Contactless Fare Media System Standard

Part IV – Security Planning and Implementation Guidelines and Best Practices

(APTA IT-UTFS-S-004-06)

Version 1.0
October 8, 2006

Note: Document renumbered March 2013, previously referenced as APTA G-UTFS-WP3-001-06. No content was changed.

Prepared by the Work Package – 3 Group of the Financial Management Committee of the American Public Transportation Association (APTA) Universal Transit Fare System (UTFS) Task Force

The APTA Rail Standards Policy and Planning Committee approved this guideline for release on October 8, 2006.

American Public Transportation Association
1666 K Street, NW
Washington, DC 20006-1215, USA

Abstract: This standard provides the basic steps and considerations that should be employed in order to define, implement, and manage a security program for a regional smart card-based fare collection system.

Keywords: fare collection, security, public transportation, transit, smart card

Introduction

(This Introduction is not part of the APTA IT-UTFS-S-004-06 Standard)

This standard is part IV (Part IV) of a suite of standards/Guidelines that together form the Contactless Fare Media System Standard (Standard). Other parts of the Standard include:

— Part I - Introduction and Overview (Part I)

— Part II – Contactless Fare Media Data Format and Interface Standard (Part II)

— Part III - Regional Central System Interface Standard (Part III)

— Part IV – Security Planning and Implementation Guidelines and Best Practices (Part IV)

— Part V - Compliance Certification and Testing Standard (Part V)

The parts of the Standard noted above are intended to be implemented as a package to complete an end-to-end integration of fare collection information processing. Detailed descriptions of all the parts of the Standard can be found in Part I - Introduction as well as within the introduction sections of each part.

The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a rail transit system's operation. In those cases, the government regulations take precedence over this Standard. APTA recognizes that for certain applications, the standards or practices or guidelines, as implemented by rail transit systems, may be either more or less restrictive than those given in this document.

The intent of this Part IV of the Standard is to provide guidelines for a consistent and uniform method of planning and implementing a security scheme for fare collection systems used in transit. By applying the Standard to the design of a new fare collection system or upgrade of an existing system, combined with adherence to a set of regional implementation needs or security and operating rules, interoperability with other compliant systems may be achieved.

In the process of providing fare collection systems, transit agencies may consider partnering with third party payment systems. These third party systems may have security schemes or business rules, processes and technical approaches that will impact transit Automatic Fare Collection (AFC) system design or operation. Since Part IV of the Standard is a guideline, and so does not specify a particular security scheme, this is an issue transit AFC programs may need to consider when planning or selecting an AFC security scheme.

Document Development Process

Development of this Guideline and its parts was guided by the APTA Universal Transit Fare System (UTFS) Task Force and its bylaws. It is the mission of the Task Force to develop a series of documents that provides industry guidance for the creation of an open architecture payment environment that promotes greater access and convenience to the public transportation network and enables integration of independent payment systems. To accomplish this mission, the Task Force membership established a broad representation of the transit industry specifically including transit system operators, the Federal Transit Administration (FTA), manufacturers, engineering and consulting firms, transit labor organizations and others with an interest in the revenue management aspects of the transit industry.

To be effective and responsive to transit industry needs, the Task Force in its effort to develop fare collection standards relies on the following guiding principles:

- Promote economies of scale for agencies and enable more competitive procurements,
- Provide a platform to support agency independence and vendor neutrality,
- Strive for an open architecture environment for hardware and software utilizing commercially available products,
- Foster development for a multi-modal and multi-application environment and
- Provide information for informed decisions and development of partnership strategies.

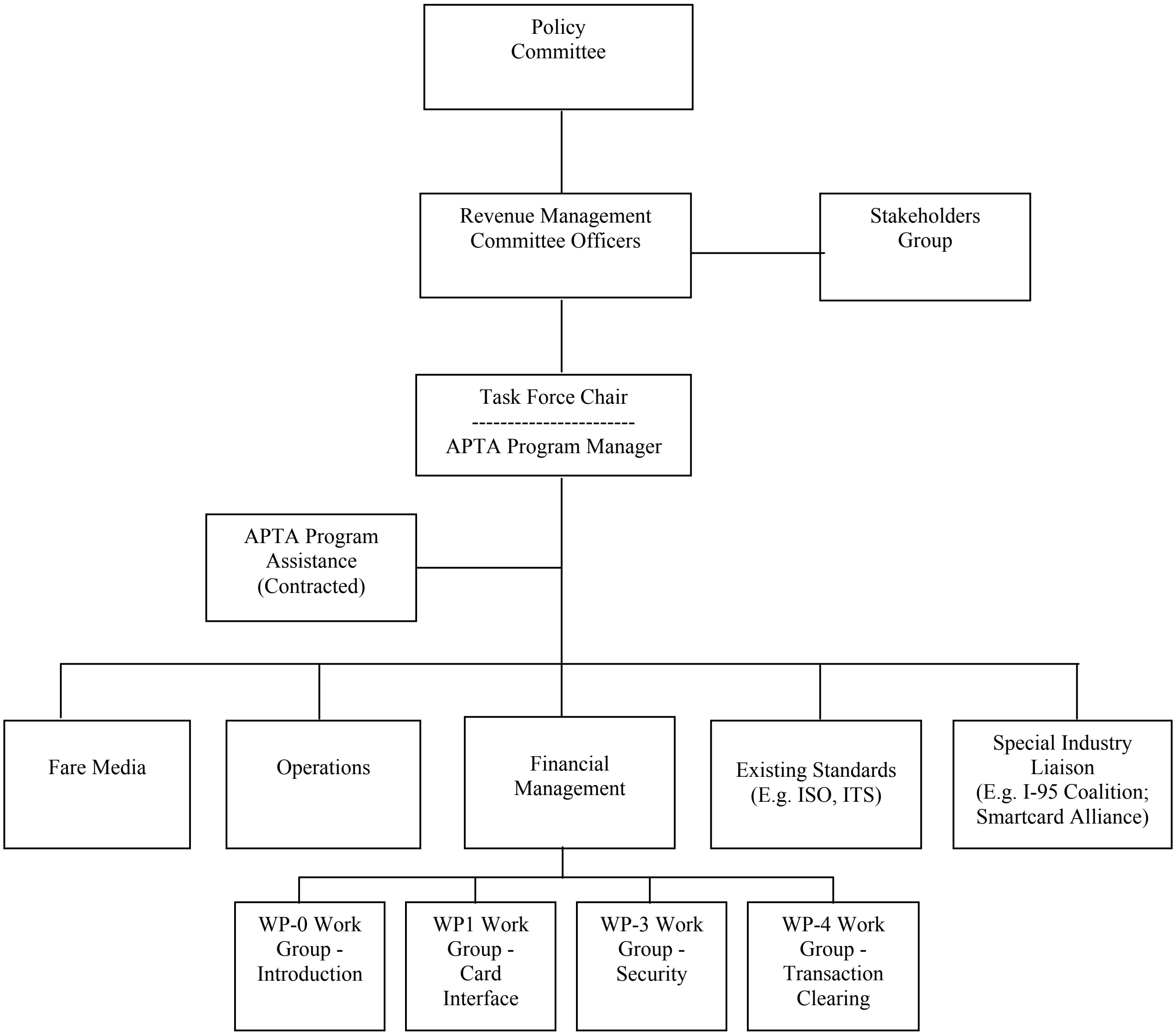
Applying these guidelines and relying on a broadly consensus driven decision process has produced these important industry-based standards.

To be successful, any consensus process involving organizations with diverse interests must have rules defining the procedures to be used. APTA developed a set of bylaws the APTA UTFS Bylaws (Bylaws) as revised September 1, 2005 to govern the process. These bylaws contain the following basic principles:

- Membership open and broadly representative of industry
- Open process and open meetings
- Consensus based (defined as 75% super-majority)
- Mandatory minimum public comment period
- Response required to all reasonable comments received
- Final approval voting based on one vote per organization
- Maximum use of electronic communication
- The policy committee retains implementation authority

The bylaws and resulting process APTA used to develop these standards followed the process required by the American National Standards Institute (ANSI) to obtain ANSI Standards Development Organization (SDO) certification.

The specific approach of the Task Force for standard development is based on a consensus driven process broadly representing all the major revenue management industry groups and stakeholders. Figure (*i*) is an organizational diagram depicting the relationships that have been established to develop, to approve and to implement revenue management standards, recommended practices and guidelines.


Policy Committee
Revenue Management Committee Officers
Stakeholders Group
Task Force Chair

APTA Program Manager
APTA Program Assistance (Contracted)
Fare Media
Operations
Financial Management
Existing Standards (E.g. ISO, ITS)
Special Industry Liaison (E.g. I-95 Coalition; Smartcard Alliance)
WP-0 Work Group - Introduction
WP1 Work Group - Card Interface
WP-3 Work Group - Security
WP-4 Work Group - Transaction Clearing

Figure (*i*)Universal Transit Fare System Standards Organization

The broad policies followed by the Task Force are set by the Rail Standards Policy and Planning Committee (Policy Committee) with oversight by the APTA Standards Development and Oversight Council (SDOC). APTA ensures that the policies set by the Policy Committee are followed. The officers of the Revenue Management Committee assist APTA staff in the implementation of policies set by the Policy Committee. The Task Force is organized into committees based on the priorities set by the stakeholders group and Revenue Management Committee officers and approved by the Policy Committee. Task Force committees develop individual work plans and schedules. Task Force committees may divide into sub-committees or working groups of subject matter experts to develop initial drafts of individual standards or recommended practices.

Given the consensus driven decision process of the Task Force, voting and balloting on release of this document for consideration by the APTA Rail Standards Policy and Planning Committee was approved using the following conditions:

- A quorum of at least sixty percent (60%) of the total Task Force voting members participated for a valid vote to take place.
- Approval of this document required a super majority of 75% of the voting members that cast ballots (do not abstain) to vote in the affirmative for the Task Force to approve this document for release.

The document approval process necessary for release of an APTA standard follows the flowchart depicted in Figure (*ii*) as documented in the APTA UTFS Bylaws (Bylaws) as revised September 1, 2005 maintained and controlled by APTA. The Bylaws also provide policies on Task Force and committee organizational structure and document balloting requirements as noted above.

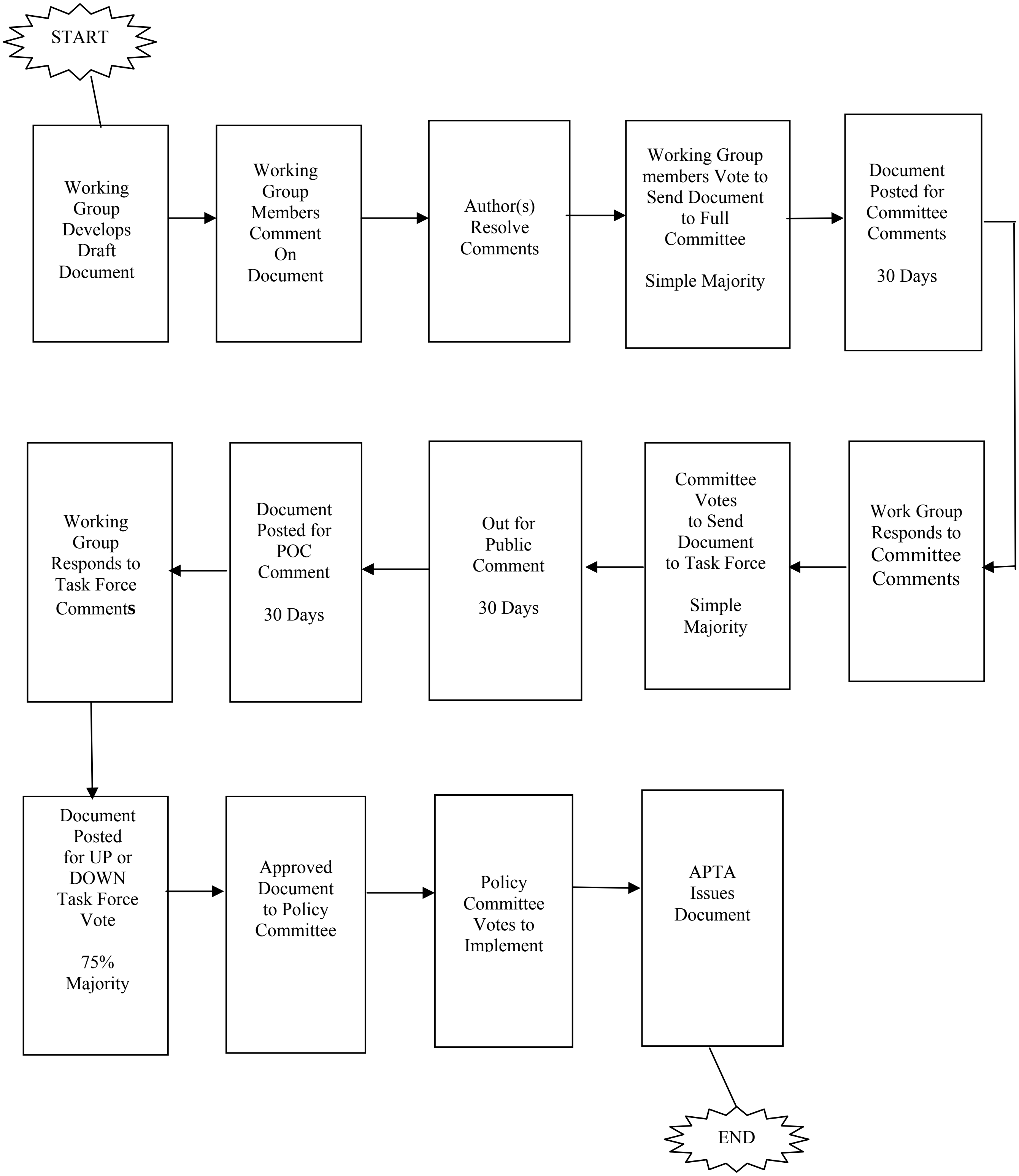

START
Working Group Develops Draft Document
Working Group Members Comment On Document
Author(s) Resolve Comments
Working Group members Vote to Send Document to Full Committee
Simple Majority
Document Posted for Committee Comments
30 Days
Work Group Responds to Committee Comments
Committee Votes to Send Document to Task Force
Simple Majority
Out for Public Comment
30 Days
Document Posted for POC Comment
30 Days
Working Group Responds to Task Force Comments
Document Posted for UP or DOWN Task Force Vote
75% Majority
Approved Document to Policy Committee
Policy Committee Votes to Implement
APTA Issues Document
END

Figure (*ii*)Document Comment and Approval Process

Intellectual Property Provisions

To protect those offering technology during development of the Standard or Guideline and to protect those using the Standard or Guideline from copyright and patent infringements, the UTFS Task Force has implemented an Intellectual Property Policy. The inclusion of intellectual property provisions addressing patents, copyrights or trademarks is in accordance with APTA's Universal Transit Farecard Standards Intellectual Property Policy and Procedures, issued September 1, 2005, and enforced beginning October 17, 2005. The terms of this IP Policy are subject to the Universal Transit Farecard Standards Task Force Bylaws and in accordance with APTA Scope document, "APTA Universal Transit Farecard Standard Work Scope Specification, ATPA UTFS-D-TC-01A-05." All other documents, besides the Bylaws, concerning UTFS IP policies and procedures are controlled by this IP Policy, and other documents shall have no effect on the interpretation of the IP Policy.

Under this policy all participants in the APTA UTFS program including but not limited to transit agencies, fare collection system suppliers, financial institutions, consultants and other third party application providers shall submit a Letter of Acknowledgement, which states that, on behalf of the Organization with which they are affiliated and/or themselves, they have received and reviewed the IP Policy, and acknowledge that their participation in the UTFS standards development process, and the standard(s) adopted in the course of this process, will be subject to the IP Policy. Under this policy contributors are required to make known any patents, copyright material or other intellectual property that may be contained within the standard or essential to the standard. If contributors have intellectual property such as patents or copyright material contained within the standard/guideline, the IP Policy requires submission of a Letter of Assurance stating the terms and conditions for use of such intellectual property.

APTA further issues a call-for-patents during its public comment period prior to release of the Standard or Guideline.

Further, federal antitrust laws prohibit contracts, combinations and conspiracies in restraint of trade. Sanctions for violating the antitrust laws include civil damages (including treble damages) and criminal fines and imprisonment. The Policy of the American Public Transportation Association and the Task Force is to strictly adhere to the antitrust laws.

Standards vs. Guidelines/Recommended Practices

APTA develops standards and recommended practices/guidelines, and such distinction between these document types needs to be clear.

Characteristics of a Standard

A standard should be developed when the document:

a) Covers a system, component, process or task that is safety critical, or

b) Ensures interoperability between parts or equipment, or

c) Standardizes a design or process, or

d) Addresses an FRA or NISB concern, or

e) May become part of a regulation.

Characteristics of a Guideline/Recommended Practice

A recommended practice/guideline should be developed when:

a) The document describes only one of several acceptable approaches, or

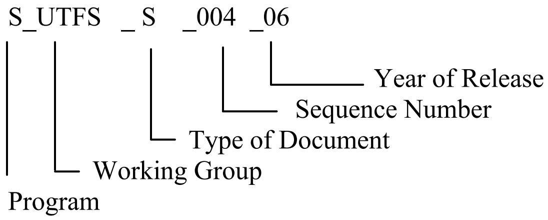
b) The document is tutorial in nature, or

c) The document does not meet one of the characteristics for a standard, or

d) Consensus could not be reached that the document should be a standard.

Document Numbering Nomenclature

Document numbering is composed of five parts. The first part designates the standard program the document falls under, in this case IT or Information Technology. The second part designates the working group or application where the standard was developed; which for this Standard is UTFS. The third part designates the type of document. A prefix "S" represents a general standard while recommended practices carry the prefix "RP" and Guidelines carry the prefix "GL." Finally, the last two sections attribute a document sequence number and the year the document was first released, respectively.



Document Maintenance & Requests for Revisions

APTA will review and update this document on an as needed basis, but at a minimum will review once every two years. The UTFS Task Force has responsibility for conducting reviews, addressing requests or suggestions for document revision or expansion and for implementing changes or revisions.

Requests for revisions of APTA standards and recommended practices/guidelines are welcomed from any interested party. Suggestions for changes to documents should be submitted in the form of a proposed change to the text along with the appropriate supporting documentation / rationale for the change.

Occasionally, questions may arise concerning the meaning of portions of these standards/guidelines as they are specifically applied. APTA will clarify such issues as necessary through the UTFS Task Force and the Rail Standards Policy and Planning Committee. Address comments, questions on interpretation or requests for changes to:

UTFS Staff Advisor
American Public Transportation Association
1666 K St., NW, 11th Floor
Washington, DC 20006

To obtain copies of this standard contact:

Information Center
American Public Transportation Association
1666 K St., NW
Washington, DC 20006

Patents

Attention is called to the possibility that implementation of this guideline may require use of subject matter covered by patent rights. By publication of this guideline, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The APTA shall not be responsible for identifying patents or patent applications for which a license may be required to implement an APTA standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

The American Public Transportation Association (APTA) greatly appreciates the contributions of Thomas Parker, Chair of UTFS Task Force and the following individuals who provided the primary effort in the drafting of this Guideline.

At the time this guideline was completed, the WP-3 (Security) Working Group had the following membership:

Gary Yamamura, *Chair*
Work Package – 3

Rick Barrett, chair FMC
Lisa Bucci
David deKozan
Henk Dennenberg
Syed Hakim
Norman Kort
Paul Legacki
Roger Merkling
Brian Monk
Gerard Najman
Ola Nowlin
Darshana Patel
Alexander Pi
Joe Pilozzi
Denis Ratier
Chris Sheeks
Chung-Chung Tam, past chair FMC
Curtis Watson
Tim Weisenberger*

Martin P. Schroeder, P.E.*,
APTA Staff Advisor for UTFS
Sr. Manager for APTA Rail Programs

* Non-voting member

Organizations contributing to the development of this Guideline included:

Quattran Associates
Scheidt & Bachmann
Philips
ERG
Cubic Transportation Systems
Infineon
Verifax Consulting, Inc.
Thales Transportation Services
Chicago Transit Authority
Philips
Aegis Technologies
Texas Instruments
Volpe National Transportation Systems Center
Three Point Consulting

APTA acknowledges the generous support of Robert Bernard and the Port Authority of New York and New Jersey for development of the Regional Interoperable Standard for Electronic Transit Fare Payments (RIS$^{©}$) on which this APTA standard has been based. APTA also acknowledges the U.S. Federal Transit Administration and the ITS Joint Program Office of the U.S. Department of Transportation for their support and guidance of this program.

CONTENTS

PART IV – Security Planning and Implementation Guidelines and Best Practices v.1.0

1. Overview

The security of an automated fare collection (AFC) system is a common concern for all transit system operators, since it entails the protection of all of the assets of the system including its passengers, transit personnel and the cash-like funds which are generated and collected by the system. Accordingly, the security mechanism employed by the system operator must be comprehensive in its nature, providing assurance that even the weakest point of that mechanism is sufficient to address the needs of all of the assets it is designed to protect. While a security program must consider and provide for the protection of all of a transit agency's valuable assets, this document addresses only the critical areas of concern for the security planning associated with the smart card-based components of AFC systems and provides recommendations and best practice guidelines for implementation of such a plan in any small, medium or large regional fare collection program. Although the descriptions provided in this document focus exclusively on the smart card elements of a regional system, some attributes of security planning techniques included herein will naturally apply to other types of fare media and/or components/systems that are not directly related to the smart card program and/or are part of an individual agency system.

This document is not intended to be a specification or to establish standards for security. Rather, it provides the reader with understanding of the terminology associated with security programs for fare collection systems and highlights the basic steps and considerations that should be employed in order to define, implement, and manage a security program for a regional smart card-based fare collection system. In order to ensure that this document addresses the needs of agencies and regional programs of all types and sizes, it has been written using relatively non-technical language and the specific guidelines are targeted toward achievement of a moderate level of security. Individual agencies and/or regional programs with mature systems and/or desiring a more advanced level of security protection may benefit from this document, but should also consider seeking the consultative assistance of transit industry security experts.

NOTE 1—In order to ensure interoperability between disparate systems within a single regional fare payments program, the owners/operators of those systems must define, implement, and adhere to a comprehensive set of business rules. Among those rules must be a security plan, which defines a minimum acceptable level of security that each component of every system must achieve. Additionally, the regional security planning rules must also prescribe the specific methodologies that will be employed by each agency in regards to such things as message authentication tools (e.g., which algorithm will be utilized by all parties), encryption/security key management (e.g., which entity will manage the master key set, what key set(s) will be received and stored by each agency) and data storage (e.g., what data elements must be encrypted, what elements must be stored centrally). As such, this document is intended to be used as an aid for the business/security rules development process, serving as a resource to identify and qualify the many security options which are available and necessary to protect the smart card related assets of a regional program.

NOTE 2—This document leaves the responsibility of developing a specification (for an interoperable security plan) to the participants of a regional program.

