Contactless Fare Media System Standard

Part I – Introduction and Overview

(APTA IT-UTFS-S-001-07)

Version 1.0
January 27, 2007

Note: Document renumbered March 2013, previously referenced as APTA S-UTFS-WP0-001-07. No content was changed.

Prepared by members of the Work Package – 0 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 standard for public release on January 27, 2007.

Director, Technical Services
1666 K Street, NW, Washington, DC 20006-1215, USA

Abstract: This standard is an introduction and overview to a contactless fare media system standard which provides for a consistent and uniform method for storing and retrieving information from smart cards used in transit applications. The standard consists of 5 parts which are designed to be implemented together as part of a foundation for end-to-end integration of fare collection information processing.

Keywords: fare collection, media, public transportation, transit and smart card

Introduction

(This Introduction is not part of the APTA IT-UTFS-S-001-07.)

This Standard is part I (Part I) of a suite of standards that together form the Contactless Fare Media System Standard (Standard). This and other parts of the Standard include the following:

- 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 designed to be implemented together as part of a foundation for end-to-end integration of fare collection information processing to best provide interoperable systems within a region. Detailed descriptions of all the parts of the Standard can be found herein 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, as implemented by rail transit systems, may be either more or less restrictive than those given in this document.

The intent of this Part I of the Standard is to provide an introduction to the Standard and its various components and concepts. 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, security and operating rules, interoperability with other compliant systems may be achieved.

Document Development Process

Development of this Standard and its parts was guided by the APTA Universal Transit Fare System (UTFS) Task Force. 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.

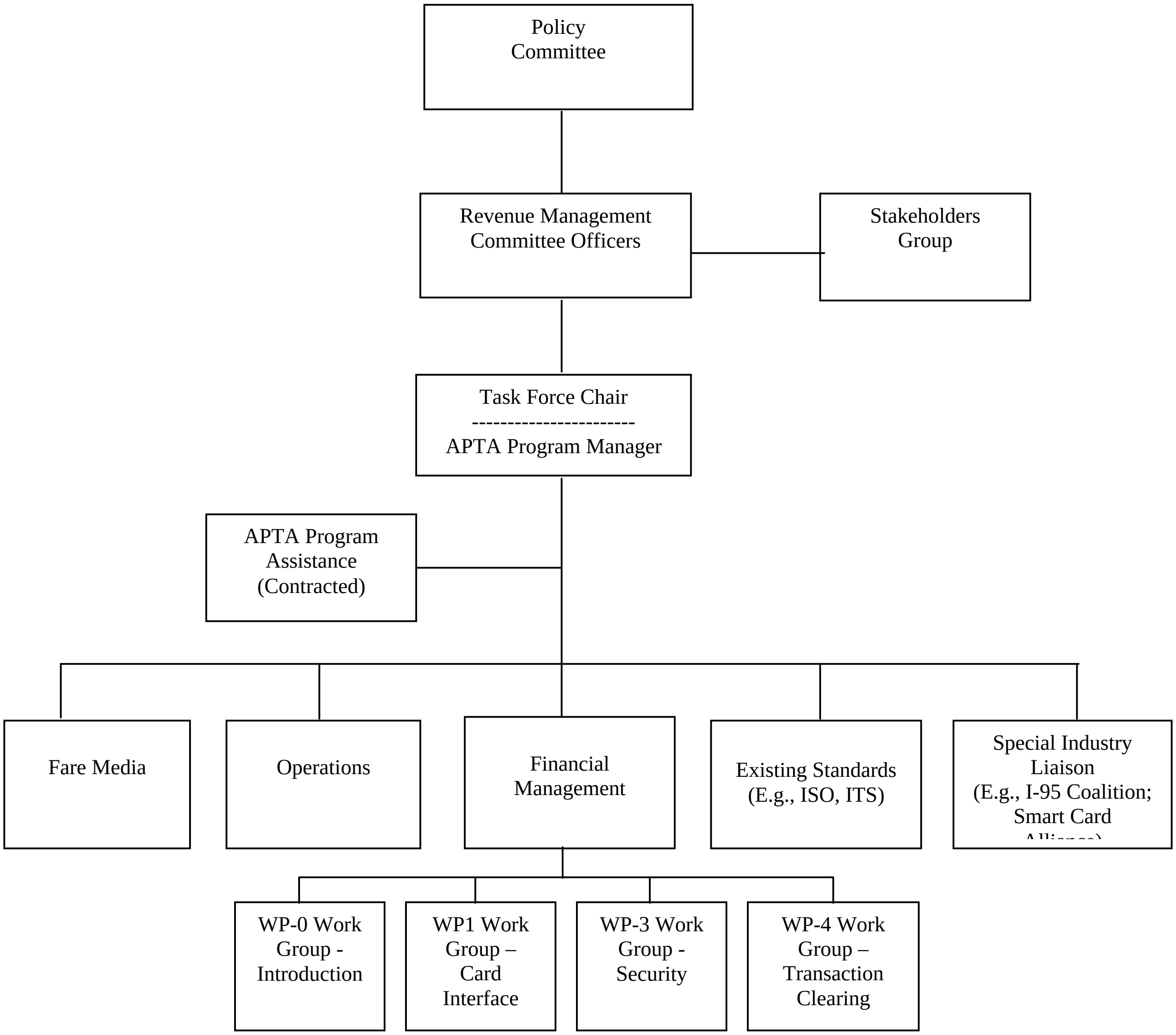
Applying these guidelines and relying on a broadly consensus driven decision process has produced this important industry-based standard.

To be successful, any consensus process involving organizations with diverse interests must have rules defining the procedures to be used. APTA developed 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, recommend 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; Smart Card 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 sixty of at least (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 approval process for documents to become a standard follows the flowchart depicted in Figure (*ii*) as documented in the APTA UTFS 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.

