TCRP
REPORT 115

TRANSIT COOPERATIVE RESEARCH PROGRAM

Sponsored by the Federal Transit Administration

Smartcard Interoperability Issues for the Transit Industry

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

TRANSIT COOPERATIVE RESEARCH PROGRAM

TCRP REPORT 115

Smartcard Interoperability Issues for the Transit Industry

ACUMEN BUILDING ENTERPRISE, INC.
Oakland, CA

IN ASSOCIATION WITH

BOOZ ALLEN HAMILTON, INC.
San Francisco, CA

Subject Areas
Public Transit

Research sponsored by the Federal Transit Administration in cooperation with the Transit Development Corporation

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2006
www.TRB.org

TRANSIT COOPERATIVE RESEARCH PROGRAM

The nation's growth and the need to meet mobility, environmental, and energy objectives place demands on public transit systems. Current systems, some of which are old and in need of upgrading, must expand service area, increase service frequency, and improve efficiency to serve these demands. Research is necessary to solve operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the transit industry. The Transit Cooperative Research Program (TCRP) serves as one of the principal means by which the transit industry can develop innovative near-term solutions to meet demands placed on it.

The need for TCRP was originally identified in *TRB Special Report 213—Research for Public Transit: New Directions,* published in 1987 and based on a study sponsored by the Urban Mass Transportation Administration—now the Federal Transit Administration (FTA). A report by the American Public Transportation Association (APTA), Transportation 2000, also recognized the need for local, problem-solving research. TCRP, modeled after the longstanding and successful National Cooperative Highway Research Program, undertakes research and other technical activities in response to the needs of transit service providers. The scope of TCRP includes a variety of transit research fields including planning, service configuration, equipment, facilities, operations, human resources, maintenance, policy, and administrative practices.

TCRP was established under FTA sponsorship in July 1992. Proposed by the U.S. Department of Transportation, TCRP was authorized as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). On May 13, 1992, a memorandum agreement outlining TCRP operating procedures was executed by the three cooperating organizations: FTA, the National Academies, acting through the Transportation Research Board (TRB); and the Transit Development Corporation, Inc. (TDC), a nonprofit educational and research organization established by APTA. TDC is responsible for forming the independent governing board, designated as the TCRP Oversight and Project Selection (TOPS) Committee.

Research problem statements for TCRP are solicited periodically but may be submitted to TRB by anyone at any time. It is the responsibility of the TOPS Committee to formulate the research program by identifying the highest priority projects. As part of the evaluation, the TOPS Committee defines funding levels and expected products.

Once selected, each project is assigned to an expert panel, appointed by the Transportation Research Board. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, TCRP project panels serve voluntarily without compensation.

Because research cannot have the desired impact if products fail to reach the intended audience, special emphasis is placed on disseminating TCRP results to the intended end users of the research: transit agencies, service providers, and suppliers. TRB provides a series of research reports, syntheses of transit practice, and other supporting material developed by TCRP research. APTA will arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by urban and rural transit industry practitioners.

The TCRP provides a forum where transit agencies can cooperatively address common operational problems. The TCRP results support and complement other ongoing transit research and training programs.

TCRP REPORT 115

Price $35.00

Project A-26
ISSN 1073-4872
ISBN-13: 978-0-309-09870-0
ISBN-10: 0-309-09870-X
Library of Congress Control Number 2006938001

Published reports of the

TRANSIT COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation through research. In an objective and interdisciplinary setting, the Board facilitates the sharing of information on transportation practice and policy by researchers and practitioners; stimulates research and offers research management services that promote technical excellence; provides expert advice on transportation policy and programs; and disseminates research results broadly and encourages their implementation. The Board's varied activities annually engage more than 5,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

FOREWORD

By Gwen Chisholm-Smith
Staff Officer
Transportation Research Board

TCRP Report 115: Smartcard Interoperability Issues for the Transit Industry defines interoperability; identifies key information needed by public agencies to implement smartcard payment systems interoperability; describes the necessary information flows; and outlines a set of functions needed for a standard public domain application programming interface (API) that may be used in the development of a uniform application protocol data unit (APDU). The report includes a prototype for an API and an APDU that demonstrates this "proof of concept" for International Organization for Standardization (ISO)-compliant Type A and Type B cards.

The report is intended for use by transit decision makers and practitioners to help guide them through the creation and implementation of interoperable smartcard payment systems. Agencies at varying points of creating and implementing an interoperable transit smartcard system will find this helpful.

Smartcards are a secure, widely accepted medium for cashless payments for a wide spectrum of financial transactions, including automatic fare collection (AFC) activities within transit districts. Smartcard electronic payment media systems are operating on transit systems across the nation. Use of smartcards can greatly increase the level of convenience and facilitate transfers for transit riders and can increase efficiency and reduce costs for transit providers. Smartcards used on public transit can have widespread application outside of transit. They can be linked to other modes of transportation (e.g., parking and highway tolls) and other industries such as retail, banking, and security.

Although seamless smartcard electronic payment systems can benefit transit passengers and operators, as well as other potential users, transit operators face substantial challenges in integrating smartcard-based AFC equipment from different manufacturers because of the lack of interoperability. Some examples of the complicating factors are application of multiple fare-payment systems and technologies, transit agencies' different operating needs and fare mechanisms, inadequate communication protocols and information exchange among transportation clearinghouses, absence of a single API to foster interoperability, and intellectual property barriers that do not allow for open architecture. These problems need to be remedied, before widespread deployment can proceed.

The TCRP researchers, Acumen Building Enterprise, Inc., in association with Booz Allen Hamilton, Inc., identified the key institutional issues that may present barriers to implementing an interoperable transit fare-payment program, described the commonalities and differences in the information exchanged between agencies, outlined the data elements and information exchanged that are critical for implementing smartcard interoperability, delineated the information flow, and examined critical data management issues and policies. The research team discussed the development of a prototype for a proposed public domain API that demonstrates a "proof of concept" for ISO 14443 Type A and B compliant cards.

CONTENTS

SUMMARY

Use of contactless smartcards for electronic fare payment for transit in the United States will probably increase over time. There is a strong desire to create interoperability within transit smartcard implementations for greater patron convenience, which would indirectly stimulate greater use of mass transit. Unfortunately, interoperability is not an attribute of the existing systems and will require some effort to attain.

TRB defines interoperability for this research project as "the ability of different agencies to coordinate and share information so that passengers can travel in a seamless fashion." This definition covers technological barriers that may preclude one agency's smartcard reader from reading a smartcard issued by another agency as a result of protocol or radio frequency incompatibility. It also addresses the need for uniformity in how data are stored on the card and what information is included on the card.

To accomplish interoperability at a technological level, use of international standards must be required. ISO/IEC 14443 is an international standard that covers the physical and radio frequency characteristics and the initialization, anti-collision, and transmission protocols for contactless smartcards. Strict adherence to ISO/IEC 14443 in transit implementations would make data exchange possible because it would ensure that transit contactless cards and readers would have a uniform basic communication channel.

To allow interoperable access to the data on the card, ISO/IEC 7816-4 defines a set of commands or application protocol data units that allow data interchange at the higher application level. This allows identity to be read, updated, and authenticated in a standard non-proprietary fashion. This standard was developed for contact smartcards; however, early contactless devices chose proprietary protocols to provide for application-level data exchange. The research done for this report found that the lack of standard use was a significant obstacle to interoperability of existing implementations in transit systems.

How data are represented on the card, or card format, is another area that needs standardization. Several standards are available for this purpose, one being the Regional Interoperability Standard for Electronic Transit Fare Payments (RIS). The RIS is under review for adoption by APTA's Universal Transit Farecard Standards (UTFS) Task Force. Compelling the use of such a standard would ensure that every agency would store data on the card in the same way; this would allow a card to be "understood" from agency to agency, provided the agencies were inclined to share the security information needed to authenticate access to the cards. A standard such as the RIS or UTFS typically includes related procedures and specifications to govern the transmission of data from the automatic fare collection (AFC) equipment to and from the agency central computer system and regional clearinghouse.