NOTE 3—Throughout this document, where a specific element of security requires a particular approach in order to attain an acceptable level of security, a strong recommendation has been provided. These recommendations have been placed in a text box which is highlighted in bright yellow.

2. System Security Overview and Architecture

2.1 General Overview

The security of an AFC system requires a comprehensive approach that recognizes and addresses all aspects of the AFC system from a security perspective. Thorough security planning must recognize the strengths and weaknesses of the design and ensure that the weakest points in that design do not compromise the protection of assets within the system. Accordingly, security planning must begin with a holistic view of the system, the assets that will require protection, and a general architecture that can be used as a skeleton upon which specific components of the security design can be applied.

2.2 What is Security?

For the purposes of this document, security is defined as the means used to minimize the vulnerability of assets to internal and external attacks for the purposes of exploiting that asset or the information it contains. For a fare collection system, assets generally come in the form of money and data, although assets may also include the hardware components (i.e., Proximity Integrated Circuit Cards - PICCs, Card Interface Devices - CIDs, load terminals, etc.) in which the data is stored and/or processed.

2.3 AFC System Components

Figure 1 is intended to identify the core assets that are common to all smart card-based AFC systems and that require some form of security protection. These assets generally include the following:

— *Cash*: Currency and coin of all denominations received from a passenger for payment of fares or made available within the system to provide change to passengers. (Not pictured in Figure 1).

— *Bankcard Payments*: Purchases of fare products or payment of fares by passengers using a credit card or debit card as a substitute for cash or other forms of payment.

— *Other Payments*: All other non-cash, non-bankcard forms of payments used by passengers or other entities to purchase fare products or to pay fares within the system. Examples include checks, Transit Checks, tokens, vouchers, electronic debits, and electronic stored value payments, etc.

— *Fare Transactions*: All types of fare product purchases and fare payments conducted within an AFC system.

— *Fare Media*: The PICC used to facilitate fare payment within an AFC system.

— *Fare Products*: The mechanisms for fare payment stored in electronic form within the PICC. These include stored value purse(s), time-based passes, and stored rides.

— *Reload Transactions*: The process and electronic record of adding a fare product to the PICC.

- *Field Equipment*: The vending machines, inquiry kiosks, fare gates, fare boxes, station/depot computers, communication tools, and other devices used to facilitate automated fare collection within a transit vehicle, depot or station.
- *Central System*: The computing equipment, services and other devices used by the transit authority to provide a common collection point and database for all fare and reload transactions and information generated and stored by the AFC system.
- *Regional System*: The computing equipment, services and other devices used by a regional body to provide a common collection point and database for all fare and reload transactions and information generated by the AFC systems within the region. Such assets also include any and all equipment and personnel related to regional clearinghouse activities such as a regional call center, centralized card initialization and distribution facility, etc.
- *Communications Infrastructure*: Hardware and communications services used within and between individual AFC systems and the regional system to transfer data.
- *Passengers*: The individuals that utilize the transit system and pay fares.
- *Personnel*: The employees and contractors of the transit authority that provide support to the AFC system.
- Off-Premise Assets
  - Card dispensing machines
  - Web sites
  - Third party automated teller machines and other load devices and kiosks
  - Outsource service providers
  - Transit authority owned but third party operated load devices
  - Cardholder controlled devices (i.e., Personal card readers, etc.)

Figure 1 also illustrates the manner in which security of the various components of a regional fare collection system have been addressed by this document.

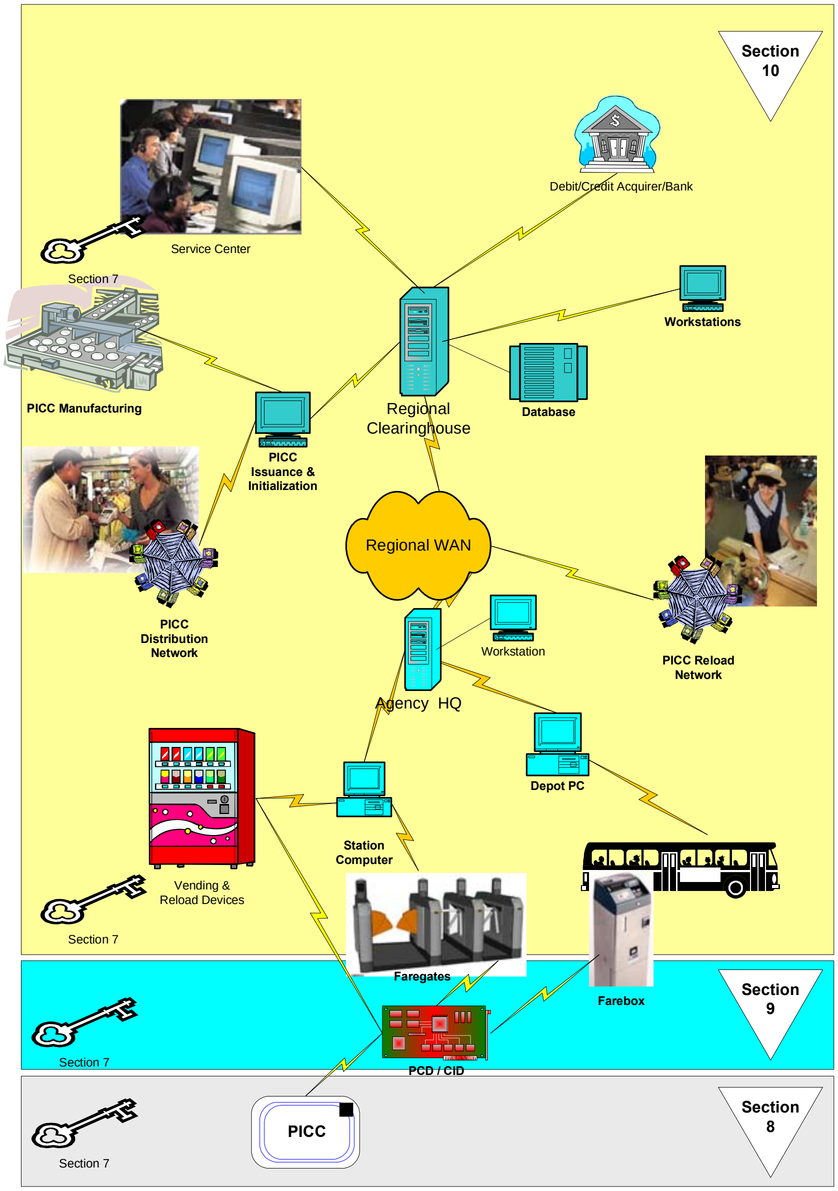


Figure 1—Regional AFC System Security Components

2.4 The Philosophy of Smart Card-Based AFC System Security

Prior to the introduction of smart cards as a primary media for fare payment, AFC systems were developed to support automated processing of bills, coins and tokens as well as more advanced mediums such as magnetically encoded tickets. As transit agencies in North America transition to regionalized fare payment programs – a nearly universal process occurring throughout the continent – the introduction of smart cards and more sophisticated AFC systems has become a requirement and, in parallel, the importance of system security has increased substantially. Where in the past security needs were primarily centered on protection of coin and currency, the advent of smart card-based systems reduces the use and security concerns associated with cash and, instead, refocus concerns around three other areas

- Fare evasion
- Physical attacks on equipment and networks
- Virtual attacks on cards, systems and communications

Although the need for more traditional security (i.e., for cash, the safety of patrons and employees, etc.) still exists, the establishment of a comprehensive security program requires a broader commitment to security and an understanding of these new areas of concern that are specific to smart card-based systems. Accordingly, this document spotlights only those new areas and assumes that a general security plan is already in place to address all other security requirements.

2.5 Common Security Terms and Phrases

Development of a comprehensive security program requires an understanding and use of numerous terms and phrases that are somewhat unique to the security domain. Following is a list of a few of the most commonly used terms/phrases. Additional terms/phrases that are specific to the security methodologies associated with protection of specific AFC system components are provided in the latter sections of this document.

Access control: Protection against unauthorized operations on information or processes in the system.

Authorization: A process giving individuals access to system objects based on their identity.

Authentication: A process of proving the identity of a document, a message, a data element, a computer, or a computer user.

Confidentiality: The act of preventing the disclosure of secret information to non-authenticated individuals, parties and/or processes.

Eavesdropping: Act of illegally listening in on a communication between two other parties, systems or system components.

Integrity: Condition existing when data is unchanged and remains in the original state defined or created at its source.

Non-repudiation: Condition wherein the integrity of data can be confirmed and, therefore, its validity cannot be challenged.

Privacy: The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed.

2.6 Security Techniques

As a general rule, security of system assets is applied using variations of four distinct methodologies. These methodologies are

- *Authentication*: A process whereby one system component can verify the identity of another and whereby a recipient of data can confirm that it has not been altered since leaving its source.
- *Encryption*: A process used to change the appearance of data so that it cannot be easily used or understood by someone other than the intended recipient.

- *Access Restriction*: Physical (e.g., doors, locks) and electronic barriers that prevent an unauthorized person or system from viewing, using, adding, removing or otherwise changing information or a physical component.
- *Detection*: Establishment of alarms and auditing practices to determine that a breach of security has occurred (or is occurring) in order to instigate mitigating action on the part of the system owner.

Specific techniques for applying these methodologies to the security of distinct system components will be addressed in the section of this document associated with the component(s).

3. Security System Planning Guidelines and Checklist

3.1 Security Planning Basics

3.1.1 Introduction - Prevalence and Consequences of Security Breaches

The 2003 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, reported the following results from a small survey of 530 large corporations and government agencies:

- 92% of respondents had detected computer security breaches within the last 12 months.
- 75% of those acknowledged financial losses due to computer breaches.
- 47% (251 respondents) quantified their financial losses: a total of $201,797,340 – with the most serious financial losses occurring through theft of proprietary information or denial of service.
- 78% identified their Internet connection as the most frequent point of attack while 22% identified their internal systems.
- Only 30% reported intrusions to law enforcement agencies; most did not to avoid potential risks of negative publicity and competitors using the information to their advantage.

These trends clearly demonstrate the need for all companies to be increasingly vigilant to protect their mission-critical networks from the growing numbers of methods that are being used to exploit vulnerabilities in those networks and the systems they support. This section provides an introduction to the concepts of security and will aid the reader by establishing an understanding of the need for security, the most basic forms of security attacks ("threats") and the process of planning, implementing and maintaining a strong security plan.

3.1.2 Security Planning 101

Security Planning is the development and execution of processes for an organization to physically and logically protect its information and information systems. Information security is a paramount concern to every organization that stores and exchanges sensitive data digitally since that data must travel over some form of network and every aspect of that network may be vulnerable to attack if not properly protected. Data in storage or data that is being passed from one user to another is susceptible to various forms of attacks as well as random events that cause alterations or loss of information and thereby reduce or eliminate the value of its information. In order to ensure that data is secure, security planning must define mechanisms to

— Protect the integrity of the data,

— Guard the confidentiality of the data,

— Validate the authenticity of the data, and

— Confirm that the entities sending and receiving the data are authorized to do so.

Over the past several decades, information and information systems have become increasingly important and highly valued assets. Accurate, reliable information has always been the basis used to make strategic decisions, perform financial settlements and to assist customers. Recent advances in technology, such as the advent of the Internet, have improved access to information and the systems which store it. In parallel, individuals and groups that seek to gain notoriety, revenge or financial gain have exploited such technologies to illegally gain access to those systems in order to obtain or alter the data within them. Today, more so than anytime in the past, consumers, legislators, businesses, and the news media recognize both, the immense value and the inherent risks associated with the use of modern information delivery systems. Accordingly, an organization's management has a fiduciary duty to preserve, improve (the accuracy and reliability of), and safeguard information and information systems. This means that management must take appropriate steps to ensure that proper measures are in place to protect information assets from a wide variety of threats including: error, fraud, embezzlement, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster. Likewise, management must also fulfill its fiduciary responsibilities by ensuring that each measure is designed in a manner commensurate with the sensitivity, value, and criticality of the assets it protects and each measure is monitored to verify that it is properly and consistently executed. Strong security, therefore, requires careful planning, careful implementation and continuous validation and must be employed for information stored on hard copy or electronic media, the systems which process it (microcomputers, firewalls, voice mail systems), and for each component of the network by which it is moved (e.g., Internet, electronic mail or facsimile).

Data protection not only includes extensive measures to secure the information against compromise but also requires a plan of action in the event a security breach occurs. For any organization to quickly and effectively respond to a security incident, a well-designed security plan must be drafted and implemented across that organization. Furthermore, for that security plan to properly ensure and protect information and assets, information security requires the participation of and support from each person and organization with access to the data. Employees (both permanent staff and temporary workers), consultants, contractors, and supplier personnel must be provided with sufficient training and supporting reference materials to allow them to properly protect company information assets.

3.2 Common Threats to a Smart Card-Based Fare Collection System

3.2.1 General

As technology advances and becomes an increasingly important component of the business process, the number of threats to that technology and the potential damage that a security breach can wreak on an organization increases proportionately. A security plan must be written to address all potential threats and enact necessary measures to respond to security breaches, as well as providing the flexibility to maintain high security standards as new threats emerge. By the same token, security plans must recognize the ultimate cost of implementation as a comparison to the cost or risk to the organization if the security threat is realized. Logically, the security plan must be scaled according to the value of the systems and information it is designed to protect and the budget and resources available for such protection. Identification of potential threats and their impact are early components of the security planning process and essential to the long-term viability of the security program. Common threats that exist today for smart card-based fare collection systems include, but are not limited to the following:

3.2.2 Social Engineering

It is often believed that years are spent by hackers or disgruntled employees trying to "crack" a password using a method known as brute force, a process in which passwords are systematically and continuously offered to a system until a real password is revealed. In reality, the hacker often has to simply persuade someone to disclose his or her password. This form of attack is known as "social engineering" and, because of its simplicity, claims more than its fair share of victims. The hacker makes an attempt to trick the user into revealing their password or executing a task that allows the hacker to observe or monitor and record the use of the password.

One relatively new approach to social engineering that has arisen with the popularity of the Internet is called "phishing." With this method, the hacker sends an official-looking e-mail message to the victim and indicates in the message that it has been distributed from a well-known company. The message informs the recipient that a security check is being conducted and the recipient must respond with their user name and password in order to avoid losing their privileges to use the company's website or services. In some cases, the victim is provided with a link to a website that has been constructed to appear very much like the legitimate web pages of the company but, in fact, is simply a front for a system designed to collect the private information of the victim.

3.2.3 Logical Attacks

In most types of smart cards, sensitive data is stored in a type of electronic storage known as the electrically erasable programmable read only memory or "EEPROM." Since the procedure for reading and writing information in EEPROM can be affected by unusual voltages and temperatures, hackers can, in theory, derive sensitive information (such as stored passwords) from the smart card by raising or dropping the temperature and/or voltage used to provide power for the smart card reader during the time it is interacting with the smart card and observing the changes in the results. This form of attack is commonly referred to as a "simple power analysis." Other forms of logical attacks include the use of software viruses (software applications designed to disrupt or disable another system or application), keystroke monitors (software applications that record each action performed on a user's keyboard), network sniffers (the computer network version of a wiretap), etc.

3.2.4 Password Attacks

One of the most common security breaches is a compromised password. Many users do not understand requirements for choosing a password and maintaining its secrecy. Some select passwords that are easily guessed (e.g., "password", "1234") or leave a written copy of their password where it can be easily found. When this information falls into the wrong hands, all of the rightful user's privileges go along with it.

3.2.5 Physical Attacks

Invasive physical attacks are attempts to steal a device in which information is stored, gain entry to a secured area/device, or to peel away layers of the computer chip's silicon within a smart card in order to access its memory stores. This form of attack requires an advance knowledge of chip circuitry since it involves the physical deconstruction of the outer portions to enable the attacker to probe the stored data through direct contact.

3.3 Common Causes of Security Breaches

Security breaches may arise from any number of different sources; however, most can usually be attributed to a small number of recurring problems. Most internal security breaches, which comprise the majority of security-related issues, result from careless or negligent application of security policies and can be linked to a lack of internal awareness of the importance of security. Most external breaches are the result of some form of social or logical attacks where the infiltration is the result of a random act of hacking or a specifically targeted attack on an organization. All of these problems can be overcome through implementation of a thorough security plan, which includes ongoing monitoring as well as training and follow-up to establish an increased sense of security awareness.

The following paragraphs provide additional descriptions for the most common causes of security breaches:

- Poor password selection:

  Many security systems today require the user to input a password or code in order to gain access. Since various personal and business passwords are often required each day, users often select simple, easy to remember numbers such as 1-2-3-4 or 1-1-1-1. These types of passwords/codes are equally easy for a hacker to guess.

- Lack of password selection and update policies and enforcement:

  Although most security systems can accommodate passwords that contain both numbers and letters, many are not supported by security policies or systematic verifications that require passwords to be non-sequential, mixed alphanumeric values. Additionally, many systems do not require the user to periodically change their password, increasing the likelihood over time that the password can be observed by a would-be hacker or compromised in some other form.

- Unsecured password storage:

  Users of even the most sophisticated security programs are often guilty of causing a security breach because they leave a written copy of their password on their desk, computer monitor, or some other unsecured area.

- Password sharing:

  One of the most frequent causes of security problems stems from the sharing of passwords. As an example, an employee calling in from home needs a vital piece of information from their computer and asks their co-worker to log-in by using the employee’s password to access their files. This practice, while expedient, opens the door to the system and creates untold opportunity for immediate and future breaches of security.

- Unsecured remote access:

  Many companies recognize that their workforce can be more efficient if it can access information systems while away from the office. Decisions are often made haphazardly to provide that access, without consideration to the security consequences associated with it and, accordingly, without adequate security protection. One form of attack that is designed to exploit this vulnerability is to randomly dial numbers within the same area code and prefix of a large company’s main phone number. If the hacker can successfully reach a modem (a device that enables computers to connect over a telephone or cable line), he can then attempt to connect and interact with the company's systems.

— Unsecured Ports:

Most computing and communications hardware devices offer a number of physical and virtual access points (“ports”) that can be used to provide an interface to or from an external system. In some cases, security programs only provide protection for the regularly used ports, leaving the unused ports vulnerable to a skilled hacker.

— Viruses and worms:

One of the most publicly visible security breaches comes in the form of a software program designed specifically to infiltrate and attack a system or application. These programs, known as computer viruses or worms, can be delivered in a variety of different ways but are most frequently delivered through e-mail. The virus or worm is sent as an attachment to e-mail to an unsuspecting individual, often disguised in a way to makes it appear to be sent by someone known to the recipient or as a solicitation for a fictitious product or service. When the attachment is opened, the software program is loaded into the individual’s computer, deleting or changing files, issuing unauthorized commands, modifying configuration and/or operating system settings and often taking over the e-mail application within the computer to distribute new copies of the program to everyone on the individual’s e-mail mailing list. This form of security breach can have the most widespread impact to an organization since e-mail is increasingly becoming the most common and frequently used form of internal communications. Not only can each computer suffer from the virus’ intended damage but also the organization’s e-mail network can be compromised as thousands of copies of the virus are created and distributed via e-mail over a short period of time. In some situations, the virus may initially direct itself toward a system’s virus protection software, causing that application to shut itself down, leaving the computer/system more vulnerable to the other effects of the virus.

3.4 Planning Process

3.4.1 Security Plan Basics

If systems and data are to be adequately protected against security threats, organizations and operators must consider security as a senior management concern requiring a serious investment of time, money, and human resources. A security plan will be most effective if it is coordinated among all departments and/or individuals that interact with the systems that require protection. Such coordination can be a challenge for any organization, thus long-term institutional commitment and top-down executive sponsorship is essential. Security plans must provide coverage for all aspects of the organizations information technology including, among others, proper collection and storage of vital information/data, cataloging or processing of that information, information exchange workflows, systems maintenance plans and schedules, staff training and permissions, and business continuation/resumption following a serious security breach, system outage or disaster.

3.4.2 Basic Steps

a) PREPARE

Set the stage for security planning. Establish a balance since both the lack of a plan and over-planning can be problematic. Adequate time and resources should be allocated to the planning effort and specific objectives and schedules for completion should be defined early in the planning process.

b) FORM SECURITY TEAM

Appoint a security manager to develop and implement your security plan and utilize the security planning group to support the security planning process. Security planning, plan implementation and ongoing plan management is a long-term responsibility. Identifying a specific individual to be responsible for the process will solidify the importance of security with the staff and will help to ensure continuity throughout the planning and implementation processes. Form a security planning group with representatives from key departments to help define, develop and implement the security plan.

c) DEFINE POLICY

Utilize the security team to define and document security policies and procedures. These policies should be consistent with the overall objectives established in the Prepare step and should establish a minimum acceptable level of security for the entire system. Always ensure that the policy is endorsed at the highest management levels.

d) PERFORM SECURITY ANALYSIS

Perform a security impact analysis to assess system weaknesses and determine the impact if a breach occurs. Understand your exposure and quantify the impacts to your organization. Apply the 80/20 rule – that is, use your security resources to identify and implement protection for the risk that represent the majority (80%) of your impacts. The remainder (20%) will, in general, represent too small of an impact to warrant extraordinary attention or protective measures within your security plan or will require the use of resources that will ultimately cost more than the assets they are protecting. Keep in mind that a security plan is only as strong as its weakest point and, therefore, the weakest point determines the level of security protecting the entire system.

e) IMPLEMENT PREVENTATIVE MEASURES

- Eliminate obvious weaknesses to ensure the security of the facilities that house your information systems.
- Install appropriate physical and logical security systems.
- Ensure that collection storage is secure and that good records are kept.
- Establish and distribute staff regulations for security.

f) DOCUMENT SECURITY RESPONSE PLAN

Identify potential security-related emergencies and plan your response to any breach of security. Document procedures for staff, provide training, practice response plans, and coordinate plans with other departments such as public relations or executive management as well as outside officials such as security firms and law enforcement.

g) MAINTAIN AND MONITOR

Establish a schedule for ongoing monitoring of security policies and program components as well as periodic review and update of your security plan. Build organizational consensus and continue to sell security within your organization. Security is value, not overhead. It is also critical that the monitoring functions include methods to enforce policies when violations are identified. One example of such enforcement might include integration of security policy adherence within individual and department performance goals. In all cases, however, enforcement techniques should be tempered with the potential risk to the system/organization that is created by a lack of adherence to policy.

3.5 Key Components & Considerations

3.5.1 Evaluating the Risk of a Security Breach

Critical to defining and following security policies and procedures outlined in the security plan, an impact analysis must be performed to evaluate the effects of a security breach on your business, so that you can identify the areas of greatest vulnerability. A security breach has several dimensions when it comes to assessing its impact on your business. That is, it's not simply a matter of determining the raw value of information and then predicting how much money you will lose when it's rendered inaccessible, stolen, or destroyed by a hack attack. Consider, for example, that systems offering an opportunity for bad press in a public forum are also very attractive to hackers. Therefore, when evaluating the technical and business impact of a security compromise, you need to consider the following four important exposure parameters:

- Relative value of the information or infrastructure component

  For example, security plans, accounting systems (especially information used for financial settlement), smart card transaction information, customer data, and so forth typically have a high value, while a company newsletter has a lower value.