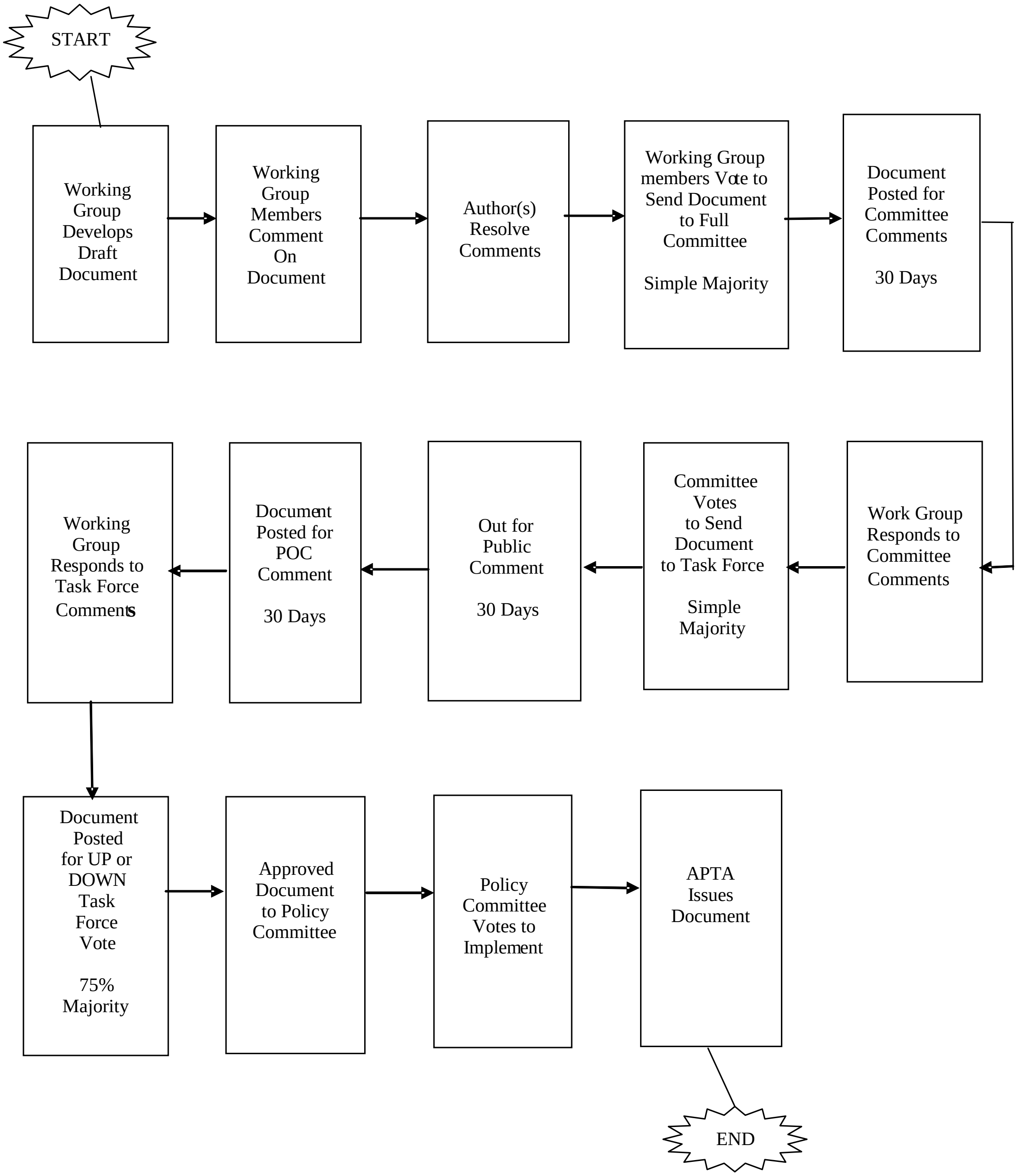

START
Working Group Develops Draft Document
Working Group Members Comment On Document
Author(s) Resolve Comments
Working Group members Vote to Send Document to Full Committee
Simple Majority
Document Posted for Committee Comments
30 Days
Work Group Responds to Committee Comments
Committee Votes to Send 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 and those using the Standard from copyright and patent infringements, the UTFS Task Force implements an Intellectual Property Policy. The inclusion of intellectual property provisions addressing patents, copyrights or trademarks is in accordance with APTA's Universal Transit Fare System Standard 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 Fare System Standard 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/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

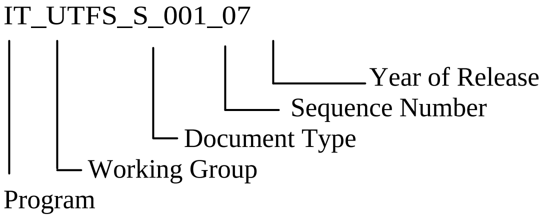
b) The document is tutorial in nature, or

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, 11th Floor
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. As of the date of this publication, no patents or copyrights essential to this Standard were claimed or made known to APTA.

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 Standard.

Brian Monk
Robert Murray
Tomas Oliva
Sigmond Rosenthal
Brian Stein
Richard Stern

At the time this Standard was completed, the Work Package 0 Group responsible for the major development of this Standard included the following membership:

Tomas Oliva, C*hair*

Work Package – 0

David McIlwraith
Brian Monk
Robert Murray
Tomas Oliva
Tom Parker
Sigmund Rosenthal
Martin Schroeder *
Brian Stein
Richard Stern
Timothy Weisenberger *

Martin P. Schroeder, P.E.*
APTA Staff Advisor

* Non-voting member

APTA would also like to acknowledge and thank the following organizations for contributing staff and other resources to this standards development effort:

Booz Allen Hamilton, Inc.
Cubic Transportation Systems, Inc.
Murray Associates
San Francisco Bay Area Rapid Transit District
Scheidt & Bachmann USA, Inc.
Tri-County Metropolitan Transportation District of Oregon
Washington Metropolitan Area Transit Authority

APTA acknowledges the generous support of Robert Bernard and the Port Authority of New York & New Jersey for development of the Regional Interoperability Standard for Electronic Transit Fare Payments© (RIS)© on which this APTA Standard has been based.

APTA acknowledges the U.S. Federal Transit Administration and the Joint Program Office of the U.S. Department of Transportation who were instrumental in supporting and guiding this program.

Disclaimer

The American Public Transportation Association (APTA) developed this guideline in consultation with a diverse group of experts, arriving at consensus positions. APTA strives to provide accurate, complete, and useful information. The information contained in this detailed guideline is based upon technical information that is believed to be reliable, but for which no responsibility is assumed. Neither APTA nor any person or organization contributing to the preparation of this document makes any warranty, expressed or implied, with respect to the usefulness or effectiveness of any information, method or process disclosed in this material. Nor does APTA assume any liability for the use of, or for damages arising from the use of, any information, methods, or process disclosed in this document. No information or suggestions shall be deemed to be a recommendation to use any specific manufacturer's product(s) or any system in conflict with an existing patent right, code or regulations. This document should not serve as a substitute for sound engineering judgment.

CONTENTS

PART I – Introduction and Overview

1. Overview

This document is Part I of a data standard for transit fare collection systems which consists of the following:

- 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 - System Security Planning and Implementation Guidelines (Part IV)
- Part V - Compliance Certification and Testing Standard (Part V)

These parts together complete the larger standard entitled, Contactless Fare Media System Standard (Standard). The parts of the Standard noted above are designed to be implemented together as part of a foundation for end-to-end integration of fare collection information processing to best provide an interoperable system. Detailed descriptions of all the parts of the Standard can be found herein as well as within the introduction sections of each part.

1.1 Scope

The Standard defines the following:

- The specification for components of the data architecture to be used on a Proximity Integrated Circuit Card (PICC) which forms the foundation for the system.
- The messages between the Regional Central System (RCS) and the Agency Central Computer or sub-system controller.
- The certification and testing criteria necessary to verify that software or hardware is compliant with the Standard.
- Recommendations (informative only) for system security.
- This Standard applies to contactless fare collection systems where two or more transit agencies share a common PICC and one or more common fare products for fare payment.

However, the Standard can also be applied to single agency systems where the agency desires to implement a system that is based on industry accepted design principles and which might at some point become part of a regional system.

For interoperability, there must be appropriate interagency agreements in place in the geographic region. Once such agreements are in place, cards and readers must comply with the Standard, and a regional "enforcement" mechanism is required to assure consistency in the application of the Standard.

