address, and role in this change for one, or more, individuals. Entry of additional POCs or phone numbers is encouraged if the primary POCs are hard to reach or are likely to change.

9. **Application/Applet Name.** Enter the name of the application that will be using the smart card or the applet that will be installed. Include an acronym if there is one. Suggest that the name be kept to 60 characters. Persons requesting test cards or smart card information to implement PKI logon should skip to Item 15 after checking the PKI LOGON FOR LAN checkbox and complete Items 11, 12, and 14.

Persons that have actually implemented an application using media on the smart card should check The IMPLEMENTED checkbox.

10. **Application Type.** Enter one of the following keywords if it applies to your application. If none are applicable, enter a short (1-3 words) descriptor that describes your type of application.
    A. access control
    B. attendance
    C. deployment
    D. food service
    E. manifesting
    F. MWR
    G. readiness
    H. utilization
    I. equipment accounting

11. **Workstations.** Enter a rough estimate of the number of workstations on which the application using the card's media, or in the case of a multifunctional applet, the applications will be running.

12. **Operating/Developer Environments.** .Identify the operating system(s), database system, or other specialized software that supports your application. Identify the developer environment (C++, Visual Basic, VBA, Java, Power Builder, etc.) that you use to develop and maintain your application. If you have a regular change release cycle, indicate the frequency of the releases and when they normally occur. Indicate whether it is operated in deployed tactical environments.

13. **Application Summary Description.** Briefly describe purpose and functions of the application. Indicate which card media is used.

14. **Readers/Encoders.** List (media, manufacturer, and model number) the readers and encoders your application uses to access the card machine-readable media. Note integrated devices, such as keyboards with built-in smart card readers.

15. **Items Requested.**

    A. Check the boxes for the items you are requesting. Note that the SCDK can be downloaded directly from the Agency web site. Any special requests should be noted in Item 16. A complete mailing address must be provided in Item 17.

    B. Indicate the number of test cards of each type you need to test your application or applet. If your application doesn't process any civilian or contractor cards, 2-3 cards should be sufficient. Five cards should give you one of each type. Note the populations processed in Item 16. If several versions of a card are in circulation, you may need more to test variations in card or middleware behavior.

    C. Requests for encoded ICC cards require approval by the Organization smart card office. See item 18. A request for more than 5 encoded ICC cards requires justification. Encoded ICC test cards use test keys and are good only against a test data base. A separate, unique e-mail address must be supplied in Item 16 for each of these test cards.

    D. Teslin refers to the thickly laminated green, red, blue, and tan ID Cards that have been in circulation since 1993.

    E. Cards supplied for bar code testing will be chip-less.

F. Cards supplied for magnetic stripe testing are blank cardstock since no magnetic stripe encoding is performed during the card issuing process.

16. **Special Requests.** Describe any special requests such as specific population types or card configurations/versions.

17. **Mailing Address.** Enter a complete address suitable for FEDEX delivery, which means the address cannot be a post office box. APO/FPOs should be used for overseas deliveries.

18. **Agency Approval Validation.** Agency will process the request, assign a tracking numbers for the test cards and SCDK, create and ship the cards/CDK, complete the remaining items.

Developer Support Request
21 MAY 2002

DEVELOPER SUPPORT REQUEST

1. APPLICATION TRACKING NO. *(Agency Use)*

2. REQUEST DATE

3. REQUESTING OFFICE

5. PRIMARY POINT OF CONTACT – REQUESTOR

A . NAME

B. TELEPHONE
COML:
DSN:

C. E-MAIL ADDRESS

6. APPLICATION/APPLET DEVELOPER OFFICE

7. PRIMARY POINT OF CONTACT – DEVELOPER

A . NAME

B. TELEPHONE
COML:
DSN:

E-MAIL ADDRESS

8. OTHER POINTS OF CONTACT

9. APPLICATION/APPLET NAME
Implemented

☐ PKI Logon for LAN ☐

10. APPLICATION TYPE

11. WORKSTATIONS

12. OPERATING/DEVELOPER ENVIRONMENTS

13. APPLICATION SUMMARY DESCRIPTION

CARD MEDIA USED: ☐ ICC ☐ Code 39 ☐ PDF417 ☐ Mag Stripe

14. READERS/ENCODERS

15. ITEMS REQUESTED

☐ SMART CARD Developer's Kit – SCDK (*compact disk)*

☐ Test Cards *(Normally 2-5 for each category)*

TEST MEDIA	CARD	TESLIN
Encoded ICC – Use ICC Card Request		
BAR CODES		
MAG STRIPE		