- Degree of public exposure

  A defaced Web site, for example, means, at a minimum, embarrassment to a company. This can translate to loss of consumer confidence in an organization's products and services.

- Denial-of-business potential

  Will an attack affect your ability to do business? Its one thing to be inconvenienced, quite another if your ability to operate your business is entirely halted. Will a short or long-term loss of a system or system component negatively impact the safety of or ability to operate the transit system or to collect fares?

- Ease of attack

  The easier a component is to attack, the more often it will be. Components closest to the public Internet, such as Web servers that receive and process information requests from customer computers, are clearly more accessible and, thus, the best and most likely initial targets. These systems also act as excellent "jumping-off points" for further attacks. Hackers compromise such systems, install their tools on them, and then launch attacks from those systems, perhaps leveraging any pre-configured trusts these systems possess, relative to other components in your infrastructure. Other areas of concern are the individual system components that are used directly by the public such as smart card readers in load terminals or faregates. What protections are needed to prevent the theft of these devices, to disable the unit or, worse, to facilitate the unauthorized loading or removal of value from smart cards?

3.5.2 Network Infrastructure, Access, and Policies:

Some standard vulnerabilities within an agency's fare collection systems infrastructure may include but are not limited to the following:

- Password command and encryption (requiring the use of passwords and/or passcodes before system or data changes can be effected)
- Security of remote administration practice and protocols used (proper control of access to the system from outside of secure agency facilities)

- Interactive access (proper control of access to change information stored in the system)
- Existence of warning banners (proper application of warning messages and flags in system that identify a potential security policy breach)
- Use of the No IP directed Broadcast and No IP source route commands
- Use of routing authentication and route filtering (establishment of specific pathways for the transfer of data from one system component to another and emplacement of "filters" in that pathway to prevent the transfer of unauthorized data or commands)
- Running of unnecessary services (proper scheduling and load management of system jobs and use of system resources)
- Service Packs/Patches (regular application of system updates and patches offered by the system developer)
- Password Policy (establishment of rules and monitoring of selection, recording, storage and changing of passwords used to access the system)
- Event Auditing (periodic review of system activities to ensure compliance with security policies)
- File And Object Access Control
- Back Doors/Trap Doors (establishment and monitoring of software policies prohibiting the use of unsecured access points in software applications)
- Viruses And Virus Protection (application and regular updating of virus protection software)
- Wiretapping (snooping and spoofing)
- Console Security (establishment of physical and logical controls over access to devices that facilitate system or data changes)
- Bypass of Controls via the operating system (OS) (establishment and monitoring of policies prohibiting access to software application commands via the operating system on which the application is developed)
- Vendor/Third Party Access (establishment and monitoring of policies properly controlling access to systems by vendors and other third party organizations that require such access to perform maintenance and repair functions and/or to perform system operations under an outsourcing contract)

3.5.3 Security Plan Compliance

As mentioned above, the security of any information system is only as good as the weakest link—typically, the end user. By increasing the security awareness of end users, an organization can make tremendous strides in increasing the overall security of its information infrastructure and meeting compliance standards and regulation. To achieve this, it is recommended to take necessary measures to not only enforce security policy, but more importantly, educate employees and users of the system about the fundamentals, objectives, and standards of the security policy.

3.5.3.1 Benefits of Security Awareness Education

- Generate company-wide awareness of the need for information security in daily activities
- Protect the system from malicious intent
- Reduce people-related errors associated with lack of knowledge

- Develop a first line of defense against threats to information assets
- Learn how to implement reasonable measures and safeguards against information security threats and vulnerabilities
- Reduce costs associated with vulnerabilities and threats to the system

3.5.3.2 Security Awareness

Awareness stimulates and motivates all individuals. The more aware your staff is of its surroundings, the more control they will have over its security. Making employees aware of the impacts of security breaches to the organization and its customers will help to ensure that security remains a serious concern. Awareness training can also be used to remind people of basic security practices such as properly selecting and securing passwords, or logging off a computer system after each use.

3.5.3.3 Awareness training means education, not just recitals of rules and procedures

Awareness must be used to reinforce the mission of the organization by protecting valuable company resources. Awareness should not be presented as simply a list of rules or procedures, but as a conduct of behavior needed to protect the agency and its critical assets. Education is the "why" of security. Informing the end-user on the risk of security breach and the potential damage that can occur is essential to gaining acceptance of a security plan. It provides information as well as insight. Awareness education should also allow participants to contribute suggestions and recommendations about improving security by end users, as well as ways to recognize and report threats and vulnerabilities and to ensure appropriate reaction when a breach occurs.

3.5.3.4 Enforcement

An agency must have tools available to enforce compliance with security policies, just as it would any other important policy. Enforcement should supplement training and awareness programs to emphasize the importance of security policy adherence and, as necessary, to provide the means to prevent gross violations.

3.6 Implementation, Validation and Updates

3.6.1 Implementation Planning

The Implementation Plan is a detailed document that establishes:

a) Definitions and personnel;

b) Objectives;

c) Assumptions and constraints;

d) Strategy and approach for implementing, managing and monitoring a security program; and

e) Corresponding security policies and procedures.

3.6.1.1 Security Program Definitions

The definitions should include a list of all participants within the security program along with their primary roles and responsibilities associated with security. For example, the system administrator is a key participant in the program and his or her responsibilities would logically include creating and administering user accounts on the system and establishing and managing a process to monitor compliance with security policies. Additionally, definitions for unfamiliar terms and phrases should also be provided.

3.6.1.2 Security Implementation Plan Objectives

The security team should establish clear objectives for the security program since all participant roles as well as planning, implementation and monitoring tasks will be defined to support and achieve these objectives. Careful consideration should, accordingly, be given to the adoption of program objectives and budget. Resource and time constraints must also be factored into this process. At a minimum, the program objectives should confirm the level of security that will ultimately be achieved either in terms of known security standards such as those documented in the Federal Information Processing Standard (FIPS) or based on a quantitative comparison to the current environment. For example, one objective may be to decrease revenue losses due to fare evasion by 10% from current levels. This subsection should create links to the day-to-day operations of the transit system and should help to cost-justify the changes that will be necessary to implement the security program.

3.6.1.3 Assumptions and Constraints

The Assumptions and Constraints subsection of the Plan documents significant assumptions that will be used to guide the development of the security plan and which may substantially affect implementation activities if those assumptions are incorrect. For example, the security team may assume that public funding is available to pay for security-related system enhancements and would, logically, develop an Implementation Plan that includes the purchase, installation and operation of new equipment and systems. If such funding is ultimately determined to be unavailable, the Plan and potentially its core objectives may need to be significantly revised. Constraints are known barriers or limitations within which the security team must operate. As a general rule, constraints should include those connected to budget (maximum available to spend on security-related enhancements and operations), schedule (deadline for implementation or target date for determining if quantitative objectives have been achieved), and resources (i.e., number, duration of time and availability of team members to actively participate). Constraints may also appear in the form of approved vendor lists, specific operating systems or programming languages, physical space available for security-related equipment/services and/or maximum fare-related transaction times.

3.6.1.4 Strategy/Approach

Once definitions, objectives, assumptions and constraints are identified, the security team should be able to formulate a strategy or approach that will be used to achieve the objectives without exceeding the known constraints. Since the strategy must define approaches for physical and logical security mechanisms across a broad spectrum of participants, systems and equipment, the strategy subsection may be quite lengthy and will almost certainly cover a wide range of topics although a great level of detail is not strictly required at this early stage. At a minimum, the strategy should clarify when and how security team members will be engaged in the effort, it should list the major changes that will be made (both to operations as well as to systems/equipment), and it should identify any objectives that are not achievable through implementation of the Plan. Implementations often include a rollout of system changes in a series of phases relative to the complexity of the changes involved, system sensitivity to change, and time to implement, etc.

Alternatively, the security manager and his or her team may feel that a single, "go live" date is achievable and preferable in order to minimize impacts on staff resources.

The strategy/approach subsection is the most comprehensive subsection and should provide sufficient detail to enable key stakeholders to understand, approve and prepare for the known impacts of Plan implementation. While a highly detailed, day-to-day project plan is not required at this point, it is essential that the security team consider and record potential impacts in order to avoid surprises and the need for significant plan changes during implementation. The strategy should be comprised of three standard categories (tasks, deliverables and milestones) which define the ultimate solution in terms of things to do, tangible elements and critical dates.

The Tasks subsection lists the major tasks that must be completed to successfully complete implementation. These tasks are listed chronologically and should identify which groups or individuals will be responsible for each task and the timeframes for when the tasks will be accomplished.

The Deliverables subsection lists the documents, equipment systems, and reports that must be created by the security team. These should be tangible items (such as a hardware security module) rather than tasks, goals or other intangible objectives (such as "reduce fraud losses") and should help to frame the tasks in terms of understandable and recognizable objects.

The Milestone Schedule is a list of the critical points in the schedule where a decision to proceed or a confirmation of approach is required. As implied by its name, a milestone is an event that indicates a significant achievement has been made and, in reference to a security implementation plan strategy, sets a timeframe for the security manager and other key stakeholders to confirm that the strategy is sound and is leading to the desired result/objective. Accordingly, the Milestone Schedule should be a short list of important events, generally spread out evenly over the course of the implementation process.

3.6.1.5 Security Policies and Procedures

This subsection may include a comprehensive list and description of all policies and procedures relating to security or, more often, will provide a reference to a separate document (or documents) where such policies/procedures have been recorded. Regardless of approach, it is essential that all other elements of the Implementation Plan be consistent with and fully support the security policies of the organization. Likewise, any procedure for implementing security within the organization must also be compliant with policy and consistent with the other elements of the Plan.

The remainder of each individual plan will vary slightly in content, but should be organized to provide sufficient information and, where necessary, details to enable the security manager and key stakeholders to understand and approve it well in advance of any significant program expenditures and long term commitment of resources.

3.6.1.6 Validation Planning

Validation planning, or the monitoring of security-related activities after the security program is in place, is important to ensure that the security plan requirements are continually being met. This validation is the assessment of the plan activities following initial implementation, a review of the quality of the program implementation and a process to ensure that the new security policies and procedures are being followed and are effective in achieving the plans objectives. Maintaining adequate security levels for a regional program requires a long-term commitment to the validation process and, therefore, it must be planned with appropriate resources that are obligated to consistently adhere to a well-considered and well-defined process.

A validation process consists of monitoring activities on both, an established as well as variable schedule, and having mechanisms in place to evaluate the results of monitoring and making decisions (i.e., redesign, correction of errors, etc.) based on that evaluation. A common approach is to use a standardized, fully defined, documented, and repeatable procedure for validation. Validation planning should always begin early in the implementation process so that necessary changes may be incorporated in the final security plan where required. Validation processes should then continue indefinitely while being expanded to include such activities as confirming that passwords have been changed and are being properly protected as defined within security policy.

Validation should also include a review of the implementation plan itself (prior to formal implementation) to confirm that it is reasonable and achievable. This "reasonability check" should be performed by a person or persons not directly responsible for the creation of the security plan in order to provide an independent and, as much as reasonably possible, unbiased review. Long-term validation responsibilities should be assigned to the security manager or another individual that is not directly linked to the performance of security-related functions.

Validation should be viewed and managed as an ongoing activity within any organization. Over time, processes, environments, tools, and personnel can change within an organization. These changes often have negative impacts on a security plan by introducing new program participants or changing the roles and responsibilities of existing participants. Periodic validation is required to counteract these impacts and to ensure that the standards of the security plan are not being compromised.

3.7 Handling Security Breaches

The role of systems administrator becomes significantly more visible when monitoring activities result in the detection of a security breach. This responsibility, however, should not belong solely to the systems administrator. Rather, all users of the system(s) should bear the responsibility for monitoring security, understand the ramifications of a breach, and understand what to do if a breach is detected. If the impacts are severe, rapid decisions and reactions may be required and precious time may be lost if a process isn't in place in advance. Accordingly, security planning should include the development of procedures for reacting to a security breach including confirmation of the breach, evaluation of its impacts, development of an impact mitigation plan, and implementing procedures or system changes to prevent similar breaches in the future.

Specific procedures that should be included in the security breach plan are

- *Detection of Incident*: What immediate steps should be taken when a breach is detected or suspected?
- *Notification of Incident*: Who should be notified of a breach and in what order of priority? Who are the alternate contact points if critical participants are unavailable?
- *Determine validity*: What steps should be taken to confirm that the breach is real and to evaluate its financial, political, and public relations impacts?
- *Formulate response strategy*: Who should be involved in defining a short and (if necessary) long term mitigation plan? At each increasing level of impact, who can approve the plan? What other persons or groups need to be involved in implementing the plan?
- *Investigation*: What steps should be taken to determine the cause or weakness in the security program that facilitated the breach? How should the information be disseminated?
- *Implement Security Measures*: Who will be responsible for coordinating and overseeing the implementation of the response strategy? What steps will be taken to confirm that the strategy is effective and when should those steps occur?

- *Isolate and Contain*: Who will be responsible for identifying the specific impacts of the breach and, where necessary, identifying and remitting compensation, apologies, issuing public announcements, etc. to external entities? Who will determine if a legal response (i.e., Prosecution, lawsuit, etc.) is required?
- *Report Results*: Who will be responsible for verifying that the urgent problem has been resolved and who should they notify?
- *Follow Up*: What changes to the base security program are required to prevent future breaches and/or to mitigate associated impacts?

Any person can check systems or equipment for unavailable services, vandalism, theft, or the introduction of potent computer viruses or "bugs". To successfully monitor for security breaches, it is important, however, not to assume that a system is safe or uncompromised based on the fact that it appears to be running. Some forms of security breaches are insidious, that is they are initially benign but ultimately lead to major problems. Accordingly, it is entirely possible that the system breach occurred before monitoring was initiated or that it has been compromised in such as way that it is not immediately visible.

The most effective methods to protect systems and information from security breaches are based on a proactive approach. Some of the simplest and most inexpensive preventative measures, such as staying current with operating system and application software patches and virus detection lists, have proven to be among the most effective in combating the litany of software virus and worms that seem to appear with daily regularity. Another important and effective action that can be taken is to turn off unnecessary systems or services if they are not associated with a function or service that requires constant operation, thereby minimizing the windows of opportunity when hacking can occur. Regardless of the approach or approaches taken, the need to have experienced and knowledgeable systems security personnel available to monitor systems and to evaluate potential breaches is critical. Properly qualified and trained staff should be able to quickly confirm that a breach has occurred, identify its source, develop a plan to counteract the negative impacts of the breach, and follow-up with a plan to prevent such breaches in the future.

3.8 Security Guidelines by System Components

In each of the sections that follow, security guidelines that are specific to a particular component or group of components are provided and discussed in detail. While the general approach to security should be the same throughout the planning, implementation and monitoring processes, distinct components have unique requirements that must be addressed individually in order to ensure that unintended weaknesses in the overall plan are prevented or identified as quickly as possible. The system components/component groups to be discussed include:

- Section 4: Key Handling & Generation

  Within this section, the subject of encryption and encryption keys will be explored and explained. Recommended methods and best practices for establishing an encryption scheme and key management program are provided.

- Section 5: PICC Security

  Within this section, security techniques associated with the protection of data stored on the PICC will be listed and described.

- Section 6: CID Security

  Within this section, the document will review the security needs relating to the protection of data stored or passed through the CID, in particular as it interacts with the PICC. This section also addresses the options for securing data before it is transferred to a higher level system.

— Section 7: CID to Higher Level Systems

In this section, the protection of data that is transferred to and from the CID, agency central computers, a regional clearinghouse, and external systems will be analyzed and supplemented with descriptions of the best practices available to provide that protection.

3.9 Security Plan Implementation and Support Checklist

3.9.1 Prepare

a) Define security team responsibilities and objectives

b) Define security program objectives, scope and planning schedule

c) Establish security planning budget

d) Define high level security program requirements

e) Confirm buy-in from and participation in planning from marketing, operations, legal, technology and other stakeholder departments/agencies within region

3.9.2 Form Security Team

a) Identify regional security program manager

b) Identify:

   1) Operations team representative(s)

   2) Marketing team representative(s)

   3) Legal team representative(s)

   4) Technology team representative(s)

   5) Other stakeholder department representative(s)

   6) Key custodians

c) Establish security team meeting schedule and initiate meetings

d) Define high level security program planning and implementation project plan and schedule

3.9.3 Define Policy

a) Define and document target security level for all regional system components

b) Define and document core policy/mission statement for regional AFC system security program

c) Define system access policy, including

   1) User name configuration and password configuration and maintenance rules

   2) Rules for remote access to system

3.9.4 Perform Security Analysis

a) Identify and categorize regional AFC system assets, components and system users

b) Prepare risk profile and risk score for each component

c) Prioritize system assets/components based on risk score

d) Refine security program planning and implementation project plan and schedule based on prioritized asset list

3.9.5 Implement Preventative Measures

a) Define security key generation key management and key storage/distribution methodologies, including:

   1) Key length

   2) Key rolling methodology

   3) Key diversification strategy

b) Select message authentication code (MAC) encryption key algorithm

c) Define security features/methodologies for:

   1) PICCs

   2) Proximity Coupling Devices (PCDs)/CIDs

   3) Communications Components

   4) All data storage and processing devices

   5) RCH and agency central computers

d) Define Data Access Rules

e) Identify sensitive data elements

f) Determine strategy for encryption of sensitive data elements

g) Define access rules for database and data stored in other software applications

h) Define data storage architecture

i) Define security methodologies for:

1) PICC distributors

2) Load terminal operators

3) External participant systems

4) Disaster recovery and business resumption

j) Define security monitoring methodology and schedule

k) Identify long-term security monitoring team

l) Define penalties for lack of compliance

m) Define system users

n) Establish system/data access levels and permissions

o) Identify/establish access level for each system user

p) Select methodology for facilitating external/remote system access

q) Conduct Operating System (OS) and Applications Security Review

r) Verify/modify OS configurations

s) Verify/modify application level back door accesses to systems/data

t) Verify/establish procedures for regular downloading of security patch and other application updates

u) Select tool(s) for computer "virus," "cookie," and "worm" protection

v) Conduct Network Domain Security Review

w) Verify/select system firewalls

x) Verify/modify router configurations

y) Define component authentication procedures

z) Conduct Data Domain Security Review

aa) Select encryption methodology for highly sensitive data elements

bb) Verify/modify security of data archives

cc) Verify/modify security of data caches

3.9.6 Document Security Response Plan

a) Categorize all known forms of security breaches

b) Identify security breach response team

c) Document procedures for responding to each category of security breach

3.9.7 Maintain and Monitor

a) Establish security monitoring team

b) Implement security monitoring and reporting plan

4. Key Generation and Management Guidelines

4.1 General

As described is Section 2.0, security of any system primarily is applied by using authentication, encryption, access restrictions, and detection methods. While all of these methods must be implemented in tandem to achieve a reasonable level of security against both physical and logical forms of attack, the basis of most logical security is in encryption. That is the use of secret codes and processes to:

a) Change the appearance and/or physical nature of the data so that it is unintelligible to someone that does not have the means to decode the information; and,

b) Facilitate authentication of a component or content via some form of encrypted value.

4.2 Simple Encryption Schemes

The simplest forms of encryption replace one value with another using an exchange table of some type. As an example, if each letter of the alphabet is replaced with another letter three positions higher in the alphabet the exchange table would begin: A=D, B=E, C=F, etc. Using this scheme, a plaintext value of: SECRET would become: VHFUHW.

These methods can provide security only as long as the exchange table remains a secret and cannot be easily guessed.

NOTE 1—Brute Force" is the name given to a method used to attempt a breach of an encryption scheme by trying every possible value for a key until the correct value is identified. By using the known computational speed of a certain computer, the amount of time required to "crack" a key of any length using a brute force approach can be estimated.

NOTE 2—As examples, using a single HP 700 class computer a 40-bit (5 byte) key DES scheme could be cracked in 212 days while a 56-bit (7 byte) key would require 1 million days. Using a DES Cracking Machine (a device specifically designed to crack such schemes), the same 40-bit key could be cracked in 12.3 seconds and a 56-bit key scheme could be broken in 53 hours. A 128-bit key would require (theoretically) hundreds of millions of years.

NOTE 3—Clearly, a longer key length is desirable and necessary to establish a reasonable level of security with an encryption scheme

4.2.1 Modern Encryption Schemes

Modern encryption schemes use more elaborate methods that are based on strings of mathematical processes known as encryption algorithms. In some schemes, secrecy is maintained by creating a unique (proprietary) algorithm that is known only to the originators and recipient(s) of data. This approach has inherent flaws, however, since a separate algorithm must be created for every new set of originators and recipients and an existing algorithm must be changed if any one of the parties that utilizes the algorithm leaves the organization or the algorithm is somehow disclosed to a non-authorized party. To resolve these issues, standardized algorithms were created and are designed to use an alphanumeric value (known as the encryption key) as part of the algorithm. Originator/recipient groups that wish to use a standard algorithm need only select a unique key and maintain the secrecy of the key in order to establish a secure encryption scheme. In these algorithms, the plaintext values (in digital form) are converted to ciphertext through a series of mathematical functions that include the encryption key. As an example, a simple encryption algorithm might be:

plaintext value multiplied by key value = encrypted value.

Original Value = 1, Key Value = 2

1 x 2 = 2 (encrypted value)

In advanced forms of encryption such as the process known as the triple data encryption standard (or "triple DES"), the algorithm (which may include several arithmetic functions) is applied not once but up to three times – once to the original value, once to the resulting value, and once again to the second result – using two different key values. Since these algorithms are publicly available, the key is the crux of the security of the scheme and, therefore, maintaining its secrecy is of critical importance. Since a short key (as an example, one with just two digits) can be ascertained by simply trying all possible combinations, as a general rule, the length of the key is proportionate to the level of security that can be offered by any encryption scheme.

Encryption schemes are also used to authenticate data, rather than to encode it. This process generally entails the creation of a hash (a digital summation of the data or record) or a MAC, which is created by applying an algorithm and encryption key to the original data in order to calculate a new value. That value is appended to the original data element before it is sent on to another system. The receiving system can then use the same algorithm and key to verify the MAC and thereby confirm that the data element has not been altered since leaving its source.

Regardless of the encryption methodology used or how it is applied, the encryption key itself must be protected since the secrecy of that value enables the scheme to be secure. In many cases, the algorithm used for encryption or for creating a hash/MAC is publicly available and, therefore, only the key is kept secret. Accordingly, the security planning process must include carefully considered procedures for the creation of the encryption key (or "keys," since a system owner may elect to use different keys for different purposes within the system), the storage of those keys, and the transportation of those keys to the authorized parties that will need to use them. This section provides an overview of the methods that can be used for each of those critical steps within the implementation of a security program.