1.2 Purpose

The purpose of this Part 1 of the Standard is to provide a high level description of the all parts of the Standard and to define the key components of a contactless fare media system as well as the major roles and functions the system must accommodate.

1.3 Exclusions

This Standard does not:

- Provide specifications or guidance for the use of Limited Use Cards or other cards not compliant with the Standard.
- Address fare structures where multiple agencies in a region have no common fare product or regional entity to coordinate fare activities.
- Prescribe specific Automatic Fare Collection (AFC) implementations, computer system types, CID types, PICC types, implementation methods, nor operational procedures.
- Provide specifications defining a specific system architecture.
- Provide specifications defining a specific scale of system architecture.
- Provide definitions defining a specific system design.
- Provide Point of Sale (POS) acquisition, implementation, or management requirements.
- Provide messaging rules for non-AFC applications, such as physical or logical security access control.
- Provide specifications for multi application PICC management.
- Address system management.
- Define CID or other asset management techniques (beyond key management, data authentication, and certification of CID software).
- Prescribe security key management. However, Part II does offer guidelines and Part III allows for key loading and selection. Part IV offers guidelines for planning and implementation of a comprehensive security key management program.
- Define requirements for card manufacture, procurement, inventory, or distribution (which are performed by PICC Issuers using their own processes).
- Define procedures for procuring contactless media for use within a given system/region.
- Provide regional or agency specific fare policy.
- Prescribe an interface between the Regional Central System and the end devices.
- The functionality or implementation of any of the system components, including the Regional Central System.
- The inner workings of fare media vending machines, fare gates, fare boxes, central computer systems, garage computer systems, station concentrator systems, etc.

— Networking.

NOTE—The standard does not cover limited use or disposable PICCs. However, provisions have been made for the inclusion of such cards into the Standard at some point in the future. For example, Section III of the Standard describes limited use card messages, even though with this release of the Standard, they would not be used.

1.4 Introduction to the Standard

The Standard has been segmented into five logical parts. While intended to be implemented together, Parts II, III and IV are stand alone documents that may be used independently.

Part I of the standard is normative and is an introduction to the other four parts, describing the how, where and why on the use of the Standard. Questions on the ownership and licensing of the Standard are also answered in Part I. In addition Part I, combines the Abbreviations, Acronyms and Definitions used in the other four parts of the Standard. This common section provides consistency among the parts of the Standard while avoiding duplication and conflict among terms and definitions.

Part II of the standard is normative and defines the data format used on PICCs. The data format is intended for transit and does not embrace other applications such as commercial purchases, banking, and building or facility security. Part II provides a consistent and uniform method for storing, retrieving and updating data from contactless fare media used in transit applications. Part II also references related international standards which define the physical, electrical and communication aspects of PICCs. The data format described by Part II enables the design of data records that cover the known requirements of fare payment systems for public transit and associated private transit systems operating in the United States. Part II requires the use of full featured PICCS rather than limited use or disposable PICCs. While the PICC data format was developed primarily with the United States public transportation in mind, provisions have been included to include systems in other countries. These provisions include country codes and region codes. A future consideration of the PICC data format standards will be a subset of the data format adapted for use in limited use PICCs.

Part III is normative and describes uniform and consistent method for transit agency fare collection systems to communicate with a common Regional Central System (RCS), defining the necessary structure and components of the messages. The data sent to the RCS is the result of transactions such as boardings, purchases or other actions performed by PICCs. The data sent from the RCS to Agency Central Computer, Sub-system Controllers and other system components are control messages, PICC directives and system configuration data. Although Part III of the standard defines a comprehensive set of messages, it is unlikely that all messages will be used in one system. It is expected that a subset of messages will be selected, based upon the functions, fare products and business rules of the system being implemented. Additionally, the message definitions contain optional elements that are only used if applicable to the situation or system.

All systems which handle monetary transactions employ rigorous security controls, including those employing PICCs. However, because of the diversity of implementations, APTA did not seek uniform agreement on rigorous security standards for this release of the Standard. Thus, Part IV of the standard is not normative. Rather, it provides the reader with understanding of the terminology associated with security programs for fare collection systems and suggests the basic steps and considerations that should be employed in order to define, implement, and manage a security program for a regional PICC -based fare collection system. In order to ensure that Part IV addresses the needs of agencies and regional programs of all types and sizes, it uses relatively non-technical language and the specific guidelines are targeted toward achievement of a moderate level of security.

In order to ensure interoperability between disparate systems within a single regional fare payments program, the owners and 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. Items such as message authentication tools, e.g., which algorithm will be utilized by all parties; encryption and 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 and security rules development process. It should serve as a resource to identify and qualify the many security options which are available and which are necessary to protect the PICC related assets of a regional program. This document leaves the responsibility of developing a specification for an interoperable security plan to the participants of a regional program.

Part V is normative and defines the product submission requirements, test methods and procedures, test apparatus, and reports needed to test, confirm, and report conformance with the Standard. However, conformance is only one of several steps that might be undertaken to confirm a products suitability for use in a mass transit system. Other steps might include testing and evaluation to verify durability, fitness for purpose, system interoperability, compliance with procurement specification(s), or conformance to one or more other standards. Conformance testing, like the Standard itself, is not intended to eliminate the requirement for comprehensive procurement specifications or such additional testing.

1.5 Guidance on how to use the Standard

The intent of the Standard is to establish a level of commonality between two or more agency systems participating in a regional program for PICC -based fare payments. In other words, agencies who share PICCs based on the Standard should be equally able to read and exchange data.

The Standard can be used as a reference in the acquisition of equipment, goods, and services. By referencing the standard in Requests for Proposals and/or contracts, it is not necessary for each transit agency to develop their own PICC format and communication protocol. It is expected that, once suppliers have designed compliant systems, there will be more uniformity and therefore lower cost to the transit agency for non-recurring engineering.

It is not necessary for a transit agency to use all parts of the Standard. For example, Part II (the card format) has been developed to support a wide variety of fare structures, modes (rail, bus, etc.), and operating practices. It is unlikely that any one agency (or, for that matter, region) will use all of the features embodied in this standard. However, by using the Standard for the applicable tariffs, there is a strong assurance that the agencies in the region will have the flexibility to implement fare policies as their environments evolve, without endangering their common use of the PICC.

However, to assure interoperability, users must comply with the mandatory requirements of all Parts. For example (again using Part II), while particular product objects may not be filled, the Directory Index Object must be present as specified. It is possible to be non-compliant with mandatory parts of the Standard, but in that case the system will not be interoperable with other agencies’ and regions’ systems that are compliant with the Standard.

The Standards are presented in a consistent format. For example, Part II presents each object with a definition, detail on the structure of the object, then application notes and supplemental information. Part III uses a definition and table format for each message object.

Finally, it is important to understand that this document is only one element of a regional smart card system, and is not, in itself, sufficient to build the system. Many other decisions must be made and implemented as to the relationship between the participating organizations and business rules. Examples may include (but are not limited to) the following:

- Choices of fare products
- Definition of how fare products will work (for example, expiration of “transit day,” term of rolling period passes, age qualifications for special fares, etc.)