Another area that could benefit from standardization would be the integration of the contactless smartcard reader to the host computer that typically operates a fare gate or ticket vending machine (TVM). Today, the programming interface for contactless smartcard readers is predominantly proprietary. This usually requires that the fare gate or TVM application software be rewritten if the contactless reader is replaced with a different model. A standard application programming interface (API) can solve this through the definition of standard functions and data types. Once an API is established, the hardware manufacturers can produce equipment with software drivers that conform to the API. As part of this project, an API and software drivers were developed to demonstrate this concept. The API approach provides an option for transit systems to reduce the cost of technological obsolescence in smartcard-based AFC deployments.

This work is intended to guide the planning of new deployments and systems. Several systems with smartcard infrastructures exist; most of these systems were planned and implemented before the current standards. The cost of transitioning one of these systems to a standards-based system will differ from system to system and cannot be generalized effectively. Perhaps the most prudent approach for such systems would be to wait and see if the acceptance of contactless bankcards may provide an effective alternative to a system rebuild.

Sufficient standards exist to provide interoperability in the use of smartcards in transit environments. The adoption of a standard API may help reduce the cost of maintaining AFC application software as contactless smartcard technology develops and matures. The key to interoperability in the future of smartcard-based AFC systems for transit lies in compelling the use of these standards.

CHAPTER 1

Introduction

The overall objective of TCRP Project A-26 was twofold. First, the task was to identify the key information that must be exchanged between transit agencies to achieve fare payment interoperability. Second, once the information was identified, the task was to develop a prototype for a proposed public-domain application programming interface (API) and uniform application protocol data unit (APDU) that demonstrates "proof of concept" for Type A and Type B smartcards that comply with International Organization for Standardization (ISO).

The report synthesizes primary research. The key activity consisted of surveying regions implementing a regionally interoperable fare payment system using smartcards. Moreover, the report references, as required, the experience gained during the implementation of interoperable fare payment system projects in locations such as New York; Washington, DC; San Francisco; Chicago; and Los Angeles.

The structure for this report is as follows:

- Chapter 1 identifies the key institutional issues that may present barriers to implementing an interoperable transit fare payment program. The research focuses on identifying institutional issues found during the implementation of projects reviewed as part of this report. The institutional issues are organized as follows:
  - Management and organizational issues,
  - Financial management issues,
  - Patron impact issues,
  - Equipment design issues, and
  - Transit industry issues.
- Chapter 2 discusses the results of the formal survey conducted to identify commonalities and differences in the information exchanged between agencies.
- Chapter 3 identifies the data elements and information exchanged that are critical for implementing smartcard interoperability.
- Chapter 4 delineates the necessary information flows as follows:
  - Information flows that define the requirements for developing the API and APDU,
  - Information that needs to reside on the card, and
  - Data flows between each level in the system architecture.
- Chapter 5 examines critical data management issues and policies.
- Chapter 6 provides a set of functions needed for a standard public-domain API that may be used in developing a uniform APDU.
- Chapter 7 discusses the development of a prototype for a proposed public domain API that demonstrates a "proof of concept" for ISO 14443 Type A and Type B compliant cards.
- Chapter 8 documents the results of the development effort.

1.1 Interoperability Defined

For this research project, TRB defines interoperability as "the ability of different agencies to coordinate and share information so that passengers can travel in a seamless fashion." Travel may occur on public transit, on a toll road or toll bridge; it may include the use of a parking facility. Travel in a seamless fashion is primarily driven by these factors:

- Coordination of transfer points;
- Schedule coordination;
- Simplified and coordinated tariff structures;
- Transfer facilities design;
- Consistent passenger processes and operational procedures,
  - Boarding,
  - Fare payment, and
  - Fare inspection;
- Common interoperable fare media; and
- Convenience in obtaining fare or payment media.

As the previous list of factors indicates, fare payment interoperability is only one factor that affects seamless travel. Contactless technologies' implementation for fare payment, both long and short range, is accelerating across the transportation industry. The capabilities of contactless technologies provide opportunities to allow regional payment coordination across multiple transportation modes. These capabilities also provide an opportunity to pay for products and services beyond transportation.

1.2 Elements of Fare Payment Interoperability

Fare payment interoperability does not necessarily require the use of a smartcard. Figure 1 illustrates the following high-level components to achieving interoperability:

- A manual system relies on human interaction such as visual inspection
- An automated system relies on technology—usually using fare media such as a contactless smartcard to validate interoperability

This research project focused on the automated system using the contactless smartcard as the fare medium. The information and data flows required to achieve smartcard interoperability also applies to other media such as magnetic stripe tickets or radio frequency identification (RFID) tags. The physical medium used for seamless payment is a medium that carries data. The most common is magnetic stripe media; however, a solid-state, silicon-chip-based data carrier, such as the contactless smartcard, is emerging as the preferred technology.

The first step in building an interoperable system is to organize the participants into a formal group. A Participation Agreement binds the participants to follow a set of common rules, also referred to as policies or business rules. At a minimum, the rules must provide the following:

- Technology requirements that include systems and fare media and
- Transaction processing that defines the data to be transferred for processing and when (how often) that occurs.

These rules may also define other business-related aspects such as

- Branding (how the product is to be identified in the market);
- Customer service processes and procedures;
- Sharing of expenses and payment for services;

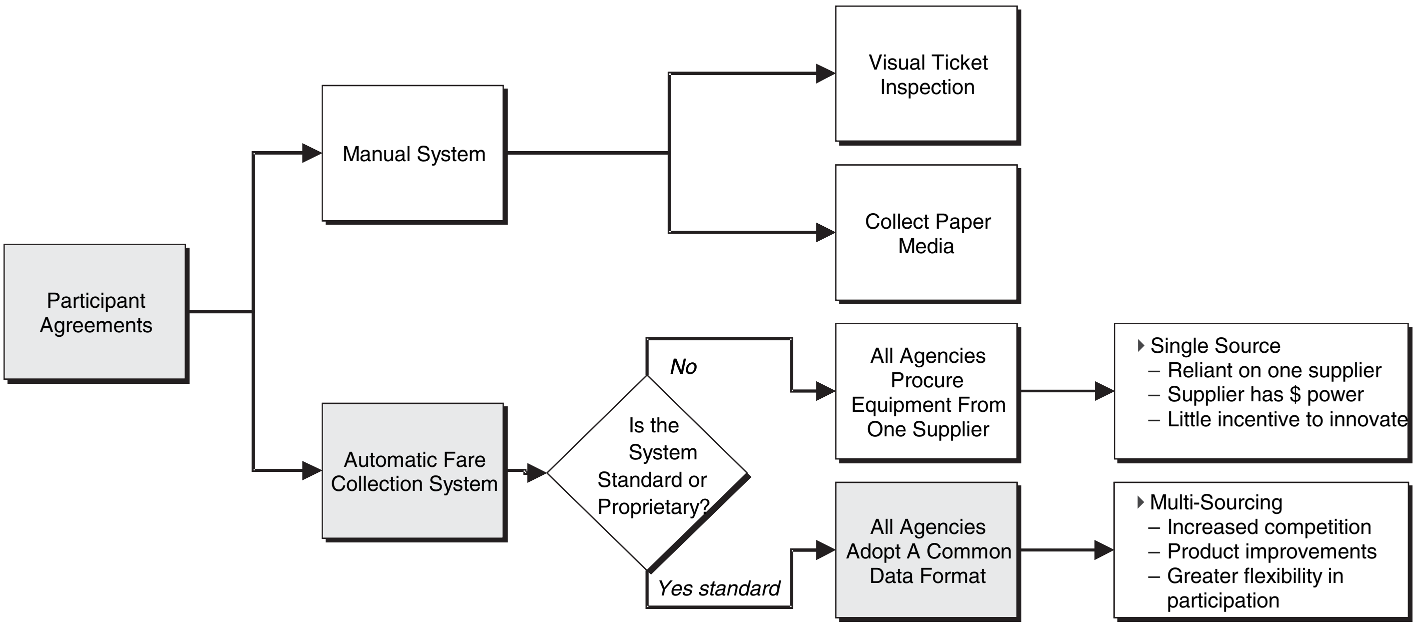

Figure 1. Interoperability model.

- Items controlled by participants;
- Dispute resolution; and
- Legal framework.

The Participation Agreement drives the information requirements for institutional interoperability. Chapter 1 discusses the issues associated with institutional interoperability in detail.

The next step is to define the technical information required to achieve interoperability. The business rules articulated in the Participation Agreement define the information to be exchanged by the interoperable smartcard system. At a minimum, the card-to-reader data format and the data format for transferring the transaction records to a central clearinghouse need to be defined.