4.2.2 Common Security Terms for Key Management

Algorithm: A specific set of mathematical functions used to perform encryption processes.

Asymmetric: A method of encryption also commonly referred to as public key infrastructure (or "PKI") that utilizes a matched pair of keys. The first key is known as the public key and the second is known as the private key. The public key (which is made available through PKI services or provided by the recipient of information) is used to encrypt a file or data element or to generate a digital signature which is appended to the file/data element. The recipient uses his or her private key to decrypt the information and/or to validate the digital signature. Elliptic Curve Cryptography (ECC), RSA and DSA are examples of asymmetric schemes.

Authentication: A process used to confirm the identity of an individual, system, or system component or to confirm that information received has not been altered since leaving the originator of the information.

Ciphertext: A phrase used to describe data or information that has been encrypted to make it unreadable without decryption.

Cleartext: See Plaintext

DES/3DES: Acronyms for the data encryption standard (DES - an encryption scheme that was adopted in 1975 as the US national standard) and triple data encryption standard (3DES - a modified form of DES that uses two different algorithms and applies the encryption process three separate times in order to significantly increase the difficulty of unauthorized decryption).

Digital Signature Standard (DSS): The digital signature algorithm developed by the U.S. National Security Agency to generate a digital signature for the documents. DSS was put forth by the National Institute of Standards and Technology (NIST) in 1994, and has become the United States government standard for authentication of electronic documents. DSS is specified in Federal Information Processing Standard (FIPS) PUB 186.

Encryption: A process whereby plaintext is converted in one or more ways in order to make it unreadable or unintelligible.

Hardware Security Module (HSM): A physical device used for the purpose of securely storing encryption keys. Some HSMs provide the ability for one or more key custodians to manually enter values that become or are converted into encryption keys. Other HSMs have the ability to generate random values, negating the need for manual entry.

Hash: An encryption process that is used to convert plaintext (of any length) into a fixed length value (known as the hash value). This process is also known as a one-way hash, compression function, contraction function, and electronic fingerprint. A hash is typically appended to the plaintext by its originator to provide the means for the recipient to confirm (by repeating the hash process) that the plaintext has not been altered from its original form.

Key: An alphanumeric value that is used within an algorithm to perform encryption processes and, since the value can be kept secret, to make public algorithms secure.

Key Custodian: Individual who is responsible for one or more encryption keys or a portion of such keys. A key custodian may be responsible for creating the key or his or her portion of a key and/or may be responsible for holding a copy of the key/portion of a key in a paper or electronic form.

Key Encrypting Key: See Master Key

Key Generation: The process used to create the key used for encryption processes with the algorithm.

Key Generation Terminal (KGT): Device used to generate random values that can be used as encryption keys. A KGT may include an HSM for storage of the generated values or a KGT can transfer the generated values into an HSM.

Key Injection: Process of securely loading a key into the memory of a device that will use the key to perform encryption processes

Key Length: The number of bits or bytes utilized by a key when presented in a digital format.

Master Key: A term generally used to refer to the key that is used to encrypt other keys so that these other keys can be securely distributed. In this context, the Master Key may also be referred to as a key encrypting key. In a diversified key system, this term may be used to describe the base key that is combined with PICC or CID specific elements to generate all other (diversified) keys.

Message Authentication Code or MAC: A hash function that utilizes a key to enable the originator and recipient of plaintext to use a public algorithm to generate a hash to confirm the unaltered state of the plaintext.

Mutual Authentication: A form of authentication wherein two parties or systems involved in an exchange of data can first confirm the identity of the other party/system.

Plaintext: A phrase used to describe data or information that is readable in its present form by anyone without the aid of decryption. Also referred to as "cleartext."

Symmetric: A method of encryption that uses a single key that is also referred to as single or secret key cryptography. In a symmetric encryption scheme, the key must be shared between the parties that will exchange information. DES and Triple DES are examples of symmetric key encryption schemes.

Transport Key: Term used occasionally to refer to a key that is used exclusively to encrypt other keys while they are being distributed to authorized key users. See Master Key. This term is also used to describe the temporary key used by a PICC manufacturer to enable injection of permanent keys by a regional program owner.

4.3 Encryption Methodologies

Numerous methods for the encryption of data have been developed and have been successfully deployed. These methods can be grouped into two broad categories, asymmetric (also known as public key infrastructure or PKI) and symmetric (or private) key. Although each of these groups offer benefits and detriments, the primary advantages of an asymmetric approach (which utilizes a matched pair of keys - one publicly known and the other secret) are not readily applicable to a regional AFC program and, more importantly, the technology to perform asymmetric encryption does not currently support the high speed, high transaction volume environment dictated by mass transit. In a symmetric key system, all keys must be kept secret and different keys may be used for different purposes. Due to the technical restrictions of modern PICCs and the relatively slow transaction speeds between PICCs and PCDs using an asymmetric system, a symmetric key approach may offer the only viable solution for security between PICCs and PCDs/CIDs.

In an asymmetric key system, each party uses a matched pair of keys – one publicly known and the other secret. When a document is signed with its private key, the originator's identity and the integrity (unaltered state) of the data can be confirmed by the recipient by using the originator's public key to authenticate the digital signature. This approach thus assures the recipient that the originator is securely identified and that the data has not been altered since its origination.

In a symmetric key system, all keys must be kept secret but are shared between all the parties that exchange information. The use of such a key system guarantees the integrity of the data, but the originator identity cannot be confirmed with 100% certainty by the recipient because the secret key is common to all parties.

4.4 Security Domains, Major Threats and Risks

4.4.1 Security Domains

The application of logical security using encryption techniques requires the system owner to identify the entities (e.g., system components, staff members/departments, service vendors, program participants) that must interact in any way with system data. Once these entities are known, the system owner can establish security zones or "domains" that require access to encryption keys and can determine which of the encryption functions apply and the number of unique keys that are needed to support the encryption scheme. If the number of domains is small, the system owner may elect to use a single key for their entire security plan, however, the nature of most regional AFC programs are too complex for this approach and, therefore, distinct keys for each domain are highly recommended.

NOTE—Regional program owners should generate a unique key/key set for each domain that must perform encryption processes

Although each AFC program may differ in its methodology, the typical system will include the following security domains:

4.4.1.1 Key Generation and Storage

In this domain, the Master Key and all encryption keys/key sets are created and stored. Since the security of this domain is the most critical, this domain must be provided with the highest levels of protection offered by the security plan.

4.4.1.2 PICC and CID Initialization

In this domain, the encryption keys are encoded onto the PICC and/or CIDs in order to enable these devices to function within the system and within the overall security plan.

4.4.1.3 PICC to CID Interface

In this domain, the keys and algorithm(s) are used to facilitate the encryption of data or the generation of a MAC when a fare transaction is performed.

4.4.1.4 CID to Higher Level Systems Interface

In this domain, data created by the CID and PICC is transferred to another system component or it can be used by a higher level system to send data (such as an update to the negative list or a new encryption key) down to the CID. Since data is not created within this domain, encryption-based security is generally not required unless one or more subcomponents within this domain must process (rather than simply transfer) data.

NOTE□This document addresses only the smart card specific requirements for security of an AFC system. Most AFC systems will transfer critical messages (i.e., equipment configuration parameters, fare table updates, etc.) between the CID and the agency central computer. It is advisable, therefore, for such messages to be encrypted or protected with a MAC.

4.4.1.5 Agency Central Computer and Regional Clearinghouse

In this domain, accumulated data as well as individual data elements are transferred from an individual agency's system to the regional system or clearinghouse or vice-versa.

4.4.1.6 Regional Clearinghouse to Participant/Support Systems Interface

In this domain, data is transferred to and from external systems that are owned and operated by non-transit agency participants of the regional program. These entities may include third party customer service organizations, third party PICC issuers, and PICC reload terminal operators (such as retail merchants), among others.

4.5 Key Generation

4.5.1 Key Length

As a general rule, the longer the length of the encryption key(s), the more difficult the encryption scheme will be to break. Therefore, longer keys = greater security. Encryption using longer keys, however, also requires more computer processing power and time, elements which must be limited within any security plan in order to maintain cost and to meet the transaction speed requirements of the mass transit industry. Regional program operators must also consider, when determining encryption key length, whether the standards and requirements of other parties/industries should be applied to their regional program. As an example, the financial service industry requires the use of Triple DES, a standard which dictates a key length of no less than 16 bytes (128 bits). Regional programs that adopt this key length should be able to meet transaction speed requirements but will reduce their options for full feature PICCs since some are not designed to support a key of this size.

NOTE 1—Due to the need to achieve at least a moderate level of security and in order to maintain compliance with the most widely accepted security standards, regional program owners should implement their security plans using a key length of not less than 16 bytes (128 bits) for PICCs and CIDs.

NOTE 2—Limited Use PICCs are excluded from this recommendation.

Smaller programs and programs that have no plans to expand PICC usage beyond basic fare payment may wish to consider shorter key lengths in order to broaden their options for PICCs, CIDs and transaction processing solutions.

4.5.2 Types and Purposes of Keys and Key Rolling

4.5.2.1 Master Key

This key is the base value in a diversified key system and is typically used to encrypt all other keys used in the system. By using the Master Key to encrypt all other keys immediately following their creation, the regional program operator can securely transfer other keys and key tables to the end devices within the system and can store such keys (in an encrypted form) with relative confidence that they cannot easily be used if would-be hackers obtain a device and are able to retrieve the key from its internal memory. When used for this purpose, the Master Key may also be referred to as the Key Encrypting Key.

4.5.2.2 Message Authentication Code (MAC) Key

This key is used with the MAC algorithm to create the message authentication codes that are appended to data records or files in order to facilitate authentication by the receiving system. In order to establish a strong process for authentication of data, the regional program owner should establish MAC keys in two-key sets, with one key of each set being used to authenticate data received from another system component and the second being used to create MACs for outbound files. A separate MAC key set should, ideally, be created for each system domain that requires authentication as described in Section 5.5 below.

4.5.2.3 Read Keys

When information that is stored within the memory of the PICC must be retrieved or "read" by a CID, the PICC architecture may require that the CID provide an authentication value (created by a unique "read" key) in order to confirm the CID's authority to obtain that data. The read key may or may not be the same as the write key although different keys for read and write are recommended.

4.5.2.4 Write Keys

When new information is added to or existing information is modified within the PICC memory, the PICC architecture should require that the CID provide an authentication value (created by a unique "write" key) in order to confirm the CID's authority to modify that data. The write key may or may not be the same as the read key although different keys for read and write functions are recommended.

It is also advisable to create both a Current and Alternate key or key set for each of the key types described above. The Alternate keys/key sets are used to support System recover procedures (via a changeover from Current to Alternate key sets) following a security breach that is the result of the unintended disclosure or cracking of a Key or Key Set. The process of generating Alternate keys and key sets may also be used periodically in a procedure known as "key rolling" wherein the Current keys are temporarily supplemented with a new set of Alternate Keys and both are used until all PICCs that are encoded with the older (Current) keys have expired and the Current keys can then be deleted.

4.5.2.5 Key Diversification

Once an original (or "master") key or key set has been created, the regional program owner may elect to create unique keys for each PICC and/or for each CID in order to minimize the risk to the overall security scheme if any one key is somehow deciphered. This process, known as key diversification, generally uses a unique algorithm that is applied to the master key and other data elements that are unique to the PICC/CID such as the serial number. Only this new value, the diversified key, is stored within and used by the device from that point forward and only that value is available to a would-be hacker that attempts to breach the security system by calculating or guessing the key value. Since the key value provides access to one and only one device, a breach of this type can be mitigated by negative listing the PICC or, if the system supports it, negative listing the CID.

The use of key diversification requires a robust key management approach, however, in particular in the management of CIDs used within the regional program. The Agency Central Computer (ACC) and the Regional Clearing House (RCH) must have a record of each CID that is deployed, must know where within the system the device is located, and must maintain a list of the key(s) used by each device. These requirements will dictate that each agency carefully maintains inventories of deployed and spare CIDs and establishes and manages a secure process for the replacement, repair, and redeployment of CIDs when required for maintenance or malfunction of field units. The process will require procedures to ensure that new and replacement CIDs are registered by the ACC and the RCH at the time of deployment in order to update system records with the appropriate encryption keys. Without such a process, a weakness in the security program is created since transactions introduced by stolen or counterfeited CIDs could be introduced into the system with relative ease.

The primary alternative to key diversification is the use of a single key for all PICCs and (separately) a single key for all CIDs. This approach offers the advantage to the regional program owner in that it reduces transaction processing time (since the device authentication process does not need to include a calculation of the diversified key) and it minimizes the need for an extensive CID registration process. If a key is cracked, all PICCs or CIDs are at risk since all are vulnerable to attack and, therefore, a breach of security in this regard will be significantly more difficult to resolve.

4.6 Applying Encryption in a Security Program

As part of a broader AFC system security program, encryption processes will be used:

- For Authentication (of systems and data);
- In Transport (to enhance the security of confidential data); and
- In Storage (to protect the secrecy of data).

As mentioned above, regional AFC programs will generally require the establishment of several different security domains and the creation of unique keys or key sets for each of those domains. For each domain, the security plan should also define the manner in which encryption and encryption keys will be used. The following sections describe how encryption security is generally applied to each of the major security domains within an AFC system.

4.6.1 Master Key Generation and Storage

Within this domain, security is essential and, therefore, a high level of security is required. The generation of the original ("master") encryption key must be performed in a secure environment wherein no single individual may ever control or see the complete key in plaintext (unencrypted) form. The actual process of generating the key is a procedure usually involving the manual or automatic selection of alphanumeric values that will comprise some portion or the entire key. In order to ensure that key generation is reasonably secure, manual input should be performed by at least two individuals that are not allowed to witness the actions of the other or (ideally), a random number generator (a device or software application that automatically selects and inputs the key values) should be used.

NOTE—All encryption keys should be generated using a secure HSM. The HSM should generate all Key Sets automatically using a random key generator so that no person knows their contents. The HSM should also generate a 3DES-based Master Key by which all other System Keys/Key Sets are encrypted. The HSM should be used to securely store the Master Key plus a Current and an Alternate Key Set, which cannot be read from the HSM in unencrypted form. The HSM should also incorporate physical and logical security features to prevent discovery of keys via tampering.

For Authentication

Not applicable within this domain

In Transport

Every other domain that utilizes encryption processes for security must obtain a copy of the key sets used by that domain and a copy of the Master Key. The Master Key is typically used to encrypt all other keys/key sets prior to their transport to other systems/components. This approach generally requires that the Master Key itself be transported without encryption or a special key encryption key used just for the purpose of encrypting the Master Key while it is being transported.

More often, the two halves of the Master Key are encoded onto separate, contact-based smart cards and manually transported to the other domains by designated key card owners. The Master Key halves are injected into secure storage devices within each domain by inserting the smart card into a reader attached to the storage device. The insertion of the smart card activates a key injection program that downloads (after key cardholder identify validation) the Master Key half from the smart card into secure memory, ensuring that the Master Key is never disclosed in plaintext and is constantly held under dual control. Agency or Region keys can only be injected into a PICC if the PICC Transport keys are known.

In Storage

Key component values should be input to a secure hardware device that is designed for key storage. These devices, known as hardware security module (HSM) or key generation terminal (KGT), provide logical and physical protections for the device memory, where keys are stored, and may also have the ability to perform cryptographic processes, such as the encryption of MAC keys with the Master Key so that the MAC keys can be forwarded safely to a CID injection facility. Alternatively, a regional program may elect to use a software module that can simulate the functions of an HSM, although this approach is generally less secure. Once the master keys have been created, they must be stored in a manner that prevents any one person from retrieving or transmitting keys in the clear.

NOTE—As a general rule, a copy of the Master Key should be transferred to at least three pairs of contact smart cards (Master Key Cards) for back up purposes. One half of the Master Key is stored on each Key Card within a set and should be stored under dual control by the Regional Program Operator. No one card in a matched pair of Master Key Cards should be interchangeable with that of another pair.

The HSM is used to generate all the required System Key Sets and to encrypt those keys using the Master Key. Once encrypted by the Master Key, the System Key Sets do not need to be stored within a high security area although at least three encrypted sets should be maintained on electronic media (Floppy Disks, Tape or CD ROM) at different locations designated by the Regional Program Operator for backup purposes.

4.6.2 PICC and CID Initialization

In order to facilitate the loading of keys to the PICCs and CIDs, the entity responsible for this function must first obtain and securely store the keys and must also have the means to encode or "inject" those keys into the receiving device without revealing the keys in the clear either before or after injection has been completed. Since a breach of key security at this level could have system-wide impacts, key storage within the CID must minimally be tamper resistant. That is, keys must be stored in an electronic form that is automatically erased if the physical enclosure for the key storage facility is opened and which ensures that electronic access to the keys is strictly limited to requests by authorized and authenticated devices.

For Authentication

If the regional system (or individual agency system) can support the downloading of key sets through its communication network, it may be necessary to append a MAC to the transmission in order to provide a mechanism that will allow the CID or the device that will be used to inject keys into the PICC to authenticate the file upon receipt. This approach is used to prevent the introduction of counterfeit keys. If injection of keys into CIDs and other key storage devices is a manual process, authentication will probably not apply within this domain.

In Transport

As described above, all key sets should be encrypted using the Master Key, prior to leaving the secure key generation facility. Once key sets are encrypted, they can be recorded on any form of electronic media (such as a diskette or CD ROM) for transport to the key injection facility. Once keys are injected into PICCs and CIDs, no additional transport security need be applied.

In Storage

PICC Regional Transit Key Sets should be loaded into PICCs using some form of secure Point of Issue Device [PID]. The PID should also utilize tamper-resistant memory to store the Key Sets and a copy of the Master Key, which is needed to decrypt the key sets received from the HSM. The PICC itself should be designed to securely store its key(s) with both physical and logical protections to prevent unintended disclosure of a plaintext key.

4.6.3 PICC to CID Interface

For Authentication

In the PICC to CID interface, fare transactions are originated and therefore the critical security requirements include authentication of PICC and CID and the ability to authenticate data after it has been generated. Due to the risks associated with a breach of security within this domain, mutual authentication of PICC to CID is highly recommended. Authentication should be accomplished via the use of an encryption algorithm that is used by the PICC and, separately, the CID at the time the transaction is being performed to generate an authentication message that can be deciphered and confirmed by the receiving device. This method, known as active calculation, ensures that no device can complete a fare transaction before verifying the identity and authority of the other device.

NOTE—Mutual authentication of PICC and PCD using an active calculation method should be utilized to enhance transaction security.

Although numerous methods are available to ensure the authenticity of data, the most commonly used approach is the generation of a MAC which is then appended to the data record. MACing also can be accomplished using a variety of different methods, differentiated primarily because of their use of proprietary and public algorithms. Since the use of proprietary solutions inhibits open interoperability, implementation using a public algorithm is also recommended.

NOTE—Regional Program owners should utilize public algorithms for all encryption processes.

In Transport

Since keys are not generally exchanged between PICCs and CIDs, this use of encryption does not typically apply within this domain. When keys are initially injected into the PICCs, however, some form of CID is required to facilitate the injection process. Accordingly, the CID used to perform key injection into the PICC should store its keys in an encrypted form and the injection of those keys into the CID should be performed in a properly secured environment, under dual control.

In Storage

See PICC and CID Initialization above.

4.6.4 CID to Higher Level Systems Interface

Since information is not created, but is only transferred from one system component to another, and as long as secret information is encrypted while being transported through this domain, it is not necessary for this domain to support encryption processes or to have its own key set.

In the event one or more system components within this domain must process, decrypt, or authenticate information received from another domain, the system architecture must be structured to support the appropriate level of encryption processes. The nature of the encryption processes and keys will be dependent upon the functions assigned to this domain.

For Authentication

Applicable only if domain components are required to validate received data or must append a MAC to an outbound data file.

In Transport/In Storage

Applicable only if domain components are required to apply encryption processes to inbound or outbound data files.

4.6.5 Agency Central Computer and Regional Clearinghouse

In this domain, transaction data, negative list updates, key table updates, and various other data elements and files must be received from or sent to other domains and, when received, must be authenticated and, in some instances, encrypted/decrypted. Accordingly, the ACC and RCH must generally have the ability to store encryption keys and perform encryption processes including MACing, MAC validation, encryption, and decryption. Since each will receive and process data from multiple sources, each must store and utilize key sets supporting all other domains. Additionally, the key set required to support the file exchanges between the RCH and the ACC must be made available to and stored by both systems.

For Authentication

Both the ACC and the RCH will be called upon to generate and validate MACs and must, therefore, have these capabilities and must receive and store a MAC key set for all other domains with which they interact. In some system designs where transactions are processed between the ACC/RCH and other domains in an on-line environment, the ACC/RCH may also need the ability to perform a real-time, mutual authentication with the system/system component in the other domain.

NOTE—Federal, state and banking industry rules/regulations typically require that all cardholder information be protected when it is stored within a database or during transport to another system. New national and state privacy laws emphasize the need for such protections. Accordingly, regional program owners should consider an approach that applies encryption to all data within cardholder, merchant, transit agency, and transaction databases.

In Transport

It is likely that the ACC and RCH will need to exchange data on a regular basis. When that data contains sensitive or secret information, the data should be encrypted by the system originating the file and decrypted by the system receiving the file. Accordingly, both systems must have full encryption processing capabilities and may need to store a unique key set generated for this purpose.

In Storage

In general, the ACC and the RCH will maintain transaction record databases and may also maintain databases of load terminal operator, cardholder, agency, and PICC distributor information. Since all or a portion of this information will be confidential, it is advisable for that portion (or for all data within the database) to be encrypted. The latter approach provides the best level of protection since a would-be hacker would only be able to obtain an encrypted (and therefore unreadable) version of the data if they are successful in breaching the other physical and logical barriers to that data.

4.6.6 Regional Clearinghouse to Participant/Support Systems Interface

In this domain, the RCH may receive negative list updates (from third party participant and support systems), fare product transaction data (from third party load terminal network participant systems), PICC and CID initialization data from initialization systems and third party PICC issuers, and potentially transaction data from third party systems that accept the PICC for non-transit payments. This domain may also need to receive and process non-PICC transaction data such as credit/debit card exception files and may also disburse data (such as transaction reports, file receipt acknowledgements, and key table updates) to third party systems. Each system within this domain must, therefore, have the ability to securely store one or more encryption keys and, depending on the system's purpose, also have the ability to perform MAC generation/validation and other encryption processes.

For Authentication

External systems that interact with the RCH may be called upon to generate and validate MACs and must, therefore, have these capabilities and must receive and store a MAC key set that is shared with the RCH. In some system designs where transactions (e.g., Debit/credit card authorizations and settlements) are forwarded by the RCH to an external acquiring system in an on-line environment, the RCH and external system may also need the ability to perform a real-time, mutual authentication.