- Central file structures and where the various databases will be maintained
- Frequency of data exchange and reconciliation between various participants
- Security, confidentiality and privacy of the data

NOTE - In addition, where multiple transit agencies are joining together in the operation of a fare collection system, they will need the political and organizational agreements appropriate to establish cooperation, and a means of enforcing compliance among all participants who may be procuring related equipment, supplies and services.

2. Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

- ISO/IEC 14443, Identification cards–Contactless integrated circuit(s) cards–Proximity cards is an international standard for PICCs and is structured in four numbered parts. These documents are available from ISO at www.iso.org.
- ISO 7816, Identification cards–Integrated Circuit Cards is an international standard for PICCs and is structured in twelve numbered parts. These documents are available from ISO at www.iso.org.
- ISO 3166, Codes for the representation of names of countries and their subdivisions is an international standard that provides a consistent number based scheme for identifying countries.

The Standard does not reference or require compliance with any other standards. However, this does not mean that other standards may not be applicable for any given Contactless Fare Media System project.

NOTE – It is the intent to align the nomenclature used in this Standard with that used in ISO/DIS 24014-1 Public Transport – Interoperable Fare Management System – Part I (to be published in July 2007) during the next Standard revision cycle.

3. Definitions, Acronyms and Abbreviations

For the purpose of this document definitions used in the Standard are provided in Annex A.1 of this document.

Acronyms and abbreviations are provided in Annex A.2.

3.1 Rts: prefix used before data element names to help identify that these data elements all belong to objects defined in Part II of the Standard (as opposed to Part III, which uses the same element names, but without the prefix).

The Standard is considered normative except where specifically labeled as “Informative” in the section or subsection title or where labeled “Example” or “Note.”

4. Theory of Operations

4.1 General

A Contactless Fare Media System (System) is a fare collection system that uses PICCs or other contactless fare media for fare payment and validation.

The purpose of this section is to describe the following:

- The main components of a contactless fare media system.
- The entities and their roles in a contactless fare media system.
- How the data and messages are structured.

4.2 Components of a Contactless Fare Media System

A contactless fare media system, illustrated in Figure 1, shall consist of the following components:

- PICC
- Card readers (Card interface device or CID)
- Host fare equipment sub-systems for the above, such as:
  - Customer self-service terminals such as vending machines and reload devices
  - Fareboxes
  - Validators
  - Faregates
  - Sales office terminals
  - Agency Central data collection and reporting Systems (ACS).
  - Regional Central data collection and reporting Systems (RCS), if implementing a regional or multi-agency payment scheme.
  - Data transmission networks

The System may also include the following optional external interfaces:

- Banking operations
- Credit and debit card operations
- Funds movement
- Other regional fare systems
- Other commercial payment systems

The PICC and CID are the foundation of a contactless fare media system and must work together in an efficient manner to ensure full and reliable compliance with the Standard. The PICC and CID are supported at the communications and messaging level of the overall system through communications and messaging between the ACS and RCS.

4.3 Roles and Functions

A Contactless Fare Media System shall be designed to enable the following roles and functions to interface with the System. The assignment of roles and functions to different entities participating in a system may vary according to system implementation.

4.3.1 Agency

An Agency is an organization that governs an affiliated group of Agency level participants including one or more of the following: Product Owner, Product Retailer, Service Operator, Card Issuer and shall be able to:

- define local fare policies,
- assist in establishing rules for the sharing of products and services with other Agencies, if the Agency is participating in a regional transit payment scheme,
- set geographic validity criteria with affiliated Product Owners and service operators within the same Agency,
- define local system attributes such as Product Type and definitions,
- define local security, employee IDs and access rights,
- define product attributes for usage and acceptance by stipulating operational constraints such as service level and times of day acceptance.

4.3.2 Cardholder

The Cardholder shall be able to use their valid card to pay for fare and to show proof of fare payment according to the Agency and if applicable, Regional Scheme Administrator specified rules and regulations.

4.3.3 Card Issuer

The Card Issuer shall be able to manage and control card issuance, distribution, and replacement as well as carry out application management when multiple applications coexist on a single card.

4.3.4 Customer Service Representative

Subject to Agency or Regional Scheme Administrator established business and security rules, a Customer Service Representative shall be able to retrieve and view transaction history from a Cardholder's PICC, change the Cardholder's profile information, and initiate a directive to add and deduct value on the PICC via autoload action requests to the Autoload Administrator or to a Product Retailer. They shall also have the means to:

- assist Cardholders via designated Interfaces,
- inform the Regional Scheme Administrator, Agencies and Card Issuer of lost or stolen cards and initiate replacement via the Card Issuer,
- initiate product replacement via autoload action requests to the Autoload Administrator or to a Product Retailer,
- initiate orders for new cards,
- enroll patrons in special programs such as autoload and account linked services.

At the Agency or Regional Scheme Administrator's option, actions by the Customer Service Representative shall be recorded and communicated to the Agency or Regional Central System.

NOTE—The Standard does not support Agency to Agency data exchange. Therefore the Agency Customer Service Representative may not have access to the tools and information needed to undertake actions related to another Agency's fare products.

4.3.5 Product Owners

The Product Owners define attributes for their products. As well, they:

- agree upon the geographic validity criteria with affiliated Service Operators within the same Agency,
- declare external (other Agency) Service Operators with whom there are agreements for acceptance of their product (s),
- agree on sales criteria with Product Retailers.

4.3.6 Regional Scheme Administrator

The Regional Scheme Administrator shall be able to:

- set the regional interconnectivity and inter-operability rules,
- define regional policies, rules, and regulations,
- define and register regional system attributes such as all participant 'entity IDs' and 'cardholder profile codes,'
- manage system assets and enforce unique Device and CID identity assignments across all participants' equipment, including monitoring of each CID's current location,
- perform financial accounting,
- execute regional funds clearing between all participating entities,
- define regional fare policies and establish rules for the sharing of regional products across Agencies,
- manage centralized services and products.

4.3.7 Regional Security Administrator

The Regional Security Administrator shall be able to:

- define system security (e.g., key management) and regional system level access rights,
- monitor security including but not limited to message authentication, network authentication, and fraud detection at the Transit Application level,
- flag fraudulent and potentially fraudulent PICC use,
- consolidate, manage and distribute the Transit Application Negative List to Agencies, Product Owners, Service Operators, and Product Retailers.

4.3.8 Regional Autoload Administrator

The Regional Autoload Administrator shall be able to receive and process action requests for autoloads from Product Retailers, Benefits Providers, and Customer Service, maintain and distribute 'master action lists' and report completed autoloads to initiators.

4.3.9 Product Retailers

Product Retailers shall be able to:

- sell and terminate products on behalf of Product Owners,
- collect and refund value from/to a Cardholder as authorized by the Product Owner,
- send autoload action requests to the Autoload Administrator, for autoloaded products,
- settle appropriate revenues with Cardholders and Product Owners.

4.3.10 Service Operator

The Service Operator defines Fare Instrument attributes for usage and acceptance by stipulating operational constraints. The Service Operator sets Fare Instrument transfer time, step-up/upgrade rules, and applicable costs and configures acceptance of products from other Agencies.