The minimum requirements for implementing an interoperable smartcard system can be accomplished by using one of the following approaches:

1. Procuring the technology from a single supplier, similar to Washington, DC, with the EZ Pass Interagency Group (IAG)
2. Developing an interface specification that defines the requirements with which each participant's supplier has to comply, similar to what is done in the financial services or telecommunications industries

1.3 Interoperability Across Regions

Most regional systems implemented across the United States and Canada use a single supplier for a specific region. Each system has unique characteristics and features. To achieve intra-regional interoperability, the business rules and technology need to be synchronized. Figure 2 illustrates the process for analyzing and identifying gaps in the business rule and technology for a specific group of regions. Each time a new region is added, the entire process needs to be repeated. The primary factor for intra-regional interoperability is the cost of making the necessary systems modifications. The most difficult situation to manage is where two competing

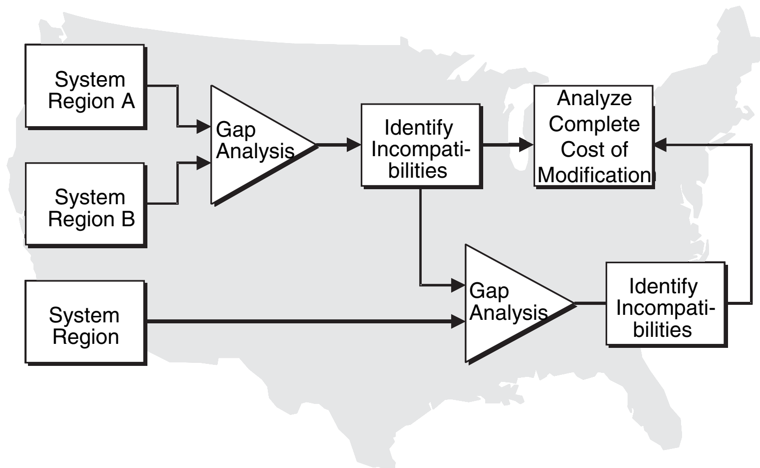

Figure 2. Intra-regional interoperability analysis.

suppliers have to work together to accomplish inter- and intra-regional interoperability, particularly when there is a significant generation gap in the technologies employed.

1.4 Interoperability Beyond Transit

The financial services industry anticipates two types of interoperability opportunities with transportation participants:

- "Real Estate" Sharing on the Card—There are two models. In each model participants do not interact. In one model, an ATM or credit card embeds a chip containing the transportation application. In the other, an ATM or credit card has the transit application resident with the credit and debit card data on the same chip. Table 1 shows the relationship of a shared-chip architecture.
- Card Functionality Sharing—This occurs when the transit application can be used to pay for services beyond transportation or a non-transit payment product can be used to pay for a ride. Table 2 shows the relationship of a shared application structure.

The interoperability elements discussed in this report also apply to interoperability with non-transportation participants. An agreement between the participants must first be established. Once an agreement is established, the interoperable technology solution can be identified and a clear set of business rules developed that, at a minimum, define the following:

- Technology requirements,
- Processes for system operation,

Table 1. Shared-chip architecture.

<table>
<tr><td colspan="7">Multi-Applications</td></tr>
<tr><td colspan="7">Security</td></tr>
<tr><td rowspan="6">Personal Identification (e.g., Drivers License)</td><td rowspan="6">Bank Card</td><td rowspan="6">Digital Signature</td><td rowspan="6">Stored Value (e.g., Coffee House)</td><td rowspan="6">Merchant Loyalty Points</td><td rowspan="6">Transit Application</td><td>Identification</td></tr>
<tr><td>Card Characteristics</td></tr>
<tr><td>Shared Value Purse</td></tr>
<tr><td>Transit Products</td></tr>
<tr><td>Trip Data</td></tr>
<tr><td>Transit Benefits Purse (Pre-Tax $)</td></tr>
</table>

Table 2. Shared application structure.

Transit Application Functions					
Identification	Card Characteristics	Shared Value Purse	Transit Products	Trip Data	Transit Benefits Purse (Pre-Tax $)

- Procedures for exchanging data, and
- Processes for clearing transactions.

The primary reason interoperability has not proliferated beyond transit is the proprietary nature of fare payment systems. Proprietary point of sale (POS) terminals purchased from an automatic fare collection (AFC) supplier for a retail application cost too much for a small merchant to acquire (i.e., approximately $1,200 to over $5,000 per unit).

1.5 Evolution of Interoperability with Open Payment Systems

Now that financial institutions are implementing contactless payment products, a baseline architecture may be used to begin developing an interoperability strategy for transit with open payment systems. Given the recent activities associated with the financial institutions migrating their credit and debit card product offerings to contactless smartcards, the following scenarios for interoperability begin to emerge:

- Acceptance of contactless bank cards on buses and at faregates,
- Two or more transit entities arrange to accept each others' closed stored-value payment products, and
- Acceptance of multiple-payment-enabled devices.

To determine the interoperability requirements with an open payment system, the characteristics of the existing transit payment architecture need to be identified. Currently, all fare collection systems combine payment with the fare calculation into a single application, and payment is embedded in every layer of the system. This type of architecture substantially increases fare system complexity, and allows equipment suppliers to control the application software. Figure 3 illustrates a current conceptual fare payment system architecture.

1.5.1 Acceptance of Contactless Bank Cards

As contactless credit cards proliferate, transit agencies become increasingly attractive customers for financial institutions. The most likely relationship that will emerge between the financial institutions and transit agencies is similar to a merchant in the retail space. Under this type of relationship, transit agencies accept a bankcard for transit fare payment and pay a transaction processing fee to the financial institutions. The key issue is that the bankcard data structure is not designed for conducting fare calculations. Therefore, two baseline system architecture configurations emerge for using a bankcard to pay a fare:

- Transit and credit card applications both reside on the same chip or
- The credit card application only resides on a contactless chip.

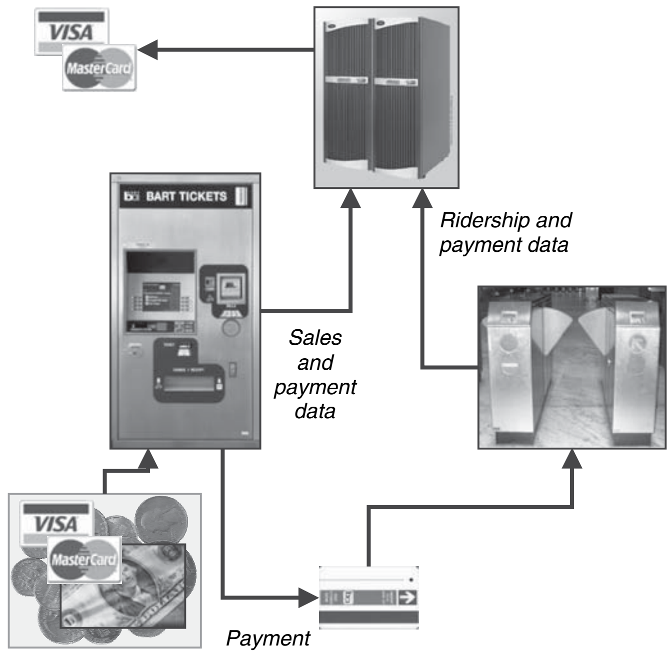

Figure 3. Current conceptual fare payment system architecture.

The transit application residing with a credit card application on the same chip has been the vision for smartcards since the early 1990s. Though technically feasible, the institutional barriers still make this configuration economically infeasible. However, using a contactless credit card product for fare payment is technically feasible in a cost-effective manner if some of the institutional constraints can be modified. The architecture for this configuration is illustrated in Figure 4.