In Transport

It is likely that the RCH will need to exchange data with the external systems on a regular basis. When that data contains sensitive or secret information, the data should be encrypted by the system originating the file and decrypted by the system receiving the file. Accordingly, both systems must have full encryption processing capabilities and may need to store a unique key set generated for this purpose.

In Storage

In the event that an external system receives and stores confidential or secret information sent by the RCH, the regional program owner may require that the external system encrypt the sensitive data elements or all data within its database in order to maintain an acceptable level of security in all domains associated with the regional program. National, state and local industry regulations should also be checked in order to ensure that the external systems are in full compliance with the data storage requirements of those regulations.

4.7 Peripheral Key Storage Methodologies

4.7.1 Security Access Modules (SAMs)

In many mobile phone systems and in most contact-based smart card programs, encryption keys are stored in a special type of smart card known as a security access module or SAM. Like any smart card, the SAM is a computer chip embedded in a plastic card although, the card used to hold a SAM is typically much smaller than a credit card in order to enable it to be placed in special slots within the smart card reader (or CID). The secure capabilities of a smart card chip can be used to securely store the key data and certain SAMs can also perform encryption/decryption processes so that the key data can be stored in an encrypted form for added security. This method is highly effective as a storage medium but has an inherent flaw in that the addition or changing of keys requires the physical replacement of the SAM or electronic access to the SAM must be created, thereby reducing its secure nature. In addition, SAMs do not typically operate at the speeds necessary to perform transactions within the split-second environment dictated by mass transit fare payment and, therefore, can only be applied where speed is a secondary concern. One variation of this approach maintains primary key storage within the SAM but temporarily transfers a copy of the key into volatile memory (see “In Volatile Memory” below) for high speed access when the system is operational and requires encryption processes to be performed.

4.7.1.1 In volatile memory

An alternative approach to using a SAM is to store keys within specially allocated secure electronic memory of the device (e.g., in the CID). This form of memory is tied to the electronics of the CID and is erased if it is improperly opened or tampered with (automatically disconnecting the power and erasing the secure memory) or is removed from its power source. While this approach offers good general security for keys, potential weaknesses are the following:

— The mechanisms that protect access to the keys could be compromised by a malicious maintainer.

— Keys must be reloaded each time the device is dismantled for maintenance/repair prior to its reinstallation in the system.

4.7.1.2 Hidden in software

With this method, the key data is stored within the lines of code that comprise the application software. Since most programs consist of tens of thousands of lines of code, a hacker would be obligated to both obtain access to the code and must then find the values that make up the key. This approach is also generally effective provided that proper care is applied to the security of the code within all peripheral devices. Since changing the key requires manual location and rewriting of the key values, this approach creates some undesirable operational impacts.

4.7.1.3 Distributed in software

A variation of hiding key values within software code is a method whereby the key values are broken into a number of different parts and then distributed in various places throughout the code. As with the original approach, modification, and replacement of keys must be performed manually or a special software application must be used to track the location of each part of the key and to redistribute new keys when needed.

4.7.1.4 Hardware Security Module (HSM)

In a system where encryption processes are performed primarily at a central processing site or where all peripheral devices have an online, real-time connection to a host system, a hardware security module can be used to store keys. Since HSMs are designed specifically for this purpose, they offer the most advanced level of security for key storage but are too costly to be deployed in more than one or two central locations.

4.8 Security Risks for Key Management

4.8.1 Internal Fraud

Although great measures may be taken to protect the security of keys, one or more individuals in most security programs will be given access to the keys or portions of the keys in order to perform security-related functions. Few safeguards exist that can prevent a security system breach that is perpetrated by a "trusted" employee/contractor or through collusion by two or more such individuals. In order to mitigate this risk, the regional program owner should ensure that dual control is established for all key generation and management functions and that appropriate checks and balances are in place to provide third party verifications that can properly detect when unauthorized key access or usage has occurred.

4.8.2 Participant Fraud

This form of security breach is enacted by individuals or entities that perform services such as PICC activation or fare product reloads for a regional program but do not fall under the categories of employee or contractors. Without preventative and verification measures in place, inherent risks exist since all reload devices must have the appropriate keys in order to read and write value to the PICC. Methods to mitigate these risks come in a variety of different forms that are geared towards the specific functions that are performed by these participant entities. These include

- By PICC Distributors:

  Providing distributors with functioning PICCs that do not have any preloaded fare product and require the patron to load fare product at an authorized reload operator terminal or on transit premises. If the distributor also has a reload terminal, each PICC sale can be tracked electronically and the failure for a terminal to upload its transactions can be tracked and flagged electronically for follow-up. The latter approach is somewhat more costly (due to the need to provide each distributor with a reload terminal).

- By Reload Terminal Operators:

  This form of security breach would be perpetrated by an authorized reload terminal owner/operator who would attempt to extract the encryption key set from the reload terminal in his possession. This attack can be mitigated through proper physical and logical protections within the reload terminal as defined in Section 9 of this document.

4.9 Key Owner

For each domain that receives and utilizes encryption keys, a key owner (or owners) should be identified to take responsibility for the security of their assigned keys or key sets. This is particularly important if a process of manual injection of keys is utilized within any domain since control of the keys may be difficult or impossible to manage in any automated form. Key owners may be required to retain an electronic copy of each key or key set used within their domain. If those keys are encrypted, storage can be facilitated via CD-ROMs, diskettes, or smart cards. If the keys must be stored in plaintext form, storage should be performed on a set of smart cards (or other portable tamper-evident device) where only a portion of the key/key set is stored on a single device and access to the devices is maintained under dual control.

4.10 Applicable Standards and Laws

Following is a list of standards documents that may provide additional information/reference to better understand key management and encryption processes.

NOTE—These documents should not be arbitrarily listed as requirements in specifications and/or procurement documents except where specific sections can be accurately referenced and are directly applicable to the specifications.

- FIPS (Federal Information Processing Standard)

  Standards published by the National Institute for Standards and Technology (NIS) for use in Federal procurements.

- 3DES (Triple Data Encryption Standard)

  A non-proprietary encryption standard used in many different industries to protect data and transactions.

- CISP (Cardholder Information Security Program)

  Security requirements developed and adopted by Visa and MasterCard for the protection of information relating to bankcards and bankcard payment transactions.

- RSA

  A public key encryption method, which was developed at taxpayer expense.

- Patriot Act

  A Federal law that requires organizations that perform any one of a variety of different financial transactions to obtain, store and make available for disclosure, information about customers and the transactions they perform.

5. Security Guidelines – PICC

This section introduces several aspects of security for a PICC, specifically, those aspects that provide protection of the data-communication between the PICC and the PCD and that of the data that is stored within the PICC.

PICC security concerns are primarily related to the following:

a) Accessing the data on the PICC

b) Protecting the data that is stored on the PICC

c) Protecting the data in the communication channel between the PCD and the PICC

d) Protecting the data from malicious applications that are resident on the PICC

e) Protecting the data from duplication to another PICC

This section describes a variety of security techniques ranging from simplistic to very sophisticated that can be applied to the transportation application of a PICC. One or more of these techniques can and should be used to establish a security level that best fits the application (simple means for low value/low risk and sophisticated means for high value/high risk).

5.1 PICC TYPES

5.1.1 General

The high speed, high throughput, self-service transit environment requires fare media that feature ease-of-use, quick and reliable utility, durability, and cost-effective application. Contactless smart cards or "proximity integrated circuit cards" (PICCs) offer an ideal solution to these requirements. As defined in Work Package 1 of the UTFS, the data exchange on compliant PICCs is through an RF interface compliant with the ISO/IEC 14443 standard.

The following are three main categories of PICCs:

- Low cost memory IC (also referenced as "limited use PICCs")
- Hard wired memory logic
- Microcontroller (also referenced as "microprocessor")

5.1.2 Limited use PICC

This type of PICC uses a paper or inexpensive plastic body has very limited data storage capacity and could use an abacus-style counting method. The abacus method uses a limited intelligence register. The registers use hard-wired logic to decrement stored transit value on the PICC through a series of counter stages with decreasing values. When all the counter stages have been used, the monetary value is depleted. Limited Use PICCs can also store time-based fare products such as a three-day, unlimited ride pass. Since the memory is not rewriteable, the PICC is discarded after the stored value is depleted or the time-based fare product has expired.

5.1.3 Hard-wired memory PICC

The hard-wired memory PICC stores the value in its non-volatile memory. Stored value can be debited or credited and a transaction is usually protected to prevent unauthorized access to that value. This type of PICC can also be used to store time-based fare products or both time-based and stored value-type instruments. The hard-wired memory PICC comes in many types, varying in memory size and with different forms of protection for access to its data.

5.1.4 Microcontroller PICC

The microcontroller PICC also stores the value in non-volatile memory. In addition to the non-volatile memory, the microcontroller PICC can have many other types of resources. The advanced versions have read-only memory to store multiple applications, firewalls to securely separate those applications, various security processors and many security features to protect the data on the chip and the communication between the PICC and the PCD.

The number of applications that reside on the PICC will depend on the memory size. For example, this type of PICC could hold transit, credit and/or debit, electronic purse, and one or more loyalty applications on a single card. For a PICC to be successfully used in a multi-application and multi-issuer program, each involved party must have confidence that the system can maintain the integrity of its application and its related data.

5.1.4.1 Card Operating Systems

A microcontroller must have a card operating system (COS) embedded into its memory in order to function. Like that of a personal computer, the operating system defines the instructions that can be understood by the PICC and how the PICC will react to those instructions. While almost all PICC manufacturers offer proprietary COS, efforts driven primarily by the financial service industry over the past decade have led to the development of standards for COS although universal adoption of those standards has yet to be achieved.

The selection of an appropriate COS can be critical to program success and to the security of that program. Choosing the correct COS may, as an example, increase the functionality of the PICC by supporting reconfiguration of applications after the card is issued. In many instances, an issuing organization initially deploys their PICC with only a single application loaded onto it; as card acceptance grows and market opportunities arise, the issuer can increase the functionality of the PICC by adding new applications if the COS supports secure dynamic loading and unloading of applications. Selection of a COS that complies with one of the leading COS standards may be the best approach to ensure that the PICC deployment can migrate to more functionality as market and consumer acceptance increase. Collaborating organizations will also be able to multi-source the smart card controller, COS, and applications if a COS standard is adopted by a regional program. The two most popular standards for COS are Open Platform (sponsored by Global Platform) and MULTOS (Multiple Operating System – a proposed standard for multi-application card operating system sponsored by Mondex and MasterCard).

Open Platform compliant cards (which utilize Java CardTM technology developed by Sun Microsystems) are able to run small applications, called applets. This technology offers platform independence, the ability to store and update multiple applications, and compatibility with current contact-based smart card standards.

MULTOS (originally developed by Mondex International) is a high security, open standard for multi-application COS. MULTOS also has a flexible and secure application load and delete mechanism, allowing the card issuer to add new contact and contactless applications in the field.

Several card manufacturers and third party software developers have developed proprietary operating systems. These operating systems are usually developed for specific applications. These operating systems can also support multiple applications, but they do not provide the interoperable and multi-sourcing advantages that open operating systems offer.

NOTE□Refer to the more detailed overview of PICC types and available products in the APTA document, "Trends in Electronic Fare Media."

5.2 PICC Security Techniques

PICCs can have a variety of features that can be utilized to support various security functions. These features include the following:

- Unique or random ID number
- One Time Programmable memory
- Password Protected Memory
- Hardware to calculate Digital Signature
- Secret keys
- Cryptographic Co-Processors
- Hardware fire walls
- Memory scrambling technologies
- Physical Logic and Memory scrambling technologies
- Security sensors to detect malicious physical attacks

5.2.1 Protect access to the data

Access to the data can be protected by the following:

5.2.1.1 Password

The PICC is prepared with a password and the PCD needs to send that password to the PICC before it will release any data. The time to find the password with a "brute force" attack depends mainly on its length (number of bytes).

Operating error counters (to count the number of password request attempts) or delay times (to slow down brute force attacks) can further enhance password-based security.

Example: Some Limited Use PICCs may use this technique as it is relatively simple to implement in silicon and does not require any key generation and management functionality.

5.2.1.2 Digital Signature or Message Authentication Code

The CID has to send a signature or MAC appended to each message. The MAC is generated using a secret key or a session key. The PICC will perform a calculation (based on data in the message and the key) and compare that with the signature or MAC that it received from the CID before it allows access to the PICC data.

This technique can also be applied to messages from the PICC to the CID.

Example: Some Memory Logic & most Microprocessor PICCs employ this technique to ensure that no reading and writing of data to and from the PICC can be achieved without the knowledge of the appropriate PICC key. If this technique is applied to each and every read and write event and is proofed against replay attacks, this technique alone could be effectively applied as the sole security mechanism protecting data access.

As an alternative to a MAC, the CID may be designed to generate a digital signature that can be used by any receiving system to confirm that a message originated from an authorized source and has not been altered in transit. The DSS algorithm is one method that can be used by a CID to generate a digital signature for or “sign” usage transactions.

5.2.1.3 Mutual Authentication

Both the PCD and the PICC perform an authentication process before either will establish a communication link. Mutual authentication requires the PCD and the PICC to exchange information that confirms knowledge of the authentication key, rather than the key itself. Although there are many ways of accomplishing mutual authentication, most start with the PCD, which sends a message to the PICC that it wants to start an authentication with a certain key. The PICC generates a random number, encrypts it with that key and sends the encrypted number over to the PCD. The PCD decrypts the message and retrieves the random number that is generated by the PICC. Now the PCD also generates a random number and concatenates that with the random number from the PCD, encrypts the concatenation with the key and sends it over to the PICC. The PICC decrypts the number, retrieves both random numbers, and is now able to compare the random number that it received back from the PCD with the number that it had generated earlier. If both are the same, then the PICC knows that the PCD knows the key and that it can therefore trust the PCD. If both are the same, the PICC will encrypt the random number of the PCD with the same key and send it to the PCD. The PCD will decrypt the message, compare the numbers, and know that it can trust the PICC if the numbers are the same and authentication is complete.

After a successful authentication, both the PCD and the PICC assemble a session key that is derived from both random numbers and use that value to secure subsequent data communications. The system works with random numbers as a session key to prevent so-called “replay attacks.” Without random numbers, an attacker could record the communication between PCD and PICC and simply “replay” it later, simulating communications from a legitimate PICC or PCD. The use of random numbers prevents this form of security attack.

NOTESome Memory Logic & most Microprocessor PICCs employ this technique to ensure that no read/write sessions with the PICC can be started without the knowledge of the appropriate PICC key.

5.2.1.4 Personal Identification Number (PIN) or Biometric

The PCD has to send a PIN or a Biometric to the PICC. The PICC compares it with the information that is stored in its memory and allows access to the data if they are the same.

NOTE□This technique is rarely used in transit fare collection systems as it tends to have long transaction times that would inhibit throughput.

5.2.2 Secret keys and Key diversification

A secret key can be used to encrypt or protect the data on a PICC for an application. However, if someone is able to break into the system and find the key, the entire system is compromised and all PICCs will be in jeopardy. Key diversification is a method that generates a different key for every PICC by combining some unique value associated with the PICC (such as the chip serial number) with a master key. In a system using diversified keys, if someone breaks the security of a PICC and finds its key, only that PICC is compromised, not the entire system.

5.2.2.1 Protect the data using Cryptography

Encrypting the data before it is stored on the PICC is an effective means of protection. The approach can be further enhanced if other parameters, like a serial number or secret key, become part of the encryption process. Since encrypted data must be decrypted before it can be used in the fare payment process, this method is typically reserved for highly sensitive data (such as personal information about the patron) stored on the PICC.

5.2.2.2 Protect the data from duplication by restoring the original value

One form of security attack is to copy the data from one PICC to another medium (like a PC) and then to rewrite the original data to the PICC after the stored value or other fare products stored on the PICC have been used. Adding irreversible memory to the PICC can prevent this.

5.2.2.3 Protect the data from duplication by copying the data to another PICC

Without proper protections, the data in a PICC can easily be copied to another PICC. This form of attack can be prevented if each PICC has a unique or random ID and that ID is used to encrypt the data before it is stored. To use the data, a PCD must decrypt the data first with the unique PICC ID before it can be used. Duplication of the same data to a different PICC would cause an error since the ID of the second PICC will not work in the PCD decryption process.

NOTE□This technique is rarely employed in transit systems.

5.2.3 Protect the data from external probing of the chip

Modern secure PICC microcontrollers offer a variety of features to protect the data that is stored on the PCD from external probing. Some of the most common features are: Glue Logic (to hide the functional blocks and data busses), Random Access Memory (RAM) Scrambling (to store the keys in a different location every time the PICC is used),. Exception Sensors (which measure variations in voltage, temperature, frequency, and light) and a constant power source.

5.2.4 Protect the data from attacks within the PICC

Modern PICCs allow the download of new functionality after personalization. That also provides the potential for malicious applications to be downloaded to the PICC with the intent to read the keys from other applications stored on the PICC. This form of security attack can be prevented with a secure COS and a hardware firewall that triggers an event if another application tries to access the data within the transit application.

5.3 Security Threats and Risks

Security attacks on a PICC are usually designed to extract or change the secret information stored in the PICC.

Possible attacks can be categorized as

a) Observing the communication between the PICC and the PCD

b) Physically "observing" the PICC activity

c) Forcing the processor on the PICC into an uncontrolled fault mode

5.3.1 Observing the communication between the PICC and the PCD

A hacker can monitor the exchange of data between the PICC and the PCD by measuring the RF field and tracing (recording) all the signals that are exchanged. By recording these signals, the hacker can gain an understanding of how information is exchanged and can attempt to duplicate or alter the process in order to affect the stored data.

5.3.1.1 Countermeasures to protect against these attacks

Encryption or authentication of the data communication with session keys that contain a random element to ensure that they will be different for every transaction.

5.3.2 Physically "observing" the PICC activity

All activity of the PICC can be observed with probes, sensors, ion-beams, and laser-beams.

Possible attacks at physical level are the following:

- Analysis of data bus by probing clock and data lines
- Analysis of memory content by tracing bus activity and memory cell content
- Monitor side-channel leakage
  - Computation time (reveal information about key length, ratio of zeroes and ones)
  - Power consumption
- SPA or Simple Power Analysis:
- Obtaining information about the secret key by direct observation of the power consumption
- DPA or Differential Power Analysis:

- Calculating the secret key by tracing the power consumption for several thousands of computations and add them all up. The difference in power consumption at a certain time may indicate processing of a "one" or a "zero" and reveal information about the key. The effectiveness of this method can be improved through statistical science.
- Electromagnetic emanation (processor activity)
- Thermal emanation (physical location of crypto coprocessors)
- DFA or Differential Fault Analysis
- Calculating the secret key by comparing correct and incorrect output data

NOTE□Each of these forms of security attack requires a large amount of time, money, equipment, and technical expertise.

5.3.2.1 Countermeasures to protect against these attacks

- Mask shields and redundant circuitry – Addition of a "mask" to shield the lower layers of chip circuitry from probing. Redundant (non-functional) circuitry is added to confuse a hacker and make it more difficult to find functional traces that may be probed and scanned for data.
- Memory scrambling – Spreading the physical location of the data in multiple locations within the chip memory to make it more difficult to trace relevant pieces of data.
- For example, when a key is stored in RAM, every time the PICC is put in the reader field, the data is scrambled randomly and, the key is stored in a different RAM location with each use of the PICC.
- Logic scrambling - The parts of the microprocessor - central processing unit (CPU), co-processor(s), and bus - are logically divided in small parts and "scrambled" in three dimensions (X/Y and Z as a number of metal layers) in order to increase the difficulty of identifying the logical functions and therefore also increasing the difficulty of physically probing the chip to obtain a useful data trace.
- Bus encryption – Encryption of all the data that is exchanged over the bus in order to make it more difficult to recognize or trace a meaningful signal.

5.3.3 Forcing the processor on the card into an uncontrolled fault mode

The hacker hopes that by forcing the PICC to encounter an unexpected error condition, the processor will reveal information that can lead to discovering the secret data. Generating hardware faults during the execution of a cryptographic algorithm can do that.

5.3.3.1 Countermeasures to protect against these attacks

- Voltage, temperature and frequency sensors
- Optical sensors to detect ion-beams and/or laser-beams

5.3.4 Non-technical Attacks

In most regional programs, individuals and/or external organizations will be selected to perform the function of PICC distribution to transit patrons. If PICCs are distributed with preloaded transit fare product, the regional program owner must accept the risk that the authorized PICC distributor will attempt an attack against the system using non-technical means such as the theft of PICCs in inventory and unpaid or underpaid distribution of PICCs. These forms of attack can be mitigated by:

- Providing distributors with functioning PICCs that do not have any preloaded fare product and require the patron to load fare product at an authorized reload operator terminal or on transit premises. If the distributor also has a reload terminal, each PICC sale can be tracked electronically and the failure for a terminal to upload its transactions can be tracked and flagged electronically for follow-up. The latter approach is somewhat more costly (due to the need to provide each distributor with a reload terminal).
- Distribution PICCs on a prepaid wholesale basis. With this approach, PICC distributors are treated in the same manner that a product wholesaler treats its retailers. PICCs are sold to the distributor at a wholesale (discounted) price which must be prepaid by the distributor to the regional program operator. Rather than receiving a commission on each PICC sale/distribution, the distributor applies a markup to the cost of each PICC and markets the PICC at the increased price. This method effectively minimizes the financial exposure of the regional program operator provided that additional shipments of PICCs are not authorized until payment for past shipments have been confirmed.

5.3.4.1 Conclusion

Sophisticated integration of software countermeasures combined with hardware security mechanisms are needed to defend attacks on PICCs. Chip and PICC manufacturers have incorporated a number of successful methods within their products. These methods are generally of a very proprietary and confidential nature.

6. Security Guidelines - PCD/CID

6.1 General

The PCD and CID represent one of the single most significant components of a PICC-based AFC system (since these devices are the interface to the PICC) and, accordingly, must also be the cornerstone for the system security program. As discussed in previous sections, the PCD must be able to securely and accurately complete transactions through interfaces with the PICC and other AFC system components such as the CID (if the CID is a separate device), faregate, farebox, vending machine, etc. If transaction processing is not properly protected, system security may be compromised and a variety of negative impacts for the system owner/operator may result. Security planning, therefore, often begins with protection of this/these device(s) as described below.

The primary purpose of this section is to educate readers on the terminology used by vendors, describe a standardized methodology for quantifying the value of the PCD/CID and other system components in terms of security risk and list some of the most commonly used methods for mitigating security threats associated with this/these device(s).

6.2 Security Domains, Threats and Risks

6.2.1 Definitions

Security domain: A collection of entities to which applies a single security policy executed by a single authority.

Security level: A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection.

Security policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

Security threat: A potential violation of security.