16. SPECIAL REQUESTS

17. MAILING ADDRESS *(Must Be FEDEX Accessible – Not PO Box)*

A. RECIPIENT'S NAME	B. ORGANIZATION/COMPANY		C. TELEPHONE
STREET ADDRESS 1	STREET ADDRESS 2		
CITY	STATE	ZIP	COUNTRY

18. AGENDY APPROVAL VALIDATION

☐ Approved ☐ Disapproved	A. DATE VALIDATED	B. DATE FULFILLED

APPENDIX F Data Risk and Privacy Compliance Assessment

PURPOSE AND SCOPE. This framework outlines the factors and issues one must address in assessing the impact of placing additional data on the smart card. The two types of risk that are recognized are personal and organizational. Personal risk includes risk from physical, psychological, financial, social, and economic harm, in a tactical and non-tactical environment. Risk to the organization(s) with which the cardholder is associated, either directly or indirectly must be accounted for. Designers of IT applications reading data from the smart card must recognize the risks posed by smart card data stored either temporarily in volatile memory or for extended periods on local storage devices. Additionally, the Agency restrictions on sharing that data with other applications and sites must be acknowledged.

SURVEY OF PERSONAL RISK. Revelation of personal data can result in the risks outlined in the following, either individually or in combination:

Physical Risk. Physical risk is associated with the tactical environment and an event where the individual may be captured and interrogated. Additionally, it could equally apply to an encounter with a criminal in a domestic setting. If the captor believes that there are Data elements on the smart card that would be helpful in an interrogation or criminal act, then the captor would have an incentive to physically compel the cardholder to reveal his/her PIN allowing the information to be accessed.

Psychological Risk. Psychological risk shares elements with the other risk types. Concern over protecting the data on the card generates the other risk types and adds to the cardholder's anxiety.

Financial Risk. Financial risk involves identity theft as the smart card is an identity token. Minimizing personal information commonly used in authentication, other than a commonly used ID number and name, can reduce this risk. Examples of such data would include date of birth, residence or home of record address, residential phone numbers, and family member names. While avoidance of Social Security Number (SSN) provides certain relief, a DIA assessment suggests that any other ID number used can be expected to be cross-referenced to SSN within six months. This risk might be exacerbated if the same access control mechanisms, such as a shared PIN, are used to access both the financial application and frequently used smart card functions where observation of PIN entry becomes a risk.

Social Risk. Social risk addresses the feeling of embarrassment or sense of self that might impact moral or performance. A social risk is the impact of revealing the cardholder's personal data (i.e. medical history) to individuals with whom the cardholder works. Data that reveals personal foibles or weaknesses in character or personality might feed personal fears or prejudices and provide one, or more, co-workers an opportunity to draw social or group lines.

Economic Risk. Economic risk is less direct than financial risk and concerns factors bearing on employment. It embodies the material damage of social risk. Data that reveals personal foibles or weaknesses in character or personality might jeopardize the employee's acceptance in the unit or office and his/her ability to function and progress as a member of the team.

ORGANIZATIONAL RISK. Revelation of personal data, especially the cardholder's PIN, can result in the following three main risks to the cardholder's organization:

Unit Intelligence Information. Personal role, qualifications, and training data or unit identity and location information stored on the smart card can reveal information about the units in the area.

Access to the Network. This access, depending on the cardholder's registered role, can provide access to sensitive information, permit sending unauthorized information, authorize an intruder initiate denial of service attacks, or give a hacker a toehold to hack into other, more sensitive, areas of the network.

Access to Physical Assets. This access may provide an intruder entry into facilities and access to specially protected assets (weapons, munitions, etc.).

The last two risks are PIN dependent and pose the greatest risk; however, the issues addressed in this framework, for the most part, represent the first risk.

PROTECTION OF DATA STORED ON SMART CARD. Safeguards built into the security framework of the smart card include the grouping of data and distribution into separate domains, which are defined by the applets. Each domain can be configured to have its own access control mechanism. The access control rules for any domain or access privilege include an option to require entry of the cardholder's PIN. For example, the basic identity data on the smart card requires the cardholder to present his/her PIN before access to any of the data is allowed. After unlocking the card with a valid PIN the data can be read by any application.

When adding new data to the smart card, the choice of domain in which the data will be stored requires careful consideration. If adding a data element to an existing domain increases the personal risk associated with that domain, either because of the personal risk posed by the data element or the added exposure from applications exposing the data, the LCM for that domain must determine whether the additional risk is acceptable.

APPLICATIONS USING THE CARD. Applications using the smart card must safeguard data read from the card and data that is made accessible as a result of unlocking domains. Applications operating on Agency networks and operating on portable devices require much more attention to protecting data. The following identifies current Federal and Agency programs that must be considered part of any strategy to protect the smart card and outlines additional steps that might be need to provide effective protection of the data:

Information Assurance Requirements. The starting point to protecting data exposed on the smart card will be the proper implementation of Agency Information Assurance guidance in terms of hardware and software, as well as procedures. If an application is compliant with the requirements, vulnerabilities against outside threats and some insider threats should be minimized. Threats from insiders must be addressed with additional strategies.

Protecting Smart Card Data When Accessible. An important strategy to reduce vulnerability of a smart card inserted into a reader is to construct the transaction so that the steps in the smart card access process are consolidated into one series of steps to minimize the time the card is in an accessible status.