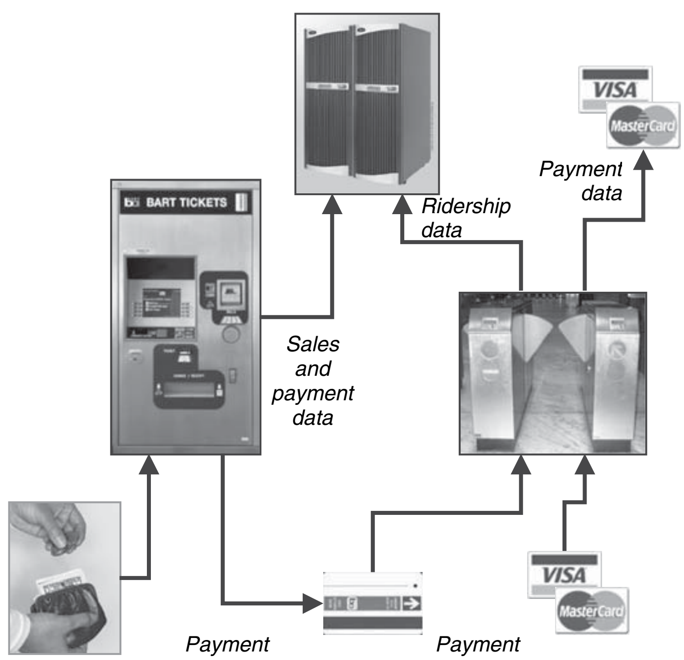

Figure 4. Disaggregation of payment from ridership and fare calculation.

The primary characteristic of this architecture is the disaggregation of payment from the ridership information. Similar to a retail transaction where the cash register calculates the sale, the faregate or farebox conducts the sale. The amount of the sale is transmitted to a POS terminal that processes the card payment. The terminal notifies the cash register when the payment is completed. At this point in the transit world, the faregate opens or the appropriate signal activates or a message displays on the farebox. The application of business rules to provide fare calculation could be accomplished by central server equipment at the agency or region as an offline process at an end-of-day period. Once calculated, an aggregate transaction could be sent to a bank representing a cardholder's transit costs for that day.

The disaggregation of payment from the ridership information collection is an intermediate step in the evolution to open interoperability for fare payment. The key challenge for making this configuration a reality is the cooperation of the supplier community. As subsequently discussed in the Financial Services Industry Interoperability Issues section of this document, the supplier community for the financial services industry has developed readers that can accommodate multiple contactless payment products. If transit adopts this model, most of the data interoperability concerns discussed in this document are alleviated by moving from a data-rich stored-value transit application to the simple recording of a bankcard presentation.

1.5.2 Multiple Closed Stored-Value Payment Products

Closed stored-value products are becoming an increasingly attractive means to create loyal customer relationships. In the retail environment, coffee shops such as Starbucks and Peet's issue closed-account-based stored-value cards. Sports venues are also beginning to recognize the benefits of a contactless stored-value payment media. Two parts are required to create interoperability between disparate closed stored-value systems:

- The need to read participants' cards or payment media and
- Agreement on how settlement will occur.

First, each participant must have a reader that can read the respective cards. The readers must be able to generate a transaction record with sufficient payment data, including time and date, purchase amount, and transaction location. Second, no complex transaction processing system is needed to conduct settlement between two disparate stored-value payment systems. If two closed stored-value payment system operators agree to accept each other's media and the readers can read each payment medium, settlement may occur by using the data collected by each system, as long as the participants trust the integrity of the transaction data generated. This type of arrangement is a referred to as a "trust model," because it requires participants to trust the integrity of the transaction data.

The trust model can create interoperability with less technical complexity and can work with most technologies or different combinations of technologies. The trust model may be used by two or more participants. The transportation council of the Smart Card Alliance has a project under way that would establish a trust model for use in clearing transactions between multiple-party closed-payment systems.

1.5.3 Multiple Payment-Enabled Devices

There are two configurations of payment-enabled devices:

- Transit-enabled contactless chips embedded into devices and
- Devices with transit application (software) that communicates with the reader in a non-ISO-14443-compliant mode (e.g., Bluetooth, 802.11, or infra-red).

The most common payment-enabled device is a key fob with the same contactless chip as a smartcard (e.g., the ExxonMobil Speedpass device). Contactless smartcard chips have also been embedded in mobile phone covers or even into a designated slot in the mobile phone. The primary difference between a contactless smartcard and a key fob or mobile phone cover is the form. Therefore, when a transit-enabled contactless chip is embedded in, for example, a mobile phone cover, interoperability is the same as for transit-issued contactless smartcards, as long as the same contactless chips are used.

Interoperability between devices that have a transit-payment application or a non-transit-payment application that may be used to pay a fare on a bus or at a faregate using a non-ISO-14443 interface will have to be established on an individual basis. The financial services community has evaluated different wireless interfaces for payment and established interface specifications that are available on the Visa website.

1.5.4 Financial Services Industry Interoperability Issues

The financial services industry is in the early stages of rolling out contactless payment products. The only standard that financial institutions have agreed to use for contactless payment is ISO 14443. MasterCard and Visa's payment applications started out differently. The MasterCard application used a separate account number on the card linked to the cardholder credit card account in the back-office system (similar to the ExxonMobil Speedpass architecture). Visa, however, encodes a magnetic stripe image in the contactless chip memory. The card associations are beginning to agree on a common specification for contactless payment. The terminal suppliers are providing POS devices that can read and process all contactless payment products. Terminal suppliers have started developing the necessary middleware (software) to provide merchants with maximum flexibility to choose which contactless payment products to accept.

1.6 Hypothetical Examples—Interoperability Between WMATA and TransLink

To determine what information must be exchanged between systems to create interoperability, two real-world systems were selected for the following hypothetical examples:

- Using a TransLink Card from the San Francisco Bay Area Region to pay for riding a Washington Metropolitan Area Transit Authority (WMATA) bus or train in Washington, DC; and
- Loading value on a SmarTrip card from Washington, DC, in San Francisco to pay a fare to ride a train or bus.

The first element of interoperability that must exist is the capability of the readers of each participant to read and write to cards. For this discussion, the process of reading and writing to the cards is addressed by ISO 14443. The second element is the data to be exchanged between the card and the reader. Such data may also be designated as the transit application. The third element is the transfer of transaction data from the devices (e.g., faregates and add-value machines) to the central processing host. The fourth element is the exchange of transaction data between the participating entities to allow settlement for value loads or uses of the card in the respective systems.

Table 3 shows the minimum information required across a typical AFC system, such as those represented in this case study. The tiers presented in the table begin with the data source for the data input, the card, and end with the data output used to generate the documentation for clearing between WMATA and TransLink, the back-office system.

Table 3. Information required at each AFC system tier.

Card	Card Number	Card Value $	Card Type	Time	Date	Location* (Terminal Number)	Fare Value $	Trans-action Number
	√	√	√	√*	√*	√*		
Payment Device								
Entry	√	√	√					
Exit	√	√	√	√	√	√	√	√
Load Device	√	√	√	√	√	√	√	√
Back Office	√	√		√	√	√	√	√

* Encoded on card for distance-based fare structures

To identify the minimum information required to allow financial settlement between two or more participating entities, which may include a non-transit merchant, the following examples have been developed for each distinct process:

- Information to be exchanged for payment only, NO card loads;
- Information to be exchanged for loading value, NO payment transactions; and
- Process used to determine settlement position by a participant, the aggregation of payments and loads.

1.6.1 Information to Be Exchanged for Payment

Figure 5 identifies the minimum information to be exchanged between each element of a fare payment system—from the inception of the transaction between the card and reader, through