6.2.2 Introduction to Risks and Threats

A proper PCD/CID security solution is determined after the threats and risks are identified. Such determination is best defined through a Risk Management Process (which identifies the priority for security planning by assigning a numerical risk assessment value to each component). The following section describes this process. Through the completion of a risk management process, system owners can make informed decisions regarding the security level that is required based, for example, on the criticality of the application residing in the PCD/CID, its physical location and the perceived value of each transaction which is performed or received by this/these device(s).

Risk management is used to:

a) Identify risks and make them understandable and tangible for the system owner;

b) Provide tools and methods to facilitate security planning and management at all levels; and

c) Discover legal liabilities and define the scope of impact of identified threats.

The goal of the risk management process is not to eliminate risk, but to help system owners quantify and prioritize their system's risks, to assess the organization's tolerance for those risks, and to manage operations in order to keep those risks within tolerable limits.

After calculating a risk assessment score for each component and transaction of a particular subsystem, the score is used as a guide during the process of developing, implementing, and maintaining the security plan. Likewise, the risk assessment can be used as a reference to evaluate various vendors' solutions, compare their approach to security and to ensure that the implemented solution provides appropriate safeguards for high priority components.

6.2.3 Assets and Asset Values

What are the assets and what value is assigned to the asset can be represented in terms of the losses that could be realized if the asset's security is compromised and based on the assets susceptibility to a security breach. Loss valuations can be based on the replacement cost of a component, the direct financial impact of the loss, and/or the non-financial impacts such as bad publicity. The latter could easily surpass the replacement cost of a component if, as an example, patron confidence or agency brand is undermined. Given that the PCD/CID is among the AFC system's most valuable assets in these terms, the protections of this asset require an approach that ensures that security is maintained at or above levels which have already been defined within known industry standards. These standards are described in Section 9.5 below.

Since the PCD/CID represents the primary interface to the PICC in order to facilitate any transaction, a breach of security associated with this/these device(s) could have substantial impacts, potentially requiring reissuance of all PICCs.

Table 1—Value of Assets

Asset	Value – impact of loss	Likelihood of security breach
PCD	High	Medium
CID	High	Medium

6.2.4 Calculate Risk

The risk associated with a threat can be considered as a function of the relative likelihood that the threat can occur, and the expected loss incurred given that the threat is realized. The risk is calculated as follows:

Risk = likelihood of threat occurring (given the specific vulnerability) x asset value

The asset value and likelihood of loss are defined as numbers from 1 to 3 (where 3 represents the highest value) and the two values are then multiplied. The result, the risk assessment, is a number ranging from 1 to 9. An assessment of 1 or 2 should be considered a low priority, an assessment of 3 or 4 should be handled as a moderate priority, and an assessment of 6 through 9 indicates assets with the highest priority for security protection.

As indicated in Table 1, the PCD and CID each represent an asset that can create significant loss impact if a security breach occurs and each has a medium potential for being the subject of a security breach since they are installed on end devices that are readily accessible to the public. With a value of 3 (high) and a likelihood rating of 2 (medium), the risk assessment value for the CID and PCD is 6, indicating a relatively high priority for the security program.

By calculating a risk value for each qualified asset, the operator will have an important tool needed to determine the type of solution/vendor to choose. In order to be more specific in determining the value for likelihood of loss, threats need to be identified, factored into the solution proposed and grouped by category. This process is defined in the next section.

6.2.5 Scope and boundary of the PCD subsystem

The threats faced by AFC system owners can be based on the entities (“actors”) associated with those threats. The following chart summarizes the groups of actors involved in the threat environments for the PCD/CID subsystem.

Table 2—Action in the Threat Environment

Parties involved in the Threat Environment	Role and Existence justification
Cardholder	User of the PCD/CID to perform transaction with the card which is in his or her possession.
Data owner	Party who has control over the data and keys within the card: e.g., the transit application provider.
PCD/CID subsystem, part of the Terminal	The device(s) and supporting software that facilitate interactions with the PICC and other AFC components.
Card Issuer	The party that issues the cards and manages its lifecycle.
PCD/CID Manufacturer, contractor to the Terminal integrator	The party that produces the subsystem, usually personalizes the device OS with applications data and keys prior to first shipment.
Load Terminal Operator	The party that is authorized to operate (and possibly own) a terminal that contains a PCD capable of reading and writing data to a PICC.
Software developer	The party who produces the application software that resides on the subsystem.

6.2.6 Risks and Threats

The risk and threats can be summarized in the following chart as possible attacks perpetrated by classes of actors interacting with the PCD/CID subsystem.

Table 3—Classes of Attacks

Classes of attack	Safeguard Options
Attacks by the terminal against the cardholder or data owner	1) Access control, Authentication, Authorization, Confidentiality 2) Encryption, secret-based authentication, Good Software Engineering practices enforced by the vendors, audited by an agency, CISSP certified staff (Certification for Information Systems Security Professionals – a formal certification process for individuals responsible for the protection of one or more systems.)
Attacks by the cardholder against the terminal	1) Access control, Authentication, Authorization, Confidentiality 2) C2 level file system, use of PIN combined with secrets for authentication and access control protection mechanisms. Encryption, key based terminal life cycle management, strong storage mechanism i.e., hardware based, Trusted Processing Module chips provided by the selected terminal vendor, audited by an agency (BS 7799), CISSP certified staff

Table 3—Classes of Attacks (continued)

Classes of attack	Safeguard Options
Attacks by the cardholder against the data owner	1) Access control, Authentication, Authorization, Confidentiality 2) Encryption, secret based authentication, Good Software Engineering practices enforced by both vendors, audited by an agency (BS 7799), CISSP certified staff
Attacks by the cardholder against the issuer	1) Access control, Confidentiality 2) Encryption, key based card life cycle management, strong storage mechanism i.e., hardware based, Trusted Processing Module chips provided by the selected card vendor, Good Software Engineering practices enforced by the Issuers, audited by an agency (BS 7799), CISSP certified staff
Attacks by the cardholder against the software manufacturer	1) Access control, Confidentiality 2) Encryption, key based application life cycle management, strong storage mechanism i.e., hardware based, Trusted Processing Module chips provided by the selected card vendor, Good Software Engineering practices enforced by the Software Manufacturers, audited by an agency (BS 7799), CISSP certified staff
Attacks by the terminal owner against the issuer	1) Access control, Confidentiality 2) Encryption, key based terminal life cycle management, strong storage mechanism i.e., hardware based, Trusted Processing Module chips provided by the selected terminal vendor, Good Software Engineering practices enforced by both the Issuers and the Terminal manufacturers, audited by an agency (BS 7799), CISSP certified staff
Attacks by the issuer against the cardholder	1) Authentication, Confidentiality 2) Encryption, key based card life cycle management, PIN or equivalent for issuer authentication, Good Software Engineering practices enforced by the Issuers, audited by an agency (BS 7799), CISSP certified staff
Attacks by the terminal manufacturer against the data owner	1) Access control, Authentication, Confidentiality 2) Encryption, key based terminal life cycle management, key based data access management, strong storage mechanism i.e., hardware based, Trusted Processing Module chips provided by the selected terminal vendor, Good Software Engineering practices enforced by both Terminal manufacturer and the Transit application provider, audited by an agency (BS 7799), CISSP certified staff

Table 3—Classes of Attacks (continued)

Classes of attack	Safeguard Options
Attacks by an authorized load terminal operator	By PICC Reload Terminal Operators: The primary risk associated with this type of attack is in the form of electronic distribution (loading) of transit fare products to PICCs by authorized personnel without the intent to remit appropriate funds to the regional program owner. This form of participant fraud can be mitigated through a variety of measures that can be implemented separately or in combinations. Specific methods include: — Postal Metering: This method establishes the means within each reload terminal to store electronic fare product which is downloaded from the RCH (or other central system). The terminal operator is typically required to pay for the fare products at the time of download. This approach not only limits the total value of fare products that can be loaded to PICCs before the operator must purchase and download additional fare products to the terminal but also minimizes the opportunity for the terminal operator to distribute fare products without proper compensation to the regional system owner. — Security/credit Checks: This method requires the regional system owner to establish security and credit qualification criteria for a fare product distributor. Standardized credit application forms and traditional legal and credit checking services can them be employed to facilitate this process. — User ID and Password Protection: This method utilizes the transit application within the reload terminal to require the input of a user identification number (ID) and a password each time that a reload transaction is performed. The application tracks each use of the terminal and reports all uses to the RCH.
Attack by an authorized land terminal operator (continued)	— This approach enables the RCH to link a specific reload transaction to a specific user, enabling the RCH and terminal owner to identify the individual that performed an unauthorized or unpaid load transaction (assuming that individuals properly protect their passwords).
Transformative or Impersonation attacks	1) Authentication, Integrity, Non-repudiation, Confidentiality 2) Encryption, secret based access management, strong storage mechanism i.e., hardware based, Good Security Engineering practices for communications protocols, based on Open Standards, reviewed/audited by an agency (BS 7799), CISP certified staff.
Attacks by third parties using stolen cards, terminals or components	1) Access control, Authentication, Integrity, Confidentiality, Audit, Accountability 2) Encryption, key based life cycle management, diversified keys, standards based diversification algorithms, trust splits among parties, customer service with emphasis on lost/stolen/malfunctioning devices/equipments, strong storage mechanism i.e., hardware based, for all chip based components, Good Software Engineering practices, effective operations management, audited by an agency (BS 7799), CISSP certified staff, trained staff. Own the business.

NOTEEach safeguard, or “security mechanism,” should be periodically checked whether it was implemented for the sake of prevention, detection/audit, or correction/recovery or whether the implementation was realized through logical, physical or procedural methods.

6.3 Security Options for the PCD/CID

6.3.1 Security Sub domains of the PCD/CID

The PCD/CID is a critical physical component of a regional AFC system and, accordingly, security protection must be approached via physical and logical means. In order to create a strategy for protection of the PCD/CID, the device should be considered in terms of three distinct security subdomains: the Cryptographic Module, the Cryptographic Boundary, and the Cryptographic interface.

NOTE 1—Security for PCDs and CIDs, regardless of manufacturer, should be designed to achieve at least the minimum security requirements level expressed as EAL-1 within the Common Criteria (a security standard that defines security of products and processes using a specific risk assessment known as a Protection Profile) or C-2 as defined within FIPS 140-2 (Federal Information Processing Standard) for security.

NOTE 2—Systems that allow broad use of T-purse, stored value purse or e-purse may require a higher level of security for the PCD/CID.

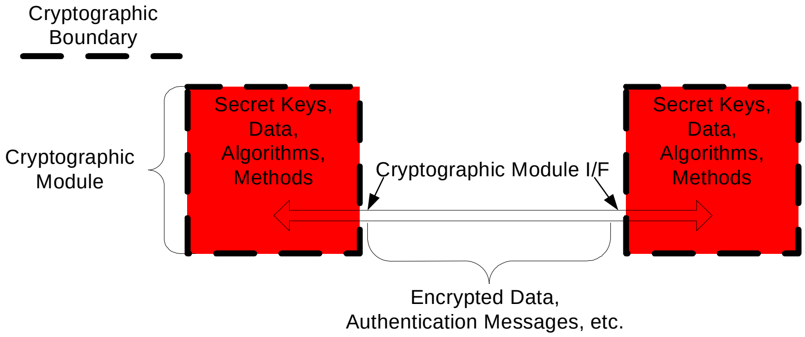
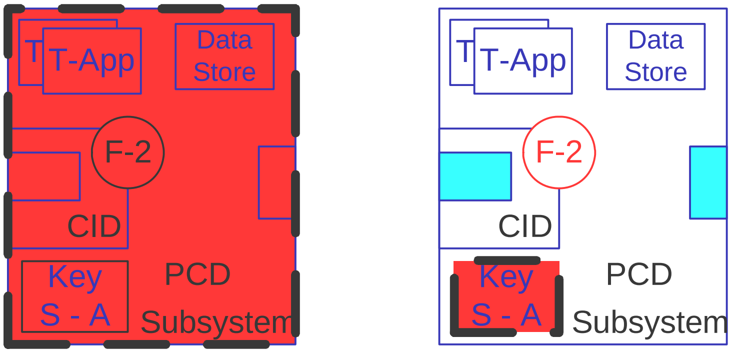

Cryptographic Boundary
Cryptographic Module
Secret Keys, Data, Algorithms, Methods
Cryptographic Module I/F
Secret Keys, Data, Algorithms, Methods
Encrypted Data, Authentication Messages, etc.

Figure 2—PCD/CID Security Subdomains

6.3.1.1 Cryptographic Module

The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) is contained within the cryptographic boundary.



CM defined as entire device

CM defined as module within device

Figure 3—Examples of Cryptographic Modules (CM) in a PCD/CID

Typically, the cryptographic module within a PCD/CID communicates to another device across an open and hostile environment. Accordingly, the cryptographic module must have the ability to send and receive encrypted data and authenticated messages in order to ensure that data is protected and has not been altered after leaving the cryptographic boundary of the transmitting module.

6.3.1.2 Cryptographic Boundary

An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of the cryptographic module.

The limits of the cryptographic boundary are critical for security of this component since they define the area that requires the greatest level of protection. Typically, the larger the boundary limits and the higher the security level the more difficult security will be to achieve and maintain. For the PCD/CID, the cryptographic boundary may encompass the entire device, a single security-specific component within the device such as a crypto co-processor chip, or several subcomponents of the device.

NOTE—As a general rule of thumb, cryptographic boundary should be defined as tight as possible in order to limit the size of the cryptographic module that must be secured.

6.3.1.3 Cryptographic Interface

A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows into or out of the module. Each physical and logical interface to the cryptographic module is a potential attack point. This includes data I/O lines, clock, power, ground & user I/O devices. Accordingly, the number of interfaces to the cryptographic module should be limited to the minimum number required to perform the functions associated with the PCD/CID. The type of physical interfaces used on the PCD/CID should also be a consideration as it is simpler to secure a serial port than a parallel port and a powered USB is typically easier to secure than separate power, clock and serial I/O lines.

Cryptographic Interfaces are discussed in greater detail in latter sections.

6.4 Interface with other system components

ISO/IEC 7498-2 defines the standards for the services that must be performed by an I/O device. This standard can be applied to a PCD/CID as described below.

Table 4 below provides a list of services that are typical of a PCD/CID and it identifies the mechanisms for security protection that are applicable to each services as defined in ISO/IEC 7498-2. This chart may be useful in the evaluation of a particular vendor's PCD/CID-based security solution.

Table 4—ISO defined Security Services

ISO defined Security Services	**Security Mechanism**						
	Decipherment	**Digital Signature or MAC**	**Traffic Padding**	**Notarization**	**Routing Control**	**Access Control List**	**Log & Event Control**
Authentication	X						
Access Control						X	
Confidentiality	X						
Traffic flow	X		X		X	X	
Non-repudiation		X		X			
Integrity	X						
Accountability & Audit	X						X

Every interface to the PCD/CID is subject to threats. The most common of these threats have been grouped and described in Table 5 below.

Table 5—Common Threats

Threat identification	Commentary
Masquerading	The pretense by a cardholder, system user to be a different cardholder, user in order to gain access to a service, to information or to acquire additional privileges. Within a smart card system, masquerading is typically accomplished when a card assigned to a patron qualifying for discounted fares is used by another individual not eligible for such discounts.
Replay	Recording and subsequent replay of a communication, in order to mimic an authorized transaction or transfer of information.
Data Interception	Logical observation of the transfer of data from one system component to another (i.e., From PICC to PCD/CID, etc.) for later use in a malicious attack.
Manipulation	Replacement, insertion, deletion, or re-ordering of data for future, fraudulent use.
Repudiation	An attempt by an authorized system user to deny having initiated an authorized transaction.
Denial of Service	The intentional overloading of a system in order to prevent the legitimate use of that system.
Misrouting	The capture and fraudulent redirection of data intended for communication between two or more system components in an attempt to cause system failures or to prevent proper tracking and settlement of transactions.

6.4.1 Recommended Implementation of Safeguards

Security mechanisms should be incorporated into the PCD/CID design to counter at least the critical threats. Listed below are the most common forms of security threats associated with transaction flow to/from a PCD/CID along with a list of the safeguards that may be employed to reduce or eliminate the security risk.

Table 6—Security Safeguards

Threat	Safeguards
Modification of transmitted data (accidental or incidental)	— Verification of the integrity of transmitted data through MACing.
Deletion of transmitted data (accidental or incidental)	— Verification of the integrity of transmitted data through MACing. — Verification of message sequence integrity through software validation of message sequence numbers.

Table 6—Security Safeguards (continued)

Threat	Safeguards
Insertion of transmitted data (accidental or incidental)	— Verification of the integrity of transmitted data through MACing. — Verification of message sequence integrity through software validation of message sequence numbers.
Impersonation of an entity (sender, receiver) involved in the communication process	— Authentication of sender through MACing — Verification of receipt through message acknowledgements process.
Unauthorized disclosure of information during transmission	— Securitization of highly sensitive data (i.e., Encryption key table updates, etc.) through encryption of messages.
Replay of transmitted data	— Verification of message sequence integrity through software validation of message sequence numbers. — Use of software validation tools that look specifically for duplicated messages.
Blockage of transmitted data	— System architecture designs that include alternative/backup communication channels. — Verification of message sequence integrity through software validation of message sequence numbers.
Raising communication traffic to decrease the system performance	— Use of filtering tools on communication lines to screen out unauthorized “traffic.”
Connection setup or transmission failure	— Authentication of sender through MACing. — Verification of receipt through message acknowledgement process. — Physical protection of key communication switches and end points. — Establishment of efficient service recovery procedures. — Alternative/backup communication channels.

6.4.2 Acceptable Residual

Each safeguard that is considered as an option to protect an asset at the predetermined security level will have a distinct implementation cost. Accordingly, cost is a critical factor in the selection of appropriate safeguards. In addition, an operator should be guided in the selection of safeguards for their PCD/CIDs (and all other system components) by the:

- Ease of integration;
- Interoperability with preferred security tools provided by other vendors;
- The level of protection provided by the safeguard.
- Durability and anticipated support requirements of the safeguard; and
- Service record of the vendor.

6.5 Applicable Standards – References

6.5.1 General

As mentioned elsewhere within this section, two existing standards for device security are particularly applicable for use by AFC system owners/operators in the creation of a security plan. These standards, FIPS 140 and Common Criteria are widely used in a variety of different industries and help to define specific levels of security that can and should be achieved by the security features of any device that is considered to be an important asset. An additional standard, ISO 7498-2 defines the inputs and outputs of a communications system and may be useful in identifying communication processes to and from a PCD/CID that require security protections.

6.5.2 FIPS 140 – 1 and 140 - 2

Standards and guidelines created and published by the National Institute for Standards and Technology (NIST) for US Government agency use in procurements.

FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information within computer and telecommunication systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and self-testing.

FIPS 140-2 validates security claims for products using cryptography. By law, U.S. government purchasing agents MUST purchase the product that is certified for FIPS 140-2 (or FIPS 140-1), over one that is not. FIPS 140-2 is also required in Canada and recognized in Europe and Australia. The financial community uses FIPS 140-2 to measure the safety of products handling monetary transactions, and the standard is also being adopted by ISO and ANSI.

6.5.2.1 FIPS Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components.

An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

6.5.2.2 FIPS Security Level 2

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Possible examples of security level 2 are ISO 7816 ICC (Smart Cards).

6.5.2.3 FIPS Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

An example of a security level 3 device is a point of sale PIN pad.

6.5.2.4 FIPS Security Level 4

Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected; resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 devices are generally used in key injection facilities to generate and distribute keys.

For agencies electing to achieve a security level greater than 2, the cryptographic boundary and the cryptographic module must be designed to be as small as possible in order to minimize the physical area that must be secured. To this end, it is reasonable to design the cryptographic module within a CID/PCD and to define the cryptographic boundary as a border around just the CM.

6.5.3 Common Criteria

Common Criteria is the name historically used for the multipart standard ISO/IEC 15408, in lieu of its official ISO name of "Evaluation Criteria for Information Technology Security."

In October 1998, the Common Criteria was created as a mutual agreement by government organizations of Canada (CSI), France (SCSSI), Germany (BSI), the United Kingdom (CESG), and the United States (NIST) to recognize security evaluation standards and methods internationally. The origins of the Common Criteria can be traced back to initial developments by the U.S. federal government in 1985 as the TCSEC or Orange Book. Since then, several criteria versions for security evaluation have been formulated by the U.S. and the European ITSEC countries. In essence, the Common Criteria is an advanced offspring of the combined research and efforts of these former organizations. It was formed as a mutual agreement complemented by the close coordination and experience of the aforementioned security evaluation bodies – with the additional focus of resolving existing conceptual and technical differences and offering a flexible approach to security functionality and evaluation in a global IT market.

Under the Common Criteria Recognition Arrangement (CCRA), today the Common Criteria signatories also include Australia, Finland, Greece, Italy, New Zealand, Norway, and Spain. In the United States, the National Institute of Standards and Technology and the National Security Agency operate the Common Criteria Scheme under the National Information Assurance Partnership.

The underlying measures of the Common Criteria are based on functional and assurance requirements of a security product. Functional requirements define the desired security of the IT product as offered by the security vendor, and assurance requirements confirm the effectiveness and implementation of the security implementation.

Key concepts used in Common Criteria evaluations and certifications include Protection Profiles (PP), Target of Evaluation (TOE) and Security Targets (ST).

6.5.3.1 Protection Profiles (PP)

Protection Profiles define a standardized set of security objectives for different products or systems that perform similar IT security functions. The certification of a product includes the verification of a protection profile used and simplifies the comparison of certified products, as well as procurement and advice to manufacturers.

6.5.3.2 Target of Evaluation (TOE)

Target of Evaluation is the specific IT product or system that is subject to evaluation.

6.5.3.3 Security Target (ST)

A Security Target contains the IT security objectives and requirements pertaining to a specific target of evaluation with the definition of its functional and assurance measures.

The Common Criteria has a defined set of Evaluation Assurance Levels (EALs) that measure the criteria of evaluation of the security product's protection profile and test the target of evaluation to verify that it meets its security claims as stated by the IT product vendor. The EALs offer a comparative platform to the consumer in selecting a product and also form the basis of Common Criteria certifications.

The evaluation levels are ordered hierarchically in increments beginning from EAL1 to EAL7, with each level requiring a more advanced and intense means of testing. To date, EAL4 is the highest level certification awarded to any security product in the market.

EAL1 is a minimum level of assurance, which only analyzes the functional and interface specification in a bare-boned frame without requiring much documentation. EAL2 level is more detailed because it includes the high-level design and detail specifications of the target of evaluation. This level and its latter counterparts require developer testing and a vulnerability analysis. EAL3 analysis expands the testing coverage of the security functions and mechanisms and offers added security measures by ensuring that the target of evaluation is not tampered during development. EAL4 requires more design description, a subset of the implementation and improved mechanisms and/or procedures in ensuring that the target of evaluation will not be tampered with during development and delivery.