Protecting Smart Card Access Mechanisms. Workstations that handle PINs and keys used to access the smart card must take special precautions to protect these data objects. Integrated devices that combine PIN keypads with smart card readers can markedly reduce vulnerabilities created by passing the PIN through peripheral cables and storage of the PIN in local memory. Where possible, transmission of PINs and keys between modules should be by secure link (using session encryption). It is important that, if a PIN or key is handled within the workstation, no trace of it is left immediately after its use.

Applications that use keys for accessing domains should take steps to obfuscate them when stored. Hardware security modules (HSMs) can prove useful in protecting the keys in these cases. Ultimately, applet managers are responsible for designing and implementing effective key management programs to secure the data in their applets.

PRIVACY REQUIREMENTS FOR APPLICATIONS. The guidance for protecting privacy in applications is extensive and detailed. A few functional areas, especially medical, have published additional guidance. Existing systems should have a System

of Records Privacy Notice, which either explicitly identifies the system or covers it by a blanket notice.

Each system identified as containing personal data accessible by a personal identifier, such as name or SSN, must publish a statement describing purpose, controls, possible distribution to other systems/organizations. This statement is known as a System of Records Privacy notice.

CONDUCTING A DATA RISK AND PRIVACY COMPLIANCE ASSESSMENT. This assessment focuses primarily on the risk assessment aspects, but needs to provide assurance that data capture processes and data storage strategies are compliant with privacy requirements. Furthermore, the data downloaded from existing databases must be consistent with the supplying system's system notice. All segments of the assessment should identify actions needed to insure that security and privacy objectives are met.

Analyze Risk of Adding Data to Smart Card. If adding new data, assess the impact in the risk areas. Identify existing smart card data elements that have comparable risk impact. Determine if combining the new data elements with existing data elements creates a new level of risk.

Assess Security Status of Applications Accessing the New Smart Card Data. Determine if the applications accessing the smart card meet all the Information Assurance security requirements as validated by an approved C&A. Additionally, determine if the environments (e.g., locked server room, networked office desktop, portable, or deployable laptop) in which the applications operate pose any risks.

Analyze Risk of Exposing Data in Application. Determine if the application or the operating environment exposes the data in such a way that personal or organizational risk increases.

Assess Applications' Compliance with Privacy Requirements. Ensure that applications meet the requirements of the Agency privacy program. Capitalize on the document and resources available at the Agency. Use the requirements of the System of Records Privacy Notice as a guide.

The following attached checklist is designed to ensure that all relevant risk and privacy issues are considered:

Guidelines for Assessing Risk of Adding Data Elements to the Smart Card – Part 1		
Factor	**Vulnerabilities/ Actions**	**Comments**
A. Risk of Adding Data to Card		
1. Identify risks posed by each of the new data elements – physical, psychological, financial, social, economic, organizational		
2. Identify existing card data elements of comparable risk		
3. Identify existing card data, when combined with the new data, could increase risk		
4. Identify periods data will be on the card and provisions for removing if not meant to be permanent		
5. Identify actions to mitigate risks		
B. Security Status of Accessing Applications		
1. Identify all applications that will have access to the new data elements		
2. Identify any unmet IA security requirements in these applications		
3. Identify C&A status of these applications		
4. Identify system/application/data vulnerabilities posed by insecure operating environments		
5. Identify actions to mitigate vulnerabilities		

Guidelines for Assessing Risk of Adding Data Elements to the Smart Card – Part 2		
Factor	**Vulnerabilities/ Actions**	**Comments**
C. Risk from Exposing Data in Applications		
1. Identify data elements read from card		
2. Identify domains/data elements exposed while accessing the target data elements		
3. Identify accessed card data elements that are not already part of the accessing application/database		
4. Identify other applications that will expose new data elements as a by product of accessing other data elements in a shared domain		
5. Explain how maintenance will be		

	limited to target data elements		
	6. Explain how maintenance applications will be separated from read-only applications		
	7. Identify specific risks posed by exposure of card data		
	8. Identify actions to mitigate risks		

Guidelines for Assessing Risk of Adding Data Elements to the Smart Card – Part 3			
Factor		**Vulnerabilities /Actions**	**Comments**
D. Compliance with Privacy Requirements			
	1. Identify applicable System Notices (# & title)		
	2. Identify applicable privacy requirements waivers		
	3. Identify all new or existing data card data elements that will be accessed but are excluded from the privacy analysis		
	4. Identify new data elements that will be collected specifically for the card, the purpose, and how the data will be backed up and transferred to new cards		
	5. Identify new card data elements that mirror official data stored in central databases, explain how card is kept current, and describe cardholder's courses of action to resolve inconsistencies		
	6. Identify any special privacy risks posed by adding new data to the card and exposing it through applications used to access the data		
	7. Identify any special actions needed to reduce privacy risks		
	8. Identify any actions needed to align System Notices with proposed system changes		

APPENDIX G Configuration Management Stakeholders

End of Document