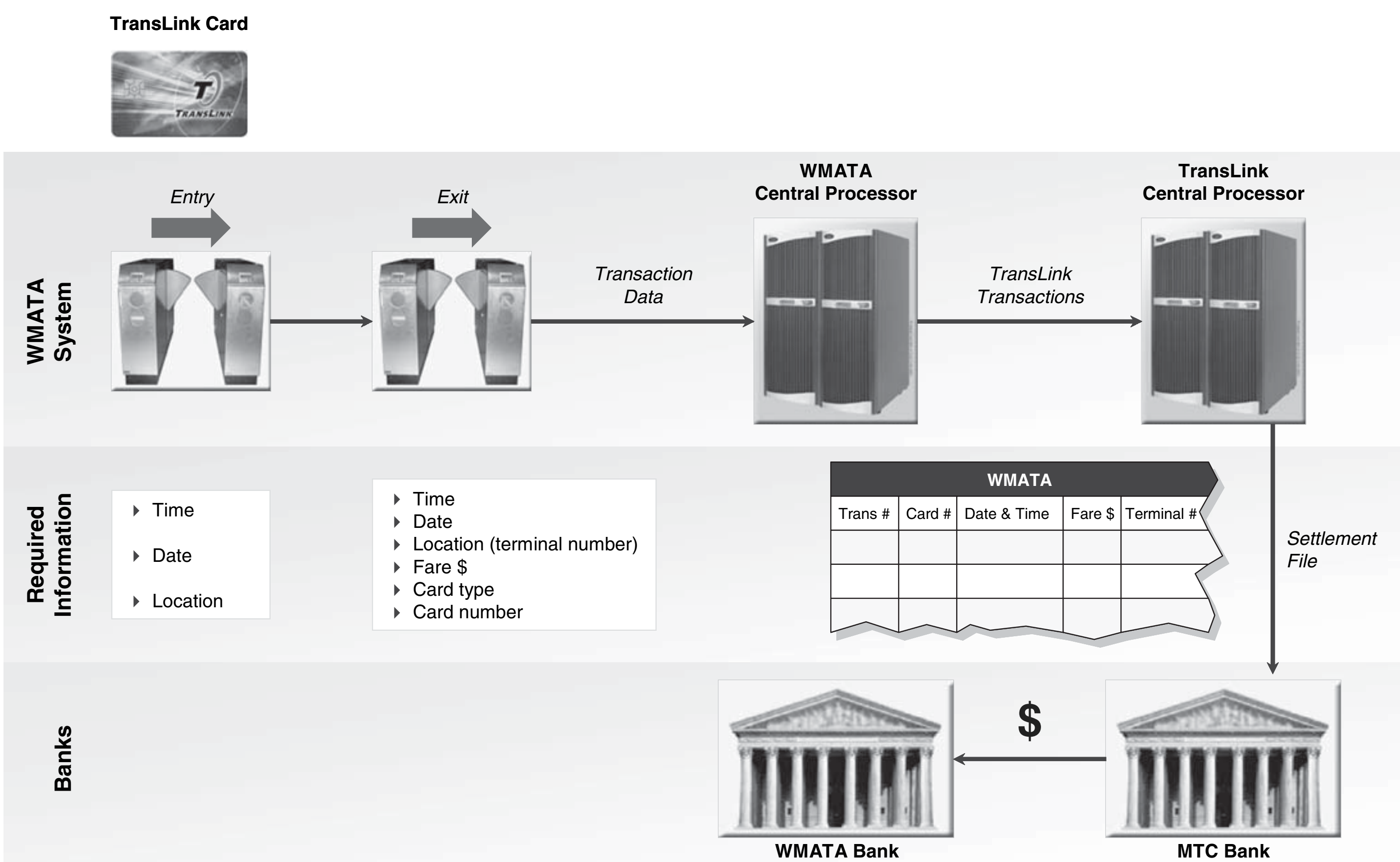

Figure 5. Using TransLink Card to pay at WMATA.

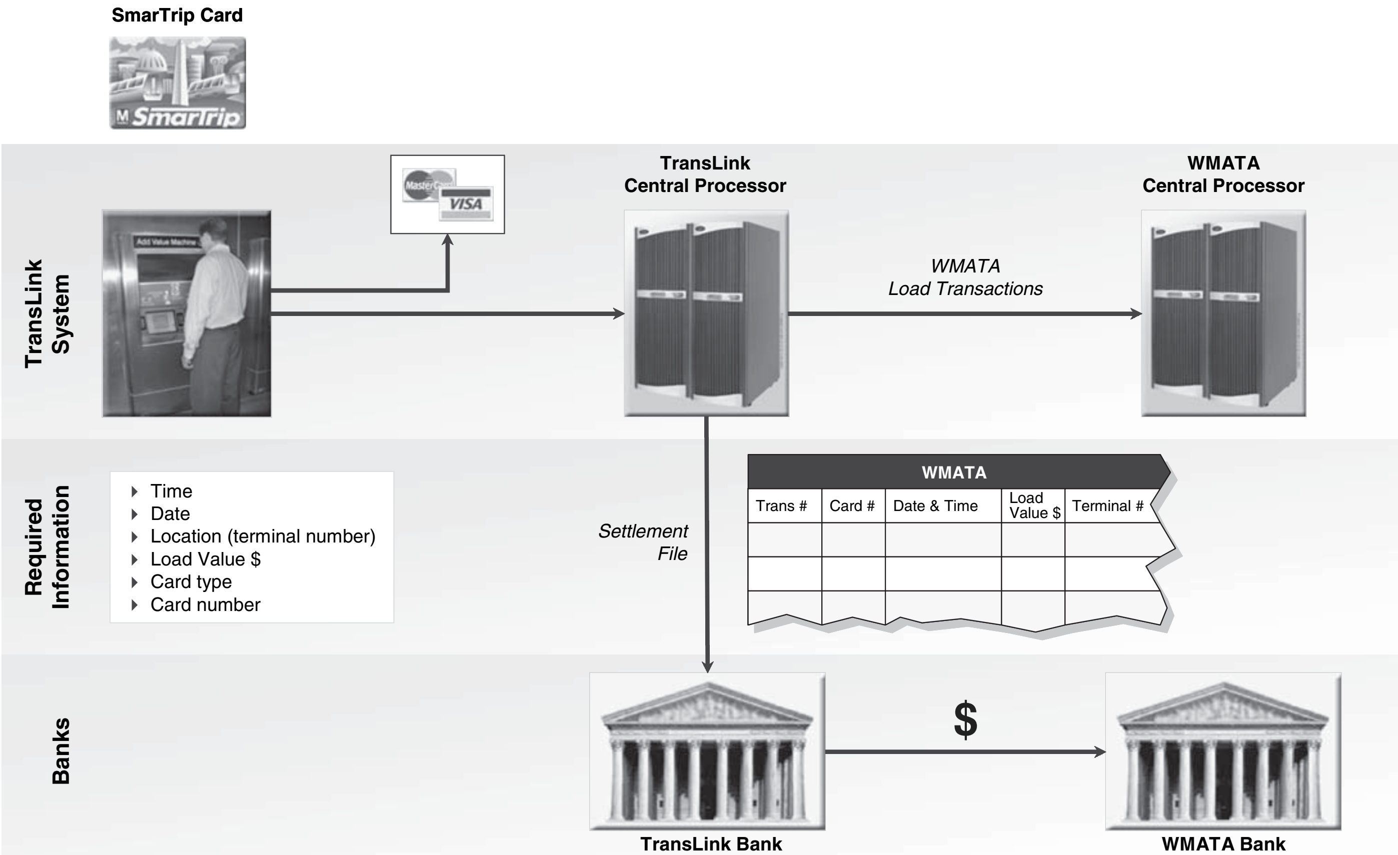

Figure 6. Loading value to the WMATA Card at a TransLink load device.

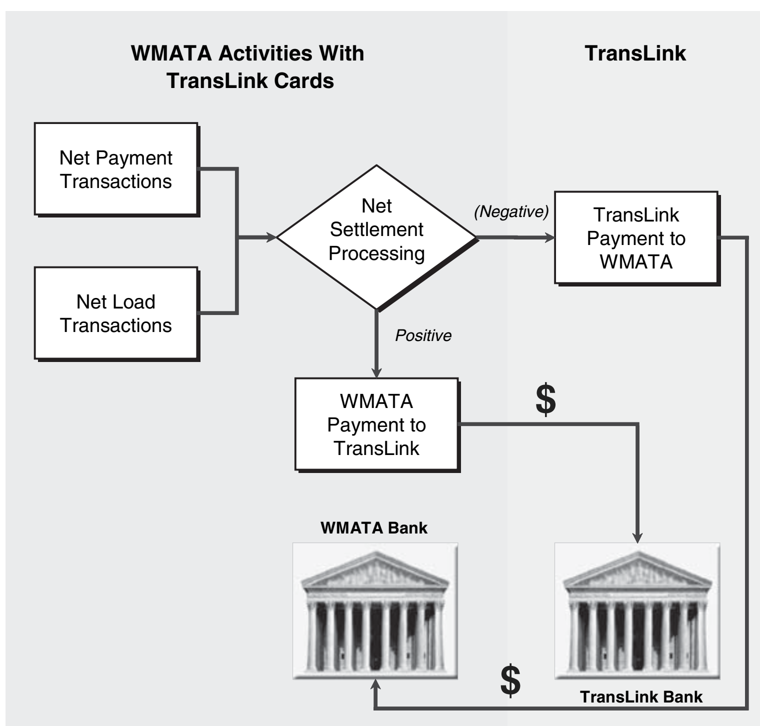

Figure 7. Process for net settlement position.

transfer of funds to the agency bank. This hypothetical example isolates the logic and dataflow to payment transactions only; no loads take place. The payment transactions are also aggregated before transfer between the participants.