Evaluations from EAL5 to EAL7 have not yet been recognized by all Common Criteria members, and the requirement for such high-level testing of product complexities has not evolved so far. This is not to say that EAL5 evaluations are not encouraged – it is expected that technology enhancement will create a situation for testing a security product for the EAL5 level, and the process of evaluation will be encouraged while member countries of the Common Criteria agree on methodologies for EAL5- to EAL7-level testing.

EAL5 to EAL7 evaluations cost substantially more to the developer, and these levels of evaluation concentrate on semi-formal and formal design.

For additional information about Common Criteria, visit: http://www.commoncriteria.org/ or http://csrc.nist.gov/cc/ on the World Wide Web.

6.5.4 ISO 7498-2

This International Standard specifies a protocol which is used to provide a contactless communications network.

This Standard specifies:

a) Procedures for the connectionless transmission of data and control information from one network-entity to a peer network-entity;

b) The encoding of the protocol data units used for the transmission of data and control information, comprising a variable-length protocol header format;

c) Procedures for the correct interpretation of protocol control information; and

d) The functional requirements for implementations claiming conformance to the Standard.

The procedures are defined in terms of:

a) The interactions among peer network-entities through the exchange of protocol data units;

b) The interactions between a network-entity and a Network Service user through the exchange of Network Service primitives; and

c) The interactions between a network-entity and a subnetwork service provider through the exchange of subnetwork service primitives.

6.6 Risk Management for the Operator

The following questions and checkpoints are adapted from FIPS 191 LAN Security Guidelines. It is recommended that Operators use the following Framework to select the proper PCD/CID hardware/software solution, beginning with a Risk Management assessment.

6.6.1 Risk Management

The term risk management is commonly used to define the process of determining risk, applying controls to reduce the risk, and then determining if the residual risk is acceptable. Risk management supports the following two goals:

— Measure the risk (risk assessment); and

— Mitigate the risk (risk mitigation) by selecting appropriate controls that will reduce risk to an acceptable level.

The issues to be addressed by the system owner/operator when assessing the security features of a PCD/CID include the following:

1) *Assets* - What should be protected?

2) *Threats* - From what do the assets need protection and what is the likelihood that a threat will occur?

3) *Impacts* - What are the immediate damages if the threat is realized (e.g., disclosure of information, modification of data)?

4) *Consequences* - What are the long-term effects of the threat being realized (e.g., damage to reputation of organization, loss of business)?

5) *Controls* - What are the effective security measures (security services and mechanisms) needed to protect the assets?

6) *Risk* - After implementation of the security controls, is the remaining risk acceptable?

6.6.2 Risk Management Process

The goal of risk assessment is to determine the risk to the PCD/CID. The risk assessment process is conducted in six steps as follows:

1) Define the Scope and Boundary and Security Methodology

2) Identify and Assign Values to all System Assets

3) Identify Threats and Determine Likelihood

4) Measure Risk

5) Select Appropriate Safeguards

6) Implement and Test Safeguards

7. Security Guidelines – RCH to CID/External Systems

7.1 General

This section provides guidelines for the security of PICC-specific information/data stored within and transferred to or from the regional clearinghouse (RCH). The RCH will perform its data transfer functions with the CID (in most cases using the agency central computer – ACC – as a switch to direct data to/from the appropriate CID) and with certain external systems – the variety of which will be dependent on the number of critical, PICC-related functions being performed on third party systems. While it is understood that numerous fare collection-related messages and transactions are transferred between the CID and the ACC, this section focuses exclusively on the PICC-related data generated as part of a regional smart card program. Accordingly, while security of other (non-PICC) messages is also important to each agency, the guidelines defined within this section will not pertain to those messages.

Once a PICC-related transaction has been performed between a PICC and CID and transaction data has been recorded, the CID must initiate the transfer of that data to the RCH for validation and processing. Since such data will, by necessity, be used by the RCH as a primary factor in determining financial settlement for all regional program participants, the security and authenticity of that data must be properly protected while in storage and during the transfer process. Likewise, messages emanating from the RCH to the CID, from the RCH to an external system or from an external system to the RCH must be packaged and transmitted in a manner that ensures that each can be authenticated and used by the receiving system or system component. In addition, the RCH must perform the critical function of creating and maintaining a central database which facilitates auditability of all transactions that are performed within the region and the RCH must perform fraud detection functions in order to complete its role within the overall security program.

Accordingly, security techniques for data residing in, received by, or transmitted from the RCH must include encryption, MACing, fraud detection, firewall protections, intrusion detection, operations monitoring, auditing, and a robust disaster recovery solution. These techniques, which are described more thoroughly below, can generally be grouped based on their contribution to the achievement of the following three broad objectives:

a) The validation and authentication of data received by the RCH

b) The security of data while in storage within the RCH

c) The authentication and acknowledgement of data transmitted from the RCH

7.2 Security Domains, Major Threats and Risks

As with all other regional system components, the application of security for data stored to or from the RCH requires the system owner to identify the entities (e.g., software programs, staff members/departments, service vendors, program participant systems) that must interact in any way with the RCH for the purpose of obtaining or sending data and then to define the applicable domains that require unique security solutions. For the RCH, the significant security domains include the following:

- *Physical*: The hardware-based elements of the RCH, ACC's, CIDs, and external systems.
- *Network*: The hardware and software components of the communications system(s) that is used to transfer data between the RCH, CID and external systems.
- *Data*: The electronic form of the transactions records, PICC records, participant information, and messages that are received or generated by the RCH.

Each of these domains must be evaluated against the three primary objectives defined above and a security plan must be established to properly protect the data as required by the objectives that are applicable to the domain.

For the Physical domain, such threats include attacks by both authorized and unauthorized users, vandalism and theft (especially for CIDs deployed in the field).

For the Network domain, threats include the introduction of network sniffers (software programs used to monitor communications on the Network much like a wire tap), disruption of service due to deliberate and accidental damage to physical communication lines, spoofing (attempts to communicate with the RCH or other systems by mimicking the messages of authentic system components), and others.

For the Data domain, the regional program owner must protect against potential attacks which may include data manipulation (the unauthorized alteration of genuine data while it is being transferred), data theft, introduction of software viruses, loss of data, and misdirection of data, among others.

7.3 Applicable Standards

- Common Criteria 2002-06-006 Operating Procedures
- Security Configuration Checklists Program for IT Products; NIST Publication 800-7- Department of Homeland Security
- Center for Internet Security CISSecurity.org; Defense Information Systems Agency Security Technical Implementation Guides: iase.disa.mil/techguid/stigs.html
- NIST: csrc.nist.gov/pcig/cig.html

7.4 Physical Domain

The physical domain encompasses all of the various components of the system, from the logical components such as applications and Operating Systems to the physical components such as actual equipment locations and hardware.

These components have been broken down into several main categories for discussion purposes. Each category will start with the most basic techniques of security and progress to the more sophisticated techniques.

7.4.1 Platforms & Operating Systems

The core of any system is the hardware and the Operating System on which the system is built. These core components must be properly secured as a breach in security of either of these components compromises all other levels of the system.

System hardware includes everything from the desktop PC to the mainframes and high end servers while Operating Systems can range from embedded Operating Systems to complex multi-user Operating Systems. The concepts of how to secure a system, regardless of the numerous and varied system and Operating System components are summarized as follows: Policy, Access Control, Authorization, and Operating System choice.

Policy is the simplest of the security techniques to implement; however, it is only effective when the policies are enforced. Some policies to implement include the following options.

7.4.1.1 Warning Banners

The simplest, yet most often overlooked 'security' technique to implement is the usage of warning banners. These banners should be used to inform users, as well as warn potential attackers, of the rules & regulations for using the system resources as well as penalties for abuse.

7.4.1.2 User & Password Policy

User access should not be arbitrarily given out, each user should have a function and a specific individual should be responsible for that user account. Most OS allow for 'groups' to be created so that users with similar functions can access system resources. Users can belong to multiple groups based on their function, e.g., a user may belong to both the 'developer' and 'engineer' groups.

As discussed in section 4.3, passwords are a critical element of many security schemes; as such password control should be strictly enforced. Policies such as password expiration, history/rotation (i.e., cannot reuse a password, etc.), and complexity (forced usage of non-alphabetic characters such as numerals) should be implemented.

Guest users should be eliminated when possible to tighten security. In addition, certain Operating System services create special users and directories as part of their process. If any services are disabled, the associated accounts and directories should be removed or disabled as well to prevent security breaches.

Access Control is another technique to implement as it assigns accountability to users of the system. Access control assigns access rights to use a particular resource, such as a file, command, or object. Access control is built into most Operating Systems and typically allows access privileges to be assigned to each resource in a system, this means that a particular user or group can be assigned rights to one file or command, but restricted from others. The system administrator has full access to all resources on the system and is responsible for assigning the appropriate access control to the other users who utilize the system resources.

Access Control should be implemented at all levels of the system to restrict system access to authorized users. The following is a subset of the more common access rights:

R – User can read the file

W – User can write to or modify the file

D – User can delete or erase the file (sometimes this is part of the W permission)

X – User can execute the command or change into the directory

C – User can modify the permissions of the object (sometimes this is part of the W permission)

Authentication of users is required to verify that a user accessing system resources is who they claim to be. There are numerous methods of authentication available, many of which can be used in combination to further improve security.

7.4.1.3 User/Password

User/password combo is the most basic form of authentication and merely requires that a user enter their username and a password that only they know. Some systems store the user and password information in a user password file. Due to the way most Operation Systems authenticate users; this file is typically a plain text file, readable by all users, with the password information encrypted for security purposes. However, since the file is readable by everyone it can be compromised.

7.4.1.4 Shadow Passwords

Shadow Passwords is an attempt to better protect password information by removing the passwords from the user password file and moving it to a file that only the system administrator can access. This file is harder to compromise as a higher level of system access is required to even access the file.

7.4.1.5 Two-factor Authentication

Two-factor authentication combines two methods of protection, usually a hardware device ('something you have') and a password/passphrase/PIN ('something you know'). The hardware device generates a unique key which is used in combination with the user's passphrase to authenticate the user for a predetermined amount of time.

7.4.1.6 Kerberos

Kerberos is a security package which is based on the usage of 'tickets' to authorize users to use system applications. Tickets are only good for certain users, at certain times, for certain services and are only issued once the users performs a password based authentication process. Kerberos offers a high level of security, but requires that all applications which require authorization be compiled with the Kerberos libraries (which may not be possible with certain applications).

Another key security technique is the selection of the Operating System as well as how the Operating System is configured and maintained. A number of different Operating Systems exist. The majority of these are either Unix based or Windows NT based. Regardless of the type of Operating System implemented, the following techniques should be applied:

7.4.1.7 Operating System Patches

Operating System manufacturers frequently release service packs and patches to address issues with their Operating System. These should be applied, when required, in order to minimize the risk of attack using unpatched exploits. Patches must be properly managed and must be evaluated to ensure that they do not cause other portions of the system to fail.

7.4.1.8 Hardened Operating System

A Hardened Operating System is an Operating System where the kernel has been specifically modified to implement additional security features. These features include separating the various Operating System and application levels from each other so that a breach or exploit of an application does not compromise the Operating System itself. Hardened Operating Systems often employ other techniques such as file system encryption, event logging, and mandatory enforcement of access control (users cannot arbitrarily assign permissions to other users).

The applications which run on the various hardware platforms within the system must also be evaluated to enhance system security. Some techniques to implement are:

7.4.1.9 Remove Unnecessary Services/Daemons, Users and Protocols

Remove all unnecessary services such as web servers, ftp servers, time/date servers, etc. unless absolutely required by the system which the service is running on. For instance, the database server should not also serve as an anonymous ftp server. When possible, services should be replaced with secured versions of the service. Common services such as telnet, trivial file transfer protocol (tftp), finger, remote who, remote copy, remote shell offer secured versions which typically connect to a secure shell daemon which uses encryption techniques to protect data.

7.4.1.10 Configuration

Proper configuration of all services that are enabled on a system is another technique which should be implemented. Many services use default settings, including usernames and passwords, which are widely known (e.g., the default simple network management protocol – SNMP - community strings are widely known). These should be changed to minimize the risk of a successful attack.

7.4.1.11 AFC Application

The AFC application is an aggregate of all of the various software which provides the AFC functionality on a system such as accepting and validating connections from field and remote systems, performing data collection, and performing equipment configuration changes. The AFC application often includes proprietary software and custom built scripts which should be evaluated to insure that they pose no security risks. Some techniques to consider include the elimination of unencrypted password or key information from scripts as well as the display of sensitive information in process listings.

System Protection software should be implemented to proactively protect a system from attack. There are several classes of protection to choose from:

7.4.1.12 Auditing and Logging

The auditing and logging features of the Operating System should be enabled to provide an audit trail. These features vary by Operating System but typically allow for the logging of major system activities such as logon/logoff activities, application startup/shutdown, and connection activities. The audit trail is required in case the system is ever compromised. For a more secure implementation, the logs should be copied to a second system and/or dumped as a hardcopy to prevent alteration of the logs in case of system compromise.

7.4.1.13 Intrusion Detection

Intrusion Detection Systems (IDS) monitor and log activities on a system and/or network and are designed to alert the administrator to suspicious activities. An IDS is typically meant to augment existing security measures.

7.4.1.14 Antivirus

Antivirus software should be installed on every server/computer in the system to prevent infection from viruses, Trojans, worms, and other destructive software as described section 6.3. It is crucial that the virus definitions remain up to date and that the system is scanned on a routine basis. Some packages allow for ‘live’ protection which scans all new files as they are created.

Also included in the same category as ‘Antivirus protection’ is software such as ‘AntiSpam’ software and email filters which are used to protect destructive software from entering the system via email or other ‘legitimate’ means.

7.4.1.15 Hardware Security

A major key to the protection of any system is control of the physical access to the actual hardware components of the system. Equipment should be located in rooms with restricted access. Rooms should include some sort of keyed access, electronic if possible, and it is preferable that they are monitored in some way via camera or other method. Examples of areas that need to be protected are Server Rooms and Communications Closets. Procedures should be implemented which monitor and control the access to these areas by all parties, including employees, vendors, and maintenance personnel.

Equipment (including consoles and peripherals) should also include physical protections such as lockable equipment cabinets and chassis. Direct access to the equipment (e.g., console, routers, switches, chassis, etc.) allows an intruder to bypass many of the built in security features of a system. As in the case of the physical access to the rooms, procedures should be in place to monitor physical access to the equipment and the activities performed.

7.4.1.16 Data Integrity

A condition in which data has not been altered or destroyed in an unauthorized manner.

7.4.1.17 File System Encryption

Section 4, discussed several methods of encrypting data, these same methods can also be used to encrypt data and files stored on the system's computers and servers. Data is typically stored in file systems created by the Operating System. The level of encryption can range from the encryption of a particular file to the encryption of entire file systems. In certain cases, such as databases, an application and not the Operating System may be responsible for the storage (and security) of the data, but these other methods also provide methods of encryption. As is the case in the encryption at the PICC/CID, the more encryption desired, the more of a performance hit the system incurs, however as this is done on the central server it should not impact the customer.

NOTE□At a minimum ALL keys should be encrypted wherever they are stored.

Validation of MAC (MAC sent from CID/PICC)

Validation of Sender (list possible options)

7.5 Network Domain

7.5.1 General

The communications network connecting the components of a regional system poses one of the largest security risks in a regional system. An attacker can gain access to the system at any node within the network, often times without being detected. In order to prevent security breaches several techniques will need to be employed to secure the network. These techniques include authentication, validation, and acknowledgement of data and data transmissions.

7.5.2 Network Basics

Most basic networks operate in what is known as 'promiscuous' mode. This means that all devices on a network segment (typically connected via a hub) can monitor the traffic between all of the other devices. Typically, a device ignores any traffic that is not meant for it (either directly or via a broadcast message). However, this method of operation allows for security issues such as wiretapping which will be discussed later.

The preferred method of network operations is known as a 'switched' network. A switched network operates by creating separate channels between each of the communicating devices. No device can monitor traffic meant for another device. Switched networks utilize devices such as routers and switches.

7.5.2.1 Firewall

A firewall is a logical (e.g., software application) or physical device which is designed to enable a system owner to set rules to restrict access to another device, software application, system or network. Firewalls are often used to guard the perimeter of a network and protect the internal network against external security risks. It is important to note that security risks also exist within the agency network which requires that additional perimeters be implemented, including that between the central servers (ACC, RCH, etc.) and all other nodes. Each of these perimeters must be protected in order to minimize security risks; however, the type and level of protection will vary.

— Packet Filtering Firewall:

The most basic type of network firewall is known as a Packet Filtering firewall. This firewall works by examining basic header information from the data packets that flow through the firewall. A packet filtering firewall is able to distinguish between the source address (where a packet came from), destination address (where a packet is going to), port (what 'service' a packet is attempting to access, and protocol (what 'type' of data the packet contains). The firewall is then able to allow or deny network traffic based on combinations of the selected criteria. For instance, a firewall could be configured to deny all traffic which is attempting to use file transfer protocol (FTP) service, or it could allow all traffic attempting to use the hypertext transfer protocol (HTTP) service. A firewall could be configured to allow all outgoing traffic from the network to any valid address (internal or on the internet) or it could be configured to deny all incoming traffic from the Internet except for particular third party vendors. The firewall provides flexibility in what combinations of rules are allowed in terms of allowing and denying network access, however this flexibility also allows a firewall to be improperly configured rendering it useless. In addition, packet-filtering firewalls while inexpensive and easy to implement, are not capable of catching sophisticated attacks.

— Application Level Gateways:

Application level gateways (a.k.a. Proxy Servers) are a more advanced type of firewall which examines the contents of packets and determines if the traffic is appropriate. The use of a proxy server allows for the actual destination machine (typically the protected servers) to remain hidden behind the firewall. All connections are made to the proxy server which then creates a connection to the protected server behind the firewall on behalf of the client machine. The proxy is responsible for forwarding all allowable traffic to and from the protected server.

NOTE— To increase system security, the central servers (ACC, RCH and other critical systems) should be protected with additional firewalls above and beyond the agency firewalls which may already be in place. This additional layer of protection provides safety from internal attacks as well as offering a failsafe in case the primary firewalls fail. Due to the increase in potential network hazards, as well as the decrease in software pricing, it is also suggested that personal firewall software be installed on each client PC within the system to further minimize security risks.

7.5.3 Protection of Data Channel

7.5.3.1 Encryption

The data channel can be protected by the use of encryption. An example of an encrypted data channel is Secure Sockets Layer (SSL) which is often used for secure web servers (URLs beginning with HTTPS denote a secure channel). Another form of an encrypted data channel is the virtual private network (VPN), which will be discussed later. In certain cases, data may be sent on an unencrypted channel, but may utilize an encrypted MAC as a form of authenticating the data. This is discussed later within this document.

7.5.3.2 Tunnels

Tunneling is the practice of using one protocol to carry traffic which uses another protocol. This is often used to bypass certain restrictions and/or configuration issues, and, unfortunately, security measures as well. For instance, it is common to tunnel unauthorized protocols/ports such as telnet traffic over an 'allowed' protocol/port such as HTTP to bypass a firewall. The use of tunneling can also be used to make a system more secure by forcing an insecure protocol to go through the same protections as a more secure protocol. One method of doing this is the usage of SSL to wrap an insecure protocol such as simple mail transfer protocol (SMTP). Other methods include tunneling of protocols over a secure shell (ssh) connection. For instance the secure copy command (a replacement for the insecure FTP command) works over an ssh tunnel.

7.5.3.3 Virtual Private Networks (VPN)

A virtual private network (VPN) is a dedicated connection between two points where all data is sent via an encrypted data channel. VPNs are often used to allow connections to a secure network via an unsecured network since encrypted messages sent over the VPN cannot be compromised via standard wiretapping techniques. The implementation of a VPN will require the purchase of network hardware as well as the installation of client software on the equipment authorized to use the VPN. A VPN is not fail safe, however, since it can still be compromised if either end of the VPN link (e.g., the client machine) is compromised.

7.5.3.4 Message Authentication Code (MAC)

As discussed earlier in this document, the use of a MAC is a method of verifying the authenticity of data by using encryption techniques to generate and append a mathematical value to any message. Since the calculation of the MAC is performed using a secret key and unique pieces of information associated with the message, only an entity with the secret key can verify that the MAC is valid and thereby confirm that the message has not been altered after it was sent by the originating system component. By combining the use of MACs (to confirm that the data was received in an unaltered state) and message acknowledgements (another type of tool that is useful in data communications to confirm that the data was received by the proper device), the network domain can increase the security of its message and data transfers.

7.5.3.5 Routing of Network Traffic

Routers are a critical link in any network as they determine how and if traffic from any point A will get to any point B. Routers pose a security risk in that if they are compromised, they can be used to redirect traffic to unauthorized users, deny traffic to authorized systems, and/or compromise the integrity of the data on the network among other things. Accordingly, routers must be afforded physical and logical protections as described below to prevent unauthorized access. Note that many servers also have some routing functionality and these protections should be applied to servers when applicable.

— Route Filtering and Authentication:

  The use of route filtering and routing authentication allows routers to determine which devices can update the router's information as well as authenticate the information which a router receives from authorized routing devices. This is extremely critical as an attacker can easily compromise an unprotected system by feeding false information to the system's routers. Route filtering allows the router to specify a list of which devices are allowed to send it routing information. All information sent from unauthorized devices is rejected. Routing authentication works by encrypting certain header information (using Message Digest Algorithm 5 -MD5) from the routing messages and adding it back into the message which is then sent out. The router receiving the information then authenticates it by decrypting the authentication information using a shared key which only the authorized routers know.

— Disabling of IP Directed Broadcast Function:

The IP directed broadcast function allows a packet to be sent to the special purpose 'network address' or 'network subnet address' of a network segment. Depending on how the network is configured, improper use of this function could result in all devices on that network segment sending a response to the specified address (which is typically 'spoofed' and not the actual address of the sending device). The result is a flood of traffic being sent to an address which could overwhelm the target device and prevent access to the resources at that address (e.g., a Denial of Service attack). IP directed broadcast features should be disabled to minimize risk.

— Disabling of IP Source Routing Function:

IP source routing allows a packet to specify the route it will use to get to a destination. This is often used to bypass the network's security as well as to attempt to probe the network for vulnerabilities. IP source routing should be disabled in the network to improve system security.

— Other Considerations:

Other things to consider in securing routers include the disabling of unnecessary protocols to minimize potential risks. Popular protocols include, Transmission Control Protocol/Internet Protocol (TCP/IP), NetBIOS, Windows Internet naming service (WINS), Internetwork Packet Exchange (IPX), Internet Control Message Protocol (ICMP), etc., however, all protocols are not needed by all systems. Many attacks use improperly configured routers and/or firewalls to attack a system, for instance ICMP (used by ping and traceroute commands) is often used to compromise systems.

7.5.3.6 Wiretapping

Wiretapping is a form of eavesdropping on the system's network. The most common forms of wiretapping are known as 'snooping' and 'spoofing'. It is also important to note that wiretapping methods are easily used against 'wireless' networks and communications as well.