4.4 Payment or Load Transaction

It is the transit application encoded in the CID that prescribes the logical flow of events that occur in processing the transaction between the PICC and CID. The flow of events during a transaction at minimum must incorporate the following:

a) Detect PICC using standard ISO/IEC 14443 detection and acceptance.

b) Select the transit application using the appropriate APDU command.

c) Read the contents of required Objects using the appropriate APDU command.

d) Perform the Fare Product Logical Processing.

e) Update the Objects used during the transaction using the appropriate APDU command.

NOTE—The process of tearing creates corruption in the user data memory of the PICC. This corruption must be prevented or resolved before the next transaction takes place. The Standard defines a method of tear mitigation that prevents tearing before a tear occurs.

Once a fare transaction between the PICC and CID has been completed, a Transaction Record shall be stored in the CID and then forwarded on to the RCS by way of the Agency fare collection system (inclusive of the Agency Central Computer (ACC)). Although the Standard does not specify the transaction storage and messaging within an Agency fare collection system, Part III does provide a transaction message definition between the Agency fare collection system and the RCS.

4.5 Data and Message Structure

The foundations of the Standard are the data objects defined in Part II of the Standard. These objects are groupings of data elements. Part III of the Standard describes the structure of the messages between the ACS or fare collection sub-system and RCS. These messages are built using the objects defined in Part II as well as other additional objects defined in Part III that are specific to Part III messages.

Each Object’s content is held within 16-bytes. However, not all objects currently make use of all the allocated 16 bytes. RFU (Reserved for Future Use) bits are provided for future use by APTA and may not be used by any implementer for any purpose.

Objects may at times require more data than 16-bytes can support. In this case, Part II makes provisions for additional data through the use of Extensions. An Extension contains 16-bytes of data capacity that act like an extension of the core Object.

Part II describes six objects that provide all the necessary grouping and support for the fare product objects. These six objects shall perform a transit application transaction with a high degree of data integrity and security.

— The Directory Index Object (DIO) gives the Transit Application a logical to physical mapping of the other Objects stored within the PICC memory. The DIO also informs the Transit Application of the possible existence of Object extensions.

— The Transit Application Profile Object (TAPO) informs the CID application of the PICC's unique serial numbers, origin information, capabilities and limitations. The TAPO shall be encoded or configured at the PICC pre-issuance stage or the PICC initialization stage. The TAPO shall be used as the first indication that a PICC is valid and accepted by the system in which the PICC is being presented.

— The PICC Holder Profile Object (PHPO) identifies the transit patron's profile relative to their personal preferences for transit fare products and services. As with the TAPO, this object shall be pre-issue encoded or encoded at issuance.

— The Product Index Objects (PIOs) contain a mandatory index of the transit fare products (defined by Product Objects) on a specific PICC application. It provides summary details of the transit fare products currently stored on the PICC and enables AFC system to quickly identify products that might be applied to the current fare payment. A PICC shall contain 2 sets of PIO Objects for tear prevention. Each set shall contain at least one PIO and one PIO extension but can have two additional extensions, if required. There are 256 distinct Product Types available to each Agency (253 pass types, one stored value (or purse type), one account linked, and one AutoValue based product type).

— The Transaction History Object (THO) is a required core object and each THO records a single transaction. A minimum of 6 and a maximum of 16 THOs must be included within the PICC data structure in order to provide for storage of the 16 most recent transactions performed by the PICC. Once the configured quantity of THOs on the card have been used to record a transaction, the oldest THO is overwritten to record the next transaction.

— Add & Deduct Value History Object (A&DVO) is an optional object used to record the most recent additions and deductions of value transactions from the T-purse and/or other stored value products. A minimum of 2 and a maximum of 8 A&DVOs must be included in the PICC data structure if any of these objects are used. Since use of the A&DVO applies only to stored value (including T-purse) transactions, it may hold information relating to transaction records that were also recorded in a THO but have been overwritten due to the limited number of transactions that can be concurrently stored in THOs on the PICC.

In addition, five fare product objects are supported by the Standard to encompass all known fare policies and fare types in the industry.

— The Pass and Transfer Product Object (P&TPO) contains the required information or functionality and data representing either a pass or transfer product. At least one P&TPO must be included to record any form of pass or transfer product stored on the PICC. Since each pass and transfer product is represented by a P&TPO, each new instance of a pass or transfer product stored on the card requires the use of a separate P&TPO.

— The Stored Value and T-Purse Product Object (SV&TPPO) contains the required information or functionality and data representing a T-Purse or an agency specific stored value product. The T-Purse shall be the regional stored value fare product, usually stored in local currency and there shall be only one instance of a T-Purse on a PICC. Each additional instance of an agency-specific stored value product must separately be represented on the PICC by a separate SV&TPPO. The Autoload feature can be enabled for the SV&TPPO.

- The Account Linked Product Object (ALPO) is used to define a fare product that is tied ("linked") to a host-based account such as a credit or debit card. It acts like a T-Purse product, except does not require pre-funding. There can be only one instance of an Account Linked product on a PICC.
- The Account Linked Reference Object (ALRO) is an object that contains the Account Linked Product reference information (e.g., bankcard number) that requires secure access. The ALRO object must occupy a dedicated file on the PICC with a separate security write key.
- The AutoValue Product Object (AVPO) is implemented when an Agency or regional operator wants to provide incentives (rewards) for frequent stored value or the T-Purse use.

The protocol for deciding which product is to be selected for use in a specific circumstance shall be agreed upon by implementers and applied consistently within a System.

4.6 Messages Description

Messages originate either at a CID (i.e., card device), Agency Central System, or the Regional Central System.

CID to PICC Interaction Messages are used to transfer transaction data such as PICC Initialization, Fare Product, and Service Load and Unload Transactions as well as Use Transactions and RCS Acknowledgements.

In the CID to PICC Interaction Messages, the objects are those defined in Part II. When such an object is read from the PICC, it is named "*Part II Object Name*" AsRead (e.g., A&DVHOAsRead). When the object is written to the PICC or when the data values associated with an existing object are changed/rewritten, it is named "*Part II Object Name*" AsWritten (e.g., A&DVHOAsWritten). Product objects can also be designated as an Agency product (e.g., AgencyPOAsRead) or a regional product (e.g., RegionalPOAsRead).

Scheme Control Messages convey information relating to the operation of the card or device such as Action Lists, Negative Lists, the fare policy framework and key management.

Extensible Markup language (XML) is the required data transmission method to be employed in transferring messages between an ACS and RCS. An XML schema shall be used to define the contents of the messages and to constrain the XML consistent with the formatting and content specifications defined within the Standard.

NOTE—If Non-XML methods were to be used by a participating agency system that system would need to emulate the XML method of transmitting the data to the RCC. For systems that rely on non-XML means for data transfer, the implementer would have to validate the data against the XML Schema and convert to XML prior to sending it to the RCC. As a consequence, a custom interpreter would need to be installed on every system that is not using XML. This would defeat the requirement of interoperability and is therefore not permitted by the Standard.

Most messages send information generated by the CID to the RCS (usually via a local computer and an Agency Central System). These messages consist of data extracted from and added to the PICC and data generated by the CID. Although the actual content will vary with message type, these messages have a common general structure where message data objects and elements are grouped into the following four sections:

- When and where used data–information on when and where the transaction occurred.
- Authentication data–used to validate the message.
- PICC data–information used or modified on the PICC as part of the transaction.
- CID data–information created by the CID as part of the transaction.