1.6.2 Information to Be Exchanged for Loading Value

Figure 6 identifies the minimum information to be exchanged between each element of the load network—from the inception of the transaction between the card and reader through transfer of funds to the agency bank. This hypothetical example isolates the logic and dataflow to loading value only; no payment transactions take place. The load transactions are also aggregated before transfer between the participants.

1.6.3 Process for Determining the Net-Settlement Position

Once an agreement has been established between agencies to accept each others' smartcards for payment, a methodology needs to be set up to allow the "net-settlement" position to be determined. (The net-settlement position is defined as the result of when the net-payment transactions are balanced against the net-load transactions for a specific agency before the information is transferred between participants.)

Net settlement processing does not necessarily need to be conducted by a central computer system. If participants can agree, a spreadsheet using data collected by the fare system is sufficient to determine how much one participant owes the other.

Figure 7 illustrates the logic for determining the net-settlement position before transferring funds between participating agencies' banks.

CHAPTER 2

Findings of Institutional Requirements for Interoperable Smartcard Fare Payment Systems

As the interoperability model shows, the first step toward creating an interoperable smartcard payment system is to identify the institutional requirements of the participants. Fare payment interoperability, regardless of technology used (e.g., smartcard, paper-based, or magnetic stripe) requires significant planning and cooperation among the participating agencies. In the transit industry, agencies have traditionally operated autonomously. Each agency's organizational cultures, policies, procedures, and fare-collection equipment are different.

Transit agencies considering implementing an interoperable smartcard fare payment system must address numerous institutional and technological issues that may create barriers to implementation. This chapter focuses on the key institutional issues that have presented themselves during the implementation of recent U.S. and Canadian transit-based interoperable smartcard projects. This chapter also discusses strategies to overcome these barriers.

The institutional issues have been categorized as follows:

- Management and Organizational Issues—Organizational cultures of the participating agencies and their effects on management decision-making processes;
- Financial Management Issues—The need to ensure that each participant does not lose revenue through participation;
- Patron Impact Issues—Maximizing the use of the smartcard fare payment system by transit patrons (riders);
- Equipment Design Issues—Ensuring equipment interoperability as an aspect of system design; and
- Transit Industry Issues—Impeding the progress of dealing with the behavior of traditional system suppliers.

Institutional requirements are formally documented in a policy statement. The policy statement becomes the reference for making decisions related to a smartcard project.

2.1 Management and Organizational Issues

One of the most significant challenges to interoperable smartcard fare payment system implementation is how the existing organizational cultures affect the participating transit agencies. Creating an interoperable fare payment system requires participating transit agencies to work together. Transit agencies that may have had limited or no previous interaction must work closely with one another for program direction and control.

Key management and organizational issues that need to be addressed on the road to interoperability include

- Establishing a governing body or project sponsor,
- Identifying and mitigating operational differences,
- Establishing a framework for program funding,
- Creating a rollout schedule, and
- Developing a contracting strategy.

2.1.1 Establishing a Governing Body or Project Sponsor

One of the primary challenges of implementing an interoperable fare payment system in a multi-agency environment is encouraging agencies to work together for the overall good of the region and riding public. In many areas of the United States and Canada, transit agencies work autonomously toward accommodating the needs of their patrons. As a result, agencies become accustomed to controlling all decisions. Operational decisions are made that preclude the sharing of resources and limit effective cooperation with peer agencies.

One of the first steps in implementing any regional fare payment system is to establish a governance structure, which will identify the institutional oversight structure and define the following:

- Items under regional control,
- Documentation of the governing structure, and
- Participant representation.

The governing body oversees the common elements of the interoperable fare payment system, which may include third-party services. Table 4 lists the different types of governing bodies. Participation in a governing body may require an agency to cede complete control over the common elements of the interoperable system. Even agencies that have an excellent working relationship may find adapting to a common governing body challenging.

The planning and implementation of a smartcard-based interoperable fare payment project is a long and often difficult process. Once the governing body is established, a project sponsor needs to emerge to direct the effort and provide leadership for the participants. It is critical that the full commitment and support of the member agencies are obtained and that a clear management

Table 4. Overview of different types of governing bodies.

Approach	How It Works	Where Used
Corporation with Privately Held Shares	Private, For-Profit Corporation • Shareholders include private transit and public operators • No majority shareholder • Not all participants are shareholders	• Hong Kong
Single Operator Owner	Owner Agency Makes Decisions • Contract specifies requirements and obligations	• London
Joint Powers Authority (JPA)	Independent Legal Entity • Created under powers of existing public entities • Composed of public entities	• Singapore
Memorandum of Understanding (MOU)	No New Organization • Specifies decision making and participation • Contractually created governance structure	• Los Angeles • Seattle • San Francisco • San Diego • Washington, DC

structure is in place before starting planning and design. The three most common types of project sponsorship are lead agency, regional planning organization, and management committee.

2.1.1.1 Lead Agency

Delegating project management to one lead agency may be an option in a region where a regional transportation planning organization does not exist or where one agency has the critical mass for establishing a system for meeting its own needs cost-effectively. The system implemented by the lead agency is used by the other participants. All participants share the cost of common services, but pay separately for any additional capabilities to meet their specific needs. A lead agency's responsibilities are similar to those of the regional planning organization. In general, a project often benefits from a shorter design and implementation schedule when a lead agency is responsible; this can result in cost savings. The challenge for the lead agency is establishing the agreements with the participating agencies.

2.1.1.2 Regional Planning Organization

The project may also be managed by a regional transportation planning organization. A regional planning organization's responsibilities are similar to those of a lead agency and management committee. For this option, the regional planning organization solicits each member agency for input on agency-specific issues before making design decisions. The project often benefits from a shorter design and implementation schedule—this can result in cost savings; however, the specific needs of participating agencies may be overlooked or not fully addressed in the interest of moving the project forward.

2.1.1.3 Management Committee

Regions that lack a lead agency or a regional planning organization to champion the interoperable fare payment project may elect to form a management committee to oversee the project. Each of the participating agencies is represented on the management committee. Each of the member agencies on a management committee can actively participate in project decisions.

The management committee must be established early in the project life cycle in order to avoid spending valuable time and resources revisiting early project decisions. Management committee responsibilities may include critical functions such as

- Preparing a governance plan—A governance plan documents the rules and bylaws by which the interoperable project operates, including areas such as dispute resolution and decision-making regarding new service offerings and addressing member agencies that leave or join the program;
- Identifying the type of integrator contract—This includes identifying the types of services procured or addressed in house and who will act as the contract administrator;
- Assigning member roles and responsibilities—This includes how and when design reviews are completed and obligations regarding attendance at project meetings;
- Drafting interagency agreements—This addresses subjects such as project cost allocations and information-sharing arrangements; and
- Developing technical direction—This includes adherence to established standards and adoption of system features.

A management committee structure requires special consideration of the contracting strategy. Given that contracting relationships must be formed between two legal entities, the management committee may need to assign a lead agency or a regional planning organization as the contract owner for the project.

Based on the surveys conducted for this project, governance issues are being resolved for most of the projects. Most projects proceed without first establishing the governing body. Projects (including those in New York; Washington, DC; Atlanta; and Los Angeles) start with a lead agency implementing a new AFC system to meet their immediate needs and then expand the use of the new AFC technology to other agencies in the region.

2.1.2 Identifying and Mitigating Operational Differences

Another challenge agencies face during the implementation of an interoperable fare payment system is the differences in the way the participating agencies conduct business. For example, many of the largest agencies have extensive internal capabilities, including technical and operational resources to support most, if not all of their design, operational, and maintenance needs. The trend to consider outsourcing to fulfill these same needs is increasing. Agencies that have extensive in-house resources tend to prioritize more control over their operations; thus, those agencies tend to avoid outsourcing. The different organizational operations philosophies of the agencies must be examined, and compromises must be considered to achieve interoperability.