— Spoofing:

Spoofing is the forging of information, such as replacing an invalid network address in a message with a valid address or the forging of a user name or system name. Spoofing is typically used to alter an unauthorized transaction so that it appears as a transaction authorized to use a particular service. A related attack is the 'phishing' attack described earlier in that it 'appears' to be from a legitimate source (e.g., your bank) in order to gain access to resources (e.g., your account information). Spoofing can be minimized by using properly configured routers and firewall equipment.

— Snooping:

Snooping (also known as 'sniffing') is the process of monitoring the traffic that flows across a network. Snooping is typically used to capture information such as user names, passwords, security keys and other sensitive information. The captured information can then be used to gain unauthorized access to system resources and/or to launch attacks against other systems/resources. Snooping is most common on 'promiscuous' mode networks since the device doing the snooping must physically be on the same network segment as the traffic being snooped. This problem can be minimized by avoiding 'promiscuous' networks and instead using a switch based network.

NOTE□In the case of wireless local area networks (WLANs) there are no physical protections between the access point and connecting devices so it is still possible to snoop traffic via the wireless access point.

7.5.4 Remote Administration and Third Party Access

Remote administration is the ability to administer equipment without physically being at that piece of equipment, this is usually performed via dial-up lines or via the network. This form of administration is often required in today's systems which often include increasing numbers of network and server hardware components and the desire to minimize the need for personnel to be physically at a site in order to perform system checks or adjustments. Since this form of administration facilitates access to equipment without being physically present with the devices, remote administration opens up potential security risks, especially if this option is not properly implemented. There are certain basic principles which should be followed to minimize security breaches when using remote administration.

First and foremost it must be determined if the risks involved with remote administration are critical enough to justify implementing it on a particular server. It defeats the purpose of implementing strong physical security if these measures are bypassed with weak network security.

The type of remote access must also be determined. A dial-up line for instance would bypass potential problems with the network by allowing direct access to the equipment. Dial-up lines pose several additional issues such as the purchase of additional equipment (such as a RADIUS server for authenticating logins), additional server/equipment configuration, and whether options such as call-back (a feature which automatically calls the user's system when network facilities are available) should be implemented. Another form of remote access is 'remote consoles' which many vendors offer with their equipment. Remote consoles work via the network and provide the 'standard' console functions that would be available if the user were physically present at the equipment. Due to the potential security risks of using remote consoles (e.g., cleartext data channels), it would be best to place them on their own network segments. Remote access could also occur directly over the network without the use of any specialized equipment.

When using the network for remote administration it is critical to make sure that the best practices are followed since sensitive information exchanges occur while doing administration (e.g., root passwords, system configuration information, key information, etc.). These practices include the elimination of any cleartext passwords as well as avoiding cleartext data channels when possible. It is also important to make sure the latest protocols are being utilized, for instance, older versions of the Simple Network Management Protocol (SNMP) sent 'community string' information (i.e., password information) in the clear while newer versions of SNMP encrypt this information. The most secure option presently available would be the use of virtual local area networks (VLANs) for the data channel. Also, the access to remote administration functions should be restricted to personnel that have a clear need for this capability and further restricted by limiting access to only those channels that are to be used by the authorized individual. For instance, many vendors allow for the restriction of which network addresses are allowed to access management features. These options should be enabled whenever possible.

7.6 Data Domain

The data domain is comprised of the database applications used within the regional system, all related elements such as report writers and archives and all of the data elements stored within the regional database or in receipt from or prepared for distribution to any of the end devices. As the database contains all of the accumulated data from the entire system, it represents the primary source for fraud checking, funds settlement and clearing, activity reporting and system auditing. Accordingly, the data domain is a resource which must be secured. Properly securing the physical and network domains (through which the data must be generated and transferred) is a key aspect that leads to protecting the data domain. There are a few additional security considerations specifically designed to address the protections of the data domain.

7.6.1 Authorization and Authentication

Just as in the other domains, authorization and authentication are critical components of security for the data domain. The determination of the level of data access to be provided to any single system user is among the most critical decisions for any system security administrator. As a general rule, each user's access to data should be restricted to the components of the data domain that are needed by the individual to perform the system tasks that are assigned to him or her. As an example, if a user is responsible for the creation of maintenance reports, that individual should only have read access to the maintenance related data in the database and nothing more. System design for the data domain should facilitate the flexible assignment of varying levels of access to data and each assignment should be carefully evaluated to ensure that access rights of all users are consistent with their job responsibilities.

Normally, data access functions are dictated by the database software, but the Operating System, Report Writers and Data Persistence should also be considered when establishing an overall plan for security of the data domain for the regional clearinghouse.

7.6.1.1 Operating System (OS)

Permissions for all database related files and resources must be configured to ensure that OS functions cannot be used to bypass the security features of the database application.

7.6.1.2 Report Writers

Many report writers (software applications that are used to automate retrieval from the database and formatting of the data elements into a report form) also offer additional levels of access rights which can be used to supplement the database security; some even provide a separate report writer server for this function. Although these rights are meant to improve security, a badly configured report writer in conjunction with an improperly configured database could result in unauthorized access and/or tampering of data.

7.6.1.3 Data Persistence

Data persistence is data that is still available within a system component after all processes have completed to prepare and transfer that data to the RCH or another system device. This data, examples of which are listed below, can be extracted and potentially used to facilitate fraudulent activities.

- Database Archives:

  Data, which is archived to tape, disk, or other media is available to anyone who has access to that media. An attacker that gains access to the media can view the data by loading the media into another system, bypassing all of the security measures in place to protect the database. Accordingly, data archives should be afforded the same levels of protection as other portions of the data domain. Physical access to archives should be restricted to authorized users and processes should be in place to record all access to the archives. Highly sensitive data archives should also be encrypted and/or password protected to prevent the media from being loaded on unauthorized systems.

- Disk Cache:

  OS level disk caches are maintained by the OS and act as virtual memory allowing the system to load more applications and data than the amount of physical memory would normally allow.

  Disk cache may also be maintained by an application such as a database or web browser and is often used to increase system performance. Many of the applications which are used to perform everyday system functions, from report writers to system administration will use disk cache in some form or another. Web browsers typically store data in the disk cache as it is faster than reloading the data via the network. The data contained in the cache could include graphics, text or even password data. This data can remain in the cache even after the application terminates. Since this information can be viewed by an attacker to gain knowledge of sensitive information, security measures should be in place within the OS and within any relevant application to limit access to disk caches to authorized personnel and to record all accesses.

- Cookies:

  Another form of data persistence is a 'cookie', hidden data files which an application saves to disk containing information which that application needs at a later time. One of the applications that commonly use cookies is the web browser, which creates cookies for its own purposes and/or allows external applications to implant cookies within the system memory. The use of cookie blocking software can help reduce the associated risks and prevent unnecessary cookies from accumulating within the system. Web browsers can further mitigate the use of cookies by encrypting sensitive data and passing it in encrypted form during the transaction processing functions.

7.6.2 Other Attacks

7.6.2.1 Data Injection

This form of attack is the use of specially constructed data input to manipulate an authorized application into performing unauthorized actions on the database. For example, a web browser may prompt a user to input user name and password information in order to authenticate a user to certain services. Without proper security protections, an attacker can force a poorly written browser script into providing unauthorized access by feeding an actual command via the user name or password input fields. As an example, an attacker might input a data retrieval command in the user name field, causing the database application to obtain and display the data, despite the lack of user authorization/authentication.

Protection against data injection includes implementing high levels of authentication and making sure that users (and applications) only have access rights to the data they actually need as described above. If a user or application doesn't have write access to critical tables, then they cannot alter the data and/or view sensitive information. In addition, applications should be well coded and should validate all input fields to screen out 'invalid' data to prevent data injection (as well as data corruption in general).

7.6.2.2 Data Interception and Manipulation

This is a form of attack whereby authentic data in transit between system components is obtained by an attacker, modified to benefit the attacker and then re-transmitted to the appropriate receiving component. As an example, an unscrupulous merchant might initiate the transfer of PICC load transactions to the RCH but would, instead, capture the output in a personal computer, delete selected transactions in order to reduce the amount the merchant owes and then transmit the altered file to the RCH.

As described in Section 5 of this document, the use of a message authentication coding process provides the most effective means to prevent this form of attack since it ensures the RCH (or other system component) that a received file has not been altered since being transmitted. In addition, regional system owners should implement device authentication processes whereby the sending and receiving components offer a “challenge” to the other device and must receive an appropriate “response” before file transfer can occur. This approach is particularly needed when the transfer is facilitated over any public network (such as a dial-up phone line, wireless system or the Internet).

Annex A

(informative)

A.1 Definitions

A

Access control/Authorization: Protection against unauthorized operations on information or processes in the system. Process giving individuals access to system objects based on their identity.

Algorithm: A specific set of mathematical functions used to perform encryption processes.

Asymmetric: A method of encryption also commonly referred to as public key infrastructure (or "PKI") that utilizes a matched pair of keys. The first key is known as the public key and the second is known as the private key. The public key (which is made available through PKI services or provided by the recipient of information) is used to encrypt a file or data element. The recipient uses his or her private key to decrypt the information. ECC, RSA and DSA are examples of asymmetric schemes.

asymmetric key: A security scheme using two keys: one key is public; one key is private. Commonly used in public key security schemes where one key, the public key used for encryption is published along with the owner's identification and the second key used for decryption is kept private by the owner.

Authentication: A process of proving the identity of a document, message, data element, computer or a computer user.

B

back door: A means of defeating or bypassing a security system or accessing data through a given mechanism used to breach built-in security.

C

Certificate: Encrypted codes that are generated using random numbers, card serial numbers, and transaction numbers. It is used to authenticate a process, for instance, to authorize the offline crediting of e-cash and/or points to a cardholder card. See also, **Authorization certificate** and **Verification certificate**.

Chip: A small piece of semi-conductive material, usually silicon, that contains miniaturized electronic circuits.

chip initialization: Manufacturer process to set the configuration options, the transport key and the chip serial number.

CID: Card Interface Device. A contactless smart card reader containing both the PCD and the application hosting processor to provide communications and application processing between the PICC and the backend system.

CISP: Cardholder Information Security Program. A set of requirements defined and published by the card associations (Visa and MasterCard) for the security of information relating to bankcards and bankcardholders. All organizations that process or stored information relating to cards that bear the associations' brands are required to adhere to the CISP requirements and must pass a formal audit to confirm compliance.

Cipher Block Chaining (CBC): Cryptographically connecting a block of ciphertext to the next plaintext block.

Ciphertext: A phrase used to describe data or information that has been encrypted to make it unreadable without decryption.

Cleartext: See **Plaintext**

Confidentiality: The act of preventing the disclosure of secret information to non-authenticated individuals, parties and/or processes.

cryptographic keys: Digital values used by encryption algorithms to convert plaintext to ciphertext.

D

Data Encryption Standard (DES): The National Institute for Standards and Technology‘s most widely accepted public-domain symmetric key cryptographic algorithm. DES is accepted by the banking industry and others for the encryption/decryption of data and PIN security. DES is based on a published algorithm with secret keys.

derived keys: The value resulting from DES encrypting a smart card serial number sequentially three times with the three keys on the master verification key set.

Differential Fault Analysis (DFA): Method of breaking an encryption scheme by subjecting the computer chip to physical stress and measuring the change in its behavior.

Differential Power Analysis (DPA): Method of breaking an encryption scheme by monitoring and measuring the power signals emitted from a computer chip.

digital signature: A counterfeit-proof, unique method of identifying an entity based on the cryptographic results of DES operations. It is used after a transaction has completed, during automated audit analysis, and during fraud analysis.

Dual Control: A method of maintaining security and reducing risk whereby two (or more) individuals must be present while performing a specific task, such as counting currency etc.

E

Eavesdropping: Act of illegally listening in on a communication between two other parties, systems or system components.

encryption: The use of ciphers to alter data, such as a PIN, before it is transmitted over a network, to ensure that the messages cannot be read during transmission and subsequently used. The data is converted from plaintext to ciphertext using cryptographic keys and a specific algorithm, such as the DES algorithm.

F

File Transfer Protocol (FTP): A mechanism for transferring files from one computer to another, often across a network or via a modem

FIPS: Federal Information Processing Standard. Standards published by the US National Institute for Standards and Technologies (NIST) which are used as guidelines for Federal procurements.

firewall: A stringent security measure designed to protect a network from unauthorized access. In general, a local network is connected to the outside world by a "gateway" processor. This gateway processor does not let unauthorized TCP/IP packets pass from inside to outside and vice versa.

fraud detection: Determining the authenticity and consistency of collected batches, missing or duplicate batches, signatures, transaction numbers, and exception-listed devices or stored value cards. It also researches the cause of certain exceptions, identified locally or by subordinate notes of a network.

G

H

Hardware Security Module (HSM): (A physical device used for the purpose of securely storing encryption keys. Some HSMs provide the ability for one or more key custodians to manually enter values that become or are converted into encryption keys. Other HSMs have the ability to generate random values, negating the need for manual entry.

Hash: An encryption process that is used to convert plaintext (of any length) into a fixed length value (known as the hash value). This process is also known as a one way hash, compression function, contraction function, electronic fingerprint, etc. A hash is typically appended to the plaintext by its originator to provide the means for the recipient to confirm (by repeating the hash process) that the plaintext has not been altered from its original form.

HTTP: Hyper Text Transfer Protocol; the protocol used on the world wide web (Internet) that performs the request and retrieve functions of a server. Commonly seen as the first part of a website address.

HTTPS: HTTP over a secure socket layer (SSL) transmission link.

hot card: The hot card status may be modified to deny transactions and eventually physically capture the card. This is a smart card that has been lost, stolen or misused. A smart card's status is managed by the organization which issues and owns the card. The card may also be referred to as a "hotlisted" card.

hotlist: A list of smart cards that are designated to be inhibited from being used or activated.

I

Identification and Authentication (I&A): The portion of the TCSEC requirements that addresses the

means by which an individual is identified to the trusted system and authenticates their actions.

Integrity: Condition existing when data is unchanged and remains in the original state defined or created at its source.

Irreversible Memory: For purposes of this document, this term refers to the use of Read-Only Memory (ROM). This form of memory is used to permanently record data within a smart card microchip. Once recorded, access to that portion of memory is permanently blocked, allowing the information to be read but preventing the reuse of that segment of memory.

J

K

Kernel: Modern operating systems are built in "layers." Each layer has different function such as serial port access, disk access, memory management, or providing a user interface. The base layer, or the foundation of the operating system, is called the kernel. The kernel provides the most basic "low-level" services, such as the hardware-software interaction and memory management. The more efficient the kernel is, the more efficiently the operating system will run.

Key: An alphanumeric value that is used within an algorithm to perform encryption processes and, since the value can be kept secret, to make public algorithms secure.

key card: A smart card that is used to securely store and transport the symmetrical (DES) keys between the key generation process and the batch personalization process.

Key Custodian: Individual responsible for one or more encryption keys or a portion of such keys. A key custodian may be responsible for creating the key or his portion of a key and / or may be responsible for holding a copy of the key/portion of a key in a paper or electronic form.

Key Encrypting Key: See **Master Key**

Key Generation: The process used to create the key used for encryption processes with the algorithm.

Key Generation Terminal (KGT): Device used to generate random values that can be used as encryption keys. A KGT may include an HSM for storage of the generated values or a KGT transfer the generated values into an HSM.

Key Injection: Process of securely loading a key into the memory of a device that will use the key to perform encryption processes.

Key Length: The number of bits or bytes utilized by a key when presented in a digital format.

Key management: The trusted system that retains the inventory of Issuing Modules, provides access to the Issuing Module vault, and keeps continuous logs of all activities related to the Issuing Modules. The life cycle management for security keys containing 5 functions.

- **Key Generation:** The process of creating a secure set of keys;
- **Key Storage:** The process of securely storing keys for later use. Key escrow is the process of storing spare key sets in a secure location;
- **Key Distribution:** The process of getting keys into the devices that are going to use them;
- **Key Usage:** The control of the use of the key in the end-point devices;
- **Key Destruction:** The secure process of retiring keys that are in use.

keys: Secret codes that are used by the encryption and decryption functions. A key is a parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment, or decipherment. “Interrelated keys” share a parameter created by an algorithm designed for this purpose. When the same value is used to control encryption, it is referred to as a “private key.” When a pair of different values is used to control a related process, it is referred to as a “public key.” A unique key generated for each session is called a "session key.”

L

M

Master Key: A term generally used to refer to the key that is used to encrypt other keys so that these other keys can be securely distributed. In this context, the Master Key may also be referred to as a key encrypting key. In a diversified key system, this term may be used to describe the base key that is combined with PICC or CID specific elements to generate all other (diversified) keys.

master keys: The cryptographic keys contained in Issuing Modules for use in initialization and those contained in Security Modules for use in cross-verification and other functions. The cardholder smart card contains keys that are derived from the master keys.

message authentication: A network security technique used to protect critical transaction information by developing a message authentication code based on the actual transaction data. An algorithm generates the code, which is included with the transaction message so that the message receiver can verify the data has not been altered fraudulently during transmission or processing. See **Message Authentication Code**.

Message Authentication Code (MAC): A hash function that utilizes a key to enable the originator and recipient of plaintext to use a public algorithm to generate a hash to confirm the unaltered state of the plaintext.

mutual authentication: A form of authentication wherein two parties or systems involved in an exchange of data can first confirm the identity of the other party/system.

N

Non-repudiation: Condition wherein the integrity of data can be confirmed and, therefore, its validity cannot be challenged.

O

Operating System (OS): The software that communicates with computer hardware on the most basic level. Without an operating system, no software programs can run. The OS allocates memory, processes tasks, accesses disks and peripherals, and serves as the primary user interface. With an operating system, like Windows, the Mac OS, or Linux, developers can write code using a standard programming interface (known as an API).

P

password: A code which is a product of a DES standard for encryption/decryption of data and PIN security. Also, a user password is the normal ID password mechanism for login security.

Patriot Act: Federal law with many aspects designed to curb terrorist activities which impacts almost all forms of real estate, financial transactions and financial accounts..

PCD: Proximity Coupling Device. Term used within the ISO/IEC 14443 standard to refer to a contactless smart card reader.

PICC: Proximity Integrated Circuit Card. Term used within ISO/IEC 14443 to refer to a contactless smart card.

Plaintext: Information that is readily readable or usable by someone before it is encrypted and converted through an encryption algorithm and cryptographic key into ciphertext (see also). Also referred to as "cleartext."

Privacy: The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed.

Q

R

RADIUS Server: A server that is responsible for receiving user connection requests, authenticating the user, and then returning all of the configuration information necessary for the client to deliver the service to the user. Its primary use is for Internet Service Providers, though it may as well be used on any network that needs a centralized authentication and/or accounting service for its workstations.

RAM: Random Access Memory. The most common computer memory which can be used by programs to perform necessary tasks while the computer is on; an integrated circuit memory chip allows information to be stored or accessed in any order and all storage locations are equally accessible.

RSA: A common, commercial public-key encryption technology that uses an algorithm developed by RSA Data Security, Inc.

S

Secure Application Module (SAM): Smart cards which are the basis for device security in a network. They are designed to facilitate the distribution of keys and security-related functionality, which control the execution of transaction processes.

Secure Hypertext Transfer Protocol (S-HTTP or HTTPS): This is a Web protocol that encrypts and decrypts user page requests and pages that are returned by the Web servers. Not all Web browsers and servers support HTTPS. It is often used in conjunction with Secure Sockets Layer (SSL).

secure session: Interactions between two devices after cross-verification determines whether the devices are authorized to perform the interactions and to what extent.

Secure Sockets Layer (SSL): A technology designed to establish a secure connection between two computers through data encryption.

security certificates: These are the cryptographic results of DES operations that are used during a secure transaction.

security domain: A collection of entities to which applies a single security policy executed by a single authority.

security level: A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection.

security policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

security threat: A potential violation of security.

Security Server: A tamper resistant device, specifically designed to provide secure cryptographic functionality. Security Servers are used in conjunction with Back-End Modules to provide secure storage of keys, high-speed verification of transaction signatures, and other related cryptographic functions.

Simple Power Analysis (SPA): Method of breaking an encryption scheme by measuring the power utilization of a computer chip when encryption processes are being performed.

Single DES: A security scheme that used one DES key and one DES function. Single DES is no longer considered secure enough for smart card implementations.

signature: Encrypted codes created by both the cardholder's smart card and security module and appended to transactions to provide unique audit trail logs.

simple mail transfer protocol (SMTP): A protocol for sending electronic mail messages between computers.

Symmetric: A method of encryption that uses a single key that is also referred to as single or secret key cryptography. In a symmetric encryption scheme, the key must be shared between the parties that will exchange information. DES and Triple DES are examples of symmetric key encryption schemes.

symmetric key: Also known as a "private" or "secret" key. A single key is used to encrypt and decrypt data.

T

Transport Key: Term used occasionally to refer to a key that is used exclusively to encrypt other keys while they are being distributed to authorized key users. See **Master Key**. This term is also used to describe the temporary key used by a PICC manufacturer to enable injection of permanent keys by a regional program owner.

Triple DES (3DES): A security scheme based on DES that uses two or three DES keys and three DES functions to perform a secure function. The use of triple DES security schemes are recommended in current smart card systems.

Trusted Computer System Evaluation Criteria (TCSEC): Also known as the "Orange Book," this document is published by the Department of Defense and describes the evaluation criteria used to assess the level of trust that can be placed in a particular computer system.

Trusted Computing Base (TCB): All of the protection mechanisms (hardware, software, firmware) within a computer system that, in combination, are responsible for enforcing a security policy.

U

V

Velocity Count: A count (or amount) that is retained for a card or account by a switch, processing system or other host in order to limit the amount of activity in a given period of time. It is a way of limiting the effects of possible fraud.

W

X

A.2 Acronyms and Abbreviations

ACC	Agency Central Computer
ACH	Automated Clearing House
ACK	Acknowledge
ASN-1	Abstract Syntax Notation One
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
ATM	Automated Teller Machine
ATR	Answer To Reset
CCRA	Common Criteria Recognition Arrangement
CID	Card Interface Device
CISP	Cardholder Information Security Program
COS	Card Operating System
CPU	Central Processing Unit
DAC	Data Authentication Code
DES	Data Encryption Standard

DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IPX	Internetwork Packet Exchange
LAN	Local Area Network
MAC	Message Authentication Code
MULTOS	Multiple Operating System
OS	Operating System
PCD	Proximity Coupling Device
PIN	Personal Identification Number
RAM	Random Access Memory
RCH	Regional Clearing House
ROM	Read Only Memory
SAM	Security Access Module
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
Ssh	Secure shell Connection
SSL	Secure Sockets Layer
SPA	Simple Power Analysis
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
3DES	Triple Data Encryption Standard
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

WINS	Windows Internet Naming Service

SECURITY TERMS (Refer to official APTA Glossary for a comprehensive list of acronyms, terms and phrases used in this document).