5. Guidance on the Administration of the Standard

5.1 General

This Standard shall be administered by the UTFS Task Force Executive Committee, under the direction of the APTA Rail Standards Policy and Planning Committee with oversight by the APTA Standards Development and Oversight Council (SDOC).

The administration of the Standard shall consist of the following two primary activities:

— Periodic review and revision of the Standard.

— Management of support activities related to the Standard.

5.2 Revisions to the Standard

All standards evolve to meet changing conditions and technology. As required by APTA's IP Policy, this Standard is subject to periodic review for reaffirmation, revision, or withdrawal every 5 years or sooner from initial general release.

Agencies and suppliers using the Standard may request APTA to implement extensions to the Standard. If approved, the extension will be included in a future revision to the Standard when the Standard is updated and reissued. Extensions not approved by APTA may be implemented, however the agency or supplier will be at risk that their product or system will no longer be compliant with the Standard.

The UTFS Task Force Financial Management Committee will coordinate and manage Standard updating. Any Task Force member or user of previously approved documents who has agreed to comply with APTA's IP Policy may request a change or correction to a previously approved document. The exact wording of the proposed change or correction and a clear statement of the reasons for proposed change or correction should be sent to:

American Public Transportation Association
Program Manager, Universal Transit Fare System Standard
1666 K Street, N.W.
Washington, DC, 20006-1215

The Program Manager will convene a meeting of the UTFS Task Force Executive Committee to consider the request for change or correction. If the Executive Committee determines that the change corrects an obvious error, the executive committee may simply instruct the Program Manager to make the correction and issue Corrigenda.

If the Executive Committee determines that the proposed change has merit, but could change the intent or application of the document, the Executive Committee shall refer the proposed change to the Financial Management Committee for consideration. The Committee may act on the change in any manner from denying the proposed change to proposing a revised document to the full Task Force for a re-vote.

If the Executive Committee determines that the proposed change has no merit, the Executive Committee may deny the change and instruct the Program Manager to inform the party that submitted the change that the proposed change has been rejected.

5.3 On-going Support and Maintenance of the Standard

The establishment, propagation and management of this Standard is carried out by APTA staff, under the direction of a Standard Maintenance Work Group appointed by the UTFS Task Force. This includes the following activities:

- Contactless Fare Media System Standard Test and Compliance Certification Program

  APTA may help identify and put in place agreements with independent test laboratories to provide Standard compliance testing to the transit industry.

- Data Element Registry

  APTA maintains a national registry for certain data elements (e.g., Regional ID, Agency ID) described in Part II of the Standard, assigning initial values and evaluating submissions proposing new data elements.

- Object Registry

  APTA maintains a registry for objects described in Part II and Part III of the Standard, and evaluates submissions proposing new objects.

- Publication and Distribution of the Standard

  APTA publishes and distributes the Standard, as well as any related amendments and corrigenda.

- Training and Certification Program

  APTA manages the development and delivery of a Contactless Fare Media System Standard training programs for fare collection system manager and technical personnel, as well as for consultants, integrators, and others who may design or advise agencies on the design of Standard compliant PICC systems.

- Card Numbering Scheme

  APTA manages and maintains a unique numbering scheme for regions in North America in order to allow for continental interoperability. This program ensures that all cards used in North American PICC electronic fare collection systems compliant with the Standard are assigned a discrete card number.

Annex A

(normative)

Definitions, Acronyms and Abbreviations

A.1 Definitions

Numeric

3DES: See **Triple DES**

A

Account Linked: A fare product type on a PICC that links a Stored Value like fare product or purse to a financial banking instrument such as a credit card.

Action List: A list of issued PICCs that are to have some action performed on each PICC in the list (such as the delivery of an Autoload) if the PICC is presented to any applicable CID in the system. The action list transmitted to all appropriate CIDs in the regional scheme.

Add Value Machine (AVM): A machine that is capable of adding value or products to a PICC.

AFC Device: A fare collection device such a farebox, turnstile or ticket vending machine that can accept and/or dispense electronic fare media.

Alternate Keys: An encryption key set any which can be used should any of the other encryption key sets become compromised.

American Standard Code for Information Inter-change (ASCII): A 7-bit character code which represents 128 characters including the upper and lower case alphabet, numerals and special characters. Some characters are special control characters used in communications control and are not printable.

Anti-Passback: A means to limit the fraudulent use of a single PICC for multiple boardings.

Anti-Tear: The method used by a system or PICC to prevent or correct corruption of data stored on the PICC when it is removed prematurely from the CID’s field prior to completing the updating of that data.

Application: Structures, data elements and program modules needed for performing a specific functionality (from ISO/IEC 7816-4:2005). However, as used in this Standard, may also mean a data set on the PICC.

Application Identifier (AID): A data field to identify an application.

Application Program Interface (API): The interface (calling conventions) by which an application program accesses the operating system or other services.

Application Protocol Data Unit (APDU): A packet of data exchanged between two application programs across a network. Within the Standard, this term is used as a reference to the commands (instructions) that are issued by a CID to a PICC in order to initiate, authenticate and perform the exchange and update of data between those devices.

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.

Audit: An examination of procedures, programs, activities, and equipment to determine how effectively they are performing, especially in terms of ensuring the integrity and security of data they process or produce.

Audit trail: A step-by-step record by which data can be traced to its source.

Authorization: The process of granting permission for some action to be taken. The most common usage is relative to the authorization of transactions. An authorization service provider determines whether a requested transaction may be completed. The process of granting (read, write or update) access to a file on a card because of correctly presenting the secret code(s).

Autoload: A method which automatically loads a PICC electronically with a transit fare product using a process which is usually transparent to the cardholder. Autoload may be implemented in three different ways: Directed, Threshold or Recurring.

AutoValue: A loyalty scheme which provides incentives to patrons for frequent use of a system.

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.

Batch: A set of transactions originating from the same identified source with an associated Batch Transaction Header. Transaction Headers contain security information and other data common to all the transactions in a batch.

Batch Personalization: Personalizing a batch of cards sequentially. See **Personalization**.

Binary: Machine-readable, non-text data.

Bits per second (bps): The speed of data transfer in a communications system measured in bits.

Block: Changing the validity of a PICC to prevent further use of the PICC, the application on the PICC or the fare product on the PICC. A temporary block can be reversed (see **Unblock**). A permanent block cannot be reversed.

Boarding: A single entry on a transit vehicle or system.

Business Rules: The set of rules which define the use of the fare collection system.

Bytes per second (Bps): The speed of data transfer in a communications system measured in bytes.

C

Card: Typically, a credit card sized media constructed of either plastic or paper or a combination of the two and which has an integrated circuit or magnetic strip for the purpose of storing information. The thickness of the card may vary depending on the material and use.

Card Initialization: Card Initialization: The step in the issuance process in which the keys, data structure and critical data objects are written to the PICC's electronic memory. This normally includes setting up the card data structure, application, products and security keys to suit the intended use.

Card Interface Device (CID): A device which contains both the PCD and the application hosting processor to provide communications and application processing between the PICC and the 'Point of Use Devices' and are also known as validators and readers.