There are two primary dimensions for implementing the system-related service functions of an interoperable system:

- Centralized—One entity performs all the functions.
- Decentralized—Each participating entity is responsible for performing its own functions according to established business rules.

The project sponsor must decide between a centralized or decentralized approach and must also decide whether the services are delivered using in-house or outsourced resources. The operational philosophies of the participating agencies will determine the approach used for performing card-system-related functions. Table 5 summarizes the key characteristics of the centralized and decentralized approach.

When choosing the delivery and service approaches, the following factors must be considered:

- A function should be centralized when it is more relevant for the patron to experience a consistent level of service across all participating agencies. Centralization of functions creates increased efficiencies.
- A function should be decentralized when it is more relevant to an individual agency's operations.
- A function is a candidate for outsourcing when
  - The function performance levels are easily quantifiable and measurable.
  - The function requires particular technical or skill-based expertise not available within an agency.

Table 5. System service approach.

		Delivery Approach		
		In-House	**Outsourced**	**Hybrid**
Service Systems Approach	Centralized	One agency performs the services for all other agencies	A selected third party performs the functions for all agencies	N/A
	Decentralized	Each agency performs the functions for itself	Each agency selects a third party to perform its functions	Some agencies select a third party while some agencies perform the functions themselves

– The function may need to scale up or down, depending on demand or utilization levels.
– There is potential for the provider to share the service across multiple projects.

Table 6 identifies the primary card service functions that need to be addressed in an interoperable smartcard-based fare payment system.

For many implementations, a mix of centralized and decentralized approaches will be the most beneficial. By adopting this hybrid approach, a region can take advantage of existing capabilities and maintain individual agency culture while also maintaining consistency of service across the region.

2.1.3 Establishing a Framework for Program Funding

Interoperable fare payment systems require a substantial capital investment for required equipment and systems. Funding for a project of this magnitude will likely come from multiple sources because of multiple agencies' participation. The challenge with multi-jurisdictional funding is to arrive at an equitable formula that each of the participating agencies can endorse.

Project funding requirements need to be determined early in the project life cycle to provide adequate time to meet the requirements for securing the funding. Member agencies also need to evaluate the benefits derived from the capital investment. The cost-benefit analysis helps to identify expensive features that do not create value. However, regional systems need to be sufficiently flexible to scale as the participating agencies needs change and grow more sophisticated.

Table 6. Primary card service functions.

Function	Description
Card Management	Includes issuance and fulfillment of all smartcard stock and management of patron account systems
Distribution Management	Involves managing card inventory and deployment to merchants, employers, and other institutions
Security Management	Includes management of all system security, including key and secure access module (SAM) management, fraud management, negative list management, application blocking, system access and controls
Patron Services	Includes providing support to the transit agencies participating in the regional system, cardholders who use the regional smartcard, and retail/distributor merchants providing third-party services
Financial Management	Includes: clearing and settlement services, funds movement processes and services, funds pool management services, revenue collection activities, general accounting for the smart card program, financial reporting services for the smartcards, and auditing services for the smartcard program
Infrastructure Systems and Operations Management	Includes management of the systems interface, network, application software, configuration control, device management, upgrades, and disaster recovery
Program Management	Includes management of the regional program, including brand management, regional program administration, policy shifts, and non-financial reporting

Development of the business case is critical in defining the funding strategy. The business case identifies the estimated capital and operating costs for the project and possible future expansion of the system. At a minimum, the business case consists of the following parts:

- Estimated capital cost of the system;
- Existing operating costs;
- Operating and maintenance costs after system implementation;
- Schedule for implementation;
- Risk factors;
- Initial operational cost (start of revenue service); and
- Regional/management/lead agency oversight, administration, and management.

Identifying specific funding sources for the interoperable fare payment project starts when the preparation of a business case is completed. The completion of the business case provides the basis for determining the relationship of capital investment balanced against long-term operating costs.

Once the specific sources of funding have been identified, funding agreements between the participating agencies need to be created. The inter-agency funding agreement establishes the level of capital investment and operating funding for which each participating agency is responsible. A commonly used strategy for allocating costs is to have each agency responsible for the deployment of its respective interoperable system components and to share operating costs based on use of the shared system components. Several formulas exist for distributing the operating costs among the member agencies. Existing projects have based these formulas on actual transaction volume, transaction dollars processed, or a combination of both.

2.1.4 Creating a Rollout Schedule

An overall project rollout schedule must be developed that details milestones for design, equipment production, testing, and implementation of the interoperable fare payment system across the participants. The rollout schedule is a critical component of operating cost. Because transaction processing and shared service, such as operating a call center, is a transaction-based business, the higher the volume, the lower the cost per transaction or call, respectively. The guiding principles to consider when developing the rollout schedule include

- Realistic milestones reflective of actual experience,
- Ability to fit within contractors' capabilities,
- Ability to be supported by the participating agencies,
- Customer reaction and acceptance to change, and
- Schedule changes in response to changing customer needs.

System rollout can follow one of two approaches:

- Phased—Different agencies and functionalities are brought on line at different times. This approach is the most common because the disruption caused by patrons having to learn a new behavior is isolated to a specific area and thus is less resource-intensive to manage.
- Full Rollout—All agencies and equipment are brought on line at the same time. This approach requires extensive testing and careful preparation to successfully launch. In addition, significant resources are required to manage the first days of operation.

The phased approach is typically adopted when the procurement is split among multiple supplier contracts. Risks associated with a phased approach include the possibility for patron confusion when the system works for limited agencies or has limited capabilities. Additionally, a phased approach needs to consider agencies that share existing fare products such as a period pass. The rollout of these agencies will need to occur simultaneously to avoid affecting patrons who use the common fare product.

Although it is more "patron friendly," a full system rollout is more likely to disrupt operation for the agencies. Project resources must be spread over a wider range and are less able to focus on those areas that may experience issues such as high degrees of confusion and lack of patron education. Additionally, unlike a phased approach, a full rollout does not afford the benefit of "lessons learned" from the earlier implementations.

Figure 8 identifies potential rollout strategies and the progression of each strategy.

Other issues that will affect the scheduling of the interoperable project include

- Availability of staffing resources,
- Availability of financial resources,
- Agency operations, and
- Patron education and orientation

2.1.5 Developing a Contracting Strategy

Participating agencies need to determine and agree on how the equipment and services will be procured. The main contracting challenge is deciding whether to procure the equipment and services under a single contract or through multiple contracts. Each approach has challenges that must

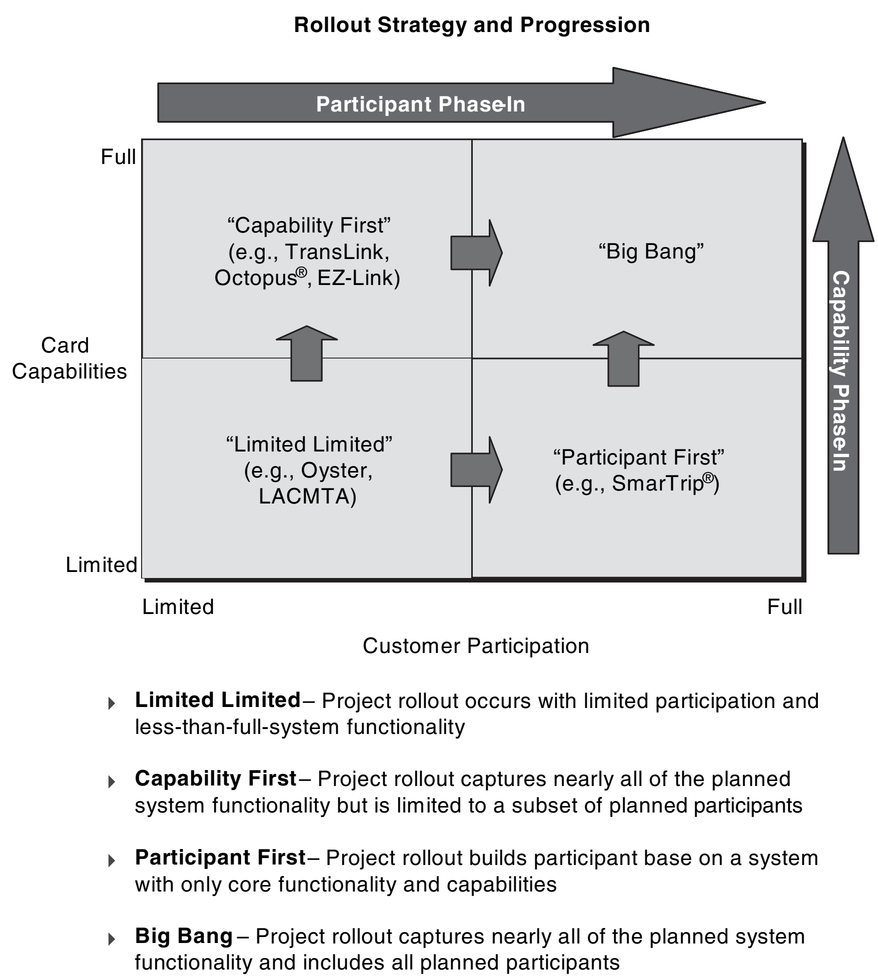

Figure 8. Rollout dimensions.

be overcome, and the selection of the approach will depend on factors such as an agency's appetite for integration risk, the availability of technical and project management resources, and the level of equipment and services to be procured. The most common contracting strategies are single procurement and contract, multiple procurements and contracts, and contract type selection.