Card Operating System (COS): The operating system on the integrated circuit chip that controls how the card works. The operating system is often proprietary to the card manufacturer.

Card Reader: See **CID** and **PCD**.

Card Serial Number: A unique serial number assigned to a PICC.

Certificate: Encrypted codes that are generated using random numbers, card serial numbers, and transaction numbers. It is used to authenticate a transaction.

Chip: Semi-conductive material, usually silicon, that contains miniaturized electronic circuits.

Clearing: Describes the functions necessary to collect card (PICC, credit card, debit card) transactions from Retailers and Service Operators and the subsequent presentation of the items to the Product Owner. The clearing process becomes the basis for settlement.

Collection: The process of transferring transaction logs from point of use devices to a system where they can be settled and reported. Point of use devices include vending machines and other offline devices, POS terminals, gates, fareboxes, and value load terminals. Collection can be performed online via a communications link to a collection system, or offline via a handheld collection device.

Contactless: Pertaining to the achievement of signal exchange with and supplying power to a PICC without the use of galvanic elements (i.e., the absence of an ohmic path from the external interfacing equipment to the integrated circuit(s) contained within the card). (From ISO/IEC 14443-1:2000).

Contactless Integrated Circuit(s) Card: A card of the card type ID-1 (as specified in ISO/IEC 7810) into which integrated circuit(s) have been placed and in which communication to such integrated circuit(s) is done in a contactless manner. (From ISO/IEC 14443-1:2000) (See **PICC**)

Contactless Smart Card (CSC): A type of smart card that does not require physical electrical contact connections between the card and a reader. Communication between card and reader is by radio frequency or other means. The ISO 14443 standard provides requirements for contactless cards.

Cryptographic Keys: Digital values used by encryption algorithms to convert plaintext to ciphertext.

D

Data Authentication Code (DAC): The DAC is a mathematical function of both the data and a cryptographic key which may be stored, or transmitted. When the integrity of the authenticy data is verified, the DAC is generated on the current data and compared with the previously generated DAC. If the two values are equal, the integrity (i.e., authenticity) of the data is verified.

Data Dictionary: A repository for the “official” names and definitions of data elements, files, entities, objects, etc. used in defining and developing system software.

Data Element: Item of information for which is defined a name, a description of logical content, a format and a coding.

Data Encryption Standard (DES): The term given to a widely used public-domain symmetric key cryptographic algorithm. DES is based on a published algorithm with secret keys.

Data Formats: A set of files containing records or objects that define the card format for a given application or a set of applications such as applications for Transit, Building Access, Biometrics, etc.

Data Object: A grouping of data elements.

Debit: A transaction that decreases the value in a purse or an account.

Digital Signature: Data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string, and protects against forgery, e.g. by the recipient of the data string. (From ISO/IEC 7816-4:2005)

Directory File (DF): An optional elementary file containing a list of applications supported by the PICC and optional related data elements. (From ISO/IEC 7816-4:2005).

Discount: A reduction in the regular fare offered by an Agency based upon customer demographics, travels characteristics or purchase characteristics.

Distributed Computing Environment (DCE): Computing systems whose hardware and software share the computing load in a cooperative manner.

Domain: A territory or region over which a set of operating rules or common control is exercised.

Download: The transfer of software or data files from an upper level or server system to a lower level or client system.

Dual Control: A method of maintaining security and reducing risk whereby two individuals must be present while performing a specific task, such as counting currency etc. Frequently each individual will posses one-half of a required security device or parameter.

E

Elementary File (EF): A set of data units or records or data objects sharing the same file identifier and the same security attribute(s). (From ISO/IEC 7816-4:2005)

Encoding: Term used within the Standard to refer to the process of recording data electronically within the memory of a PICC.

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

F

Fare: The value paid for travel.

Fare Evasion: Unlawful use of transit facilities by riding without paying the applicable fare.

Fare Media: An electronic portable media (see Card) used to gain access to public transportation system services.

Fare Policy Framework: A logical structure for classifying and organizing a Product Owner’s transit fare structure, fare prices, and tariff rules.

Fare Products: Term used to refer to the specific types of pre-paid products (e.g., monthly pass, single ride, T-purse) that are used to gain access to services within a transportation system and defined by agency or regional fare policy.

Fare Tables: The set of prices, fare products and usage rules that define the acceptable methods of fare payment and prices for transportation system services.

File ID: A data element used to address a file. (From ISO/IEC 7816-4:2005)

File: Structure for application or data or both in the PICC, as seen at the interface when processing commands. (From ISO/IEC 7816-4:2005)

Firewall: A stringent security measure designed to protect a network from unauthorized access. For example, the measures employed when a local network is connected an outside network by a "gateway" processor. This gateway processor does permit unauthorized communication data to pass from inside to outside and vice versa.

Fraud Detection: Determining the authenticity and consistency of collected transactions or batches of transactions to determine missing or duplicate transactions, batches, signatures, transaction numbers, and negative -listed cards or stored value cards. It also includes the research to determine the cause of certain exceptions which may be identified locally or by subordinate nodes of a network.

Funds Movement: Automatic transfer of funds from one organization to another in financial institution accounts.

G

Graphical User Interface (GUI): A term used to refer to the use of pictures (graphics) and icons, rather than strictly text, in a computer display of a software application to simplify the use of that application and to minimize the need to use or understand complex computer languages and/or application codes. See also **User Interface**.

H

Hotlist: See **Negative List**

Hypertext Markup Language (HTML): A set of text-formatting and layout codes used to create Web pages than can be interpreted by a browser.

Hypertext Transfer Protocol or Hypertext Transport Protocol (HTTP): The protocol used on the world-wide-web (Internet) that performs the request and retrieve functions of a server, and is commonly seen as the first part of a website address. Also see **Secure Hypertext Transfer Protocol**.

I

Identification number: On an identification card, the number that identifies the cardholder.

Integrated Circuit: Electronic component(s) designed to perform processing and/or memory functions. (From ISO/IEC 14443-1:2000)

Interface: That point at which one system component or subsystem comes into physical or functional contact with another.

International Organization for Standardization (ISO): A global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide.

J

Journey: Term used to describe a single passenger's travel which may consist of one or more boardings, transfers and disembarkments in order to move the patron from origin to destination.

K

Key: Secret code that is 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.”

Key Management: A trusted system that keeps encryption keys and modules secure and keeps continuous logs of all activities related to key access and utilization. The life cycle management for security keys encompasses seven 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:** 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 which are in use.

— **Key Rollover:** Replacing a set of active security keys in a CID with a new key set.

L

Limited Use (LU) Smart Card: A non-microprocessor card, generally designed to satisfy the need for a low cost fare media albeit with limited functionality and features (e.g., reduced data storage capacity, reduced durability, lower security) when compared to a typical PICC but still meeting the standards set forth in ISO/IEC 14443, Parts 2 and 3 (for type A or B PICCs).

Load: The function of adding value, a product or an application onto a PICC. A product could be a period pass or stored rides.

Local Area Network (LAN): Typically an Ethernet Network within a local area (i.e., within the same building), that interconnects Devices. Also see **Wide Area Network**.

Log: A file or report which lists a series of events or transactions over time.

Loyalty Program: A promotional program in which value, rides, discounts or other encouragement to use transit (or other product or services) is credited to a cardholder’s card for various reasons.

M

Message Authentication Code (MAC): An encrypted code sent with a message to authenticate the contents of the message.

N

Negative List: A list of issued cards that are to be prevented from normal use if presented to any applicable Card Interface Device in the system.

Network Manager: Party responsible for monitoring and servicing devices within a network.

O

Online: Connected to a communications network.

Open System: A vendor independent system that is designed to interconnect with a variety of commonly available technology products. For example, payment systems involving multiple issuers of cards that can be used to access transit services or products at multiple Service Operators and Retailers. The system is termed “open” because the technical requirements to participate are widely available without restriction.

P

Participating Entities: Refers to all entities within the regional scheme. "Participating Entities" can be Agencies, Product Owners, Service Operators, Retailers and PICC Issuers.

Pass Fare Product: A means of transit prepayment that permits a passenger a specified number or unlimited number of trips during a defined time period or in a defined geographic area or on a defined service or a combination of these criteria.

Password: Data that may be required by the application to be presented by its user for authentication purpose. (From ISO/IEC 7816-4:2005)

Personal Identification Number (PIN): Numeric data that may be required by the application to be presented by its user for authentication purpose.

Personalization: The step in the PICC issuance process in which the data values specific to the cardholder are encoded within the PHPO on the PICC. **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.

Point-of-Sale (POS) Device or Terminal: A device used to make purchase transactions at the point they occur (e.g., at the Retailer location) or to load value or product on PICCs.

Proof of Payment: A means to prove that a fare has been paid for the transport of a patron. The 'proof of payment' may be printing, a punch hole, a cut corner, magnetic encoding or a PICC record.

Proximity Coupling Device (PCD): The reader and writer device that uses inductive coupling to provide power to the PICC and also to control the data exchange with the PICC. (From ISO/IEC 14443-1:2000)

Proximity Integrated Circuit Card (PICC): A card into which Integrated Circuit(s) and coupling means have been placed and in which communication with such Integrated Circuit(s) is done by inductive coupling in proximity of a coupling device. (From ISO/IEC 14443-1:2000)

Q

R

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

S

Secure Hypertext Transfer Protocol (S-HTTP): 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). Also see **Hypertext Transfer Protocol (HTTP)**.

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

Security Access Module (SAM): A security module in the form of software or hardware such as an integrated circuit for storing a security scheme. A SAM is often referred to as the module that contains the master keys of the security system.

Session: The duration of communication between two devices.

Session Key: A non-repeating value used for encryption during a secure session.

Settlement: The process by which the daily amount of funds generated by the clearing process is reported and transferred between participants in a payment system.

Signature: Encrypted codes such as those created by the PICC and CID and appended to data.

Single DES: A security scheme that used one DES key and one DES function.

Smart Card: See **Proximity Integrated Circuit Card**.

Stored Value (SV): Pre-purchased transit value residing on the cardholder's PICC, which can be used for travel within the transit system.

Switch: A processor that routes transactions or other types of data from a sending processor to the appropriate receiving processor.

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

System: Related set of devices that are integrated and interconnected to perform a specific function.

T

Timestamp: A time data field that is appended to a transaction by a processing system, switch or host at the time that it is sent or acquired.

T-Purse: A transit purse containing stored value used primarily as a transit regional purse product.

Transaction: A collection of interrelated steps for payment, that when completed the totality of which is described as a transaction. As applied to a card or device, this usually means a single activity, such as a pass purchase or load value.

Transmission Control Protocol/Internet Protocol (TCP/IP): A set of communications protocols that support peer-to-peer connectivity functions for both local area networks (LANs) and wide are networks (WANs).

Transport Key: A key used to control access to a memory logic card's data files when it is delivered from the manufacturer.

Triple DES (3DES): A security scheme based on DES that uses two or three DES keys and three applications of the DES functions algorithm to perform a secure function.

Type A: Is one of the two types of signal interfaces of the ISO/IEC-14443 standard. Type A uses 100% ASK modulation of the RF carrier and Miller Pulse Position coding to send data from the coupling device to the card. For the return link the carrier frequency is loaded to generate an 847 kHz sub-carrier. Type A uses On/Off Keying of the sub carrier with Manchester bit coding.

Type B: Is one of the two types of signal interfaces of the ISO/IEC-14443 standard. Type B uses 10% ASK modulation of the RF carrier and non-return to zero (NRZ) coding to send data from the coupling device to the card. For the return link the carrier frequency is loaded to generate an 847 kHz sub-carrier. Type B uses Binary Phase Shift Keying of the sub-carrier with NRZ bit coding.

U

Unblock: Changing the state of a blocked card, application or product so that it can again be used normally.

Unload Value: To remove an amount from a stored value or T Purse card balance.

Upload: The transfer of data files from a lower level or client system to an upper level or server system.

V

W

Wide Area Network (WAN): A communication network that connects geographically separated areas and locations.

X

Y

Z

A.2 Acronyms and Abbreviations

AFC	Automatic Fare Collection
AID	Application Identifier
ALPO	Account Linked Product Object.
ALPOX	Account Linked Product Object Extension
APDU	Application Protocol Data Unit
API	Application Program Interface
APTA	American Public Transportation Association
ASCII	American Standard Code for Information Inter-change
ATQA	Answer To Request for ISO/IEC 14443 Type A PICCs
ATQB	Answer To Request for ISO/IEC 14443 Type B PICCs
AVM	Add Value Machine
AVPO	Auto Value Product Object
AVPOX	Auto Value Product Object Extension
bps	bits per second
Bps	Bytes per second
CID	Card Interface Device
COS	Card Operating System
CSC	Contactless Smart Card
CSR	Customer Service Representative
DAC	Data Authentication Code
DCE	Distributed Computing Environment
DES	Data Encryption Standard
DF	Directory File
DIO	Directory Index Object
DIOX	Directory Index Object Extension
EEPROM	Electrically Erasable Programmable Read Only Memory
EF	Elementary File
GUI	Graphical User Interface
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol
IC	Integrated Circuit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Organization for Standardization
LAN	Local Area Network
LU	Limited Use Smart Card
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OS	Operating System
P&TPO	Pass and Transfer Product Object
PCD	Proximity Coupling Device
PHPO	PICC Holder Profile Object
PHPOX	PICC Holder Profile Object Extension
PICC	Proximity Integrated Circuit Card
PIN	Personal Identification Number
PIO	Product Index Object
PIOX	Product Index Extension
PO	Product Object
POS	Point of Sale Device or Terminal
RAM	Random Access Memory
RF	Radio Frequency
RFU	Reserved for future use (From ISO/IEC 7816-4:2005)
ROM	Read Only Memory
SAM	Security Access Module
S-HTTP	Secure Hypertext Transfer Protocol
SSL	Secure sockets Layer
SV	Stored Value
SV&TPPO	Stored Value and T-Purse Product Object
TAPO	Transit Application Product Object
TCIP	Transit Communications Interface Profiles

TCP/IP	Transmission Control Protocol/Internet Protocol
THO	Transaction History Object
UID	Unique Identifier
WAN	Wide Area Network