2.1.5.1 Single Procurement and Contract

Procuring all equipment and services under a single contract transfers most of the integration and interoperability risk (faregates, fareboxes, ticket vending machines (TVMs), card readers, and back-office systems) to the contractor. The contracting agencies have a single point of responsibility for lack of performance. The single procurement approach can accommodate a more aggressive rollout schedule because the schedules of multiple procurements and contractors do not have to be coordinated. However, the single procurement approach may be less competitive because of the limited number of suppliers for highly specialized equipment (e.g., the farebox). Therefore, the procurement will result in fewer bids.

2.1.5.2 Multiple Procurements and Contracts

By choosing to procure the equipment and services separately, agencies are likely rewarded with more competitive procurements and lower costs for "best-in-class" elements of the system. However, the risk of integrating the services and equipment supplied under separate contracts will be borne by the contracting agencies. Another variant of the multiple procurements approach is to contract with a systems integrator to take responsibility for pulling separate pieces together and ensuring interoperability. While a systems integrator may be better equipped to deal with technical and programmatic issues than the contracting agencies, this approach may also result in a higher cost than self-selected teams because each supplier must factor in a fee for technical and management issues caused by the systems integrator during the contract's execution. In either case, the integration of multi-vendor equipment will result in higher overall system cost initially because of the increased software development and testing that result from the task of integration.

2.1.5.3 Contract Type Selection

The type of contract structure must also be decided. The contract structure is driven by the types of services that the participating agencies can support and their current way of doing business. For example, if the member agencies decide to outsource clearing and settlement, patron support, and card management, a design-build-operate-and-maintain (DBOM) contracting structure may be advantageous because the contractor will design the system so that operating costs are balanced against the selection and cost of equipment components. If, on the other hand, the member agencies decide that these services will be supported in house, design-build contracting may be a better alternative. The challenge is to choose a type of contracting that takes advantage of existing in-house resources with minimal overlap.

2.1.5.4 Other Management Strategies

To help address contracting issues related to interoperability, most U.S. and Canadian deployments have retained the services of consultants specializing in transit and electronic payments. As an outside party with best practices developed over multiple projects, experts can assist the participating agencies with overall program strategy, document preparation, procurement assistance, and critical decision making throughout design and implementation. Using outside expertise can also serve to moderate the partisanship that can develop among the participating agencies and between suppliers. The outside expert provides an objective view based on best practices from other industries. Using the services and expertise of outside consultants will add initial cost to the project, but has proven to lower integration risk. Lowering integration risk prevents contractors from taking control of critical parts of an interoperable fare payment system and using this control to generate supernormal profits during the program's life cycle.

2.2 Financial Management Issues

Financial integrity is the highest priority for any agency participating in an interoperable fare payment system. This section discusses the key financial management decisions and issues that must be addressed, including

- Transaction clearing and settlement,
- Funds pool management, and
- Financial exposure risk associated with advanced features.

2.2.1 Transaction Clearing and Settlement

In a fare payment program where multiple operators are selling fare value accepted by more than one operator, transaction clearing and settlement allows each agency to be reimbursed for the services provided, regardless of where the fare product is purchased. Again, the challenge is obtaining agreement from all participating agencies on an approach to transaction clearing and settlement. As presented in Section 2.1.2, clearing and settlement can be accomplished applying either a centralized or decentralized model.

2.2.1.1 Centralized Clearing and Settlement

In a centralized clearinghouse, all transaction information (purchases and fare payments) is transmitted to a central system where the net settlement position for each operator is calculated, usually by using settlement software. Differences in sales versus usage will determine whether a given member agency is owed or owes money. The centralized model can be performed in house by one of the member agencies or outsourced to a third party.

2.2.1.2 Decentralized Clearing and Settlement

In a decentralized clearinghouse, the member agencies establish financial relationships with each other to enable the movement of funds. The decentralized model often takes advantage of existing infrastructure, but, because of multiple points of aggregation, effort is often duplicated.

In both centralized and decentralized models, the frequency at which settlement occurs must be decided by the participating agencies. In a high-transaction environment where large amounts of money are involved, settlement is usually performed daily. However, in an environment where transaction volume is relatively low or where an agency's existing procedures have revenue collection performed at intervals of multiple days, the increased cost of daily settlement may not be warranted.

2.2.1.3 Clearing and Settlement Strategies

The finance departments of the participating agencies must be intimately involved in the project to address financial management decisions. Ideally, a separate finance committee—consisting of financial professionals supported by technical experts from each agency—should be formed. This type of organization is necessary given the responsibility of having to make decisions that affect the movement and management of funds within interoperable fare payment systems. The finance committee would decide whether clearing and settlement should be centralized or decentralized.

2.2.2 Funds Pool Management

The funds pool is created as a result of revenue collected (card loads) but not yet used in the system. The funds pool may be in a central account managed on behalf of the participants or it may be a "virtual" funds pool where each agency holds its own share of the total amount. Examples of how the money within the funds pool can be used are

- Periodic movement of funds between member agencies to compensate for fare payments, purchases, or loads by one participant's cardholders on another participant's system;
- Periodic payment of transit services used by cardholders; and
- Coverage of charge-backs for transactions that should not have been posted.

Revenue is generated by investing the funds pool float (i.e., interest earned on unallocated funds) contained within the funds pool. The member agencies must decide how the float should be invested [e.g., certificates of deposits (CDs) or money markets] so that the money can grow in a low-risk manner, or alternatively, how the funds may be used to meet the working capital needs of the agencies. It can be a challenge for the member agencies to agree how to allocate the float.

2.2.2.1 Funds Pool Float Strategies

Regional programs that have followed a central clearinghouse model have developed float allocation formulas to arrive at how revenue from e-cash sales within the funds pool float is distributed among the participating agencies. The formulas are typically tied to the amount of electronic purse (or transit-specific purse) loads that occur on equipment at a given agency. Responsibility for negotiating the float allocation formula is usually assigned to the finance committee.

2.2.3 Financial Exposure and Risk Associated with Advanced Features

Smartcard technology allows for features not supported by other fare payment technologies, including

- Autoload—The automatic loading of fare value once a specified threshold is reached; and
- Balance Protection—Value replacement insurance if a card is lost or stolen.

Although beneficial to both the patron and agency, these features represent a potential risk for the member agencies. The challenge for participating agencies is agreeing on a common way of managing the risk of added functionality.

2.2.3.1 Autoload

The autoload feature involves linking a smartcard to a debit or credit account that automatically adds funds from the account to the smartcard when a predetermined value threshold is reached. Depending on how the feature is implemented, autoload can result in a situation where a card has been loaded with additional value before receiving bank authorization to debit the linked account.

The autoload feature can be implemented following one of two models. In a post-funded autoload model, the card is loaded with additional funds once it reaches a predetermined threshold, and the funds are then subsequently obtained from the linked account. In a pre-funded autoload model, when the card balance falls below a predetermined threshold, a load request is initiated, the funds are obtained, and the card is loaded with the additional value on the next entry to the system. An additional pre-funded autoload type is a directed autoload, where the patron requests a load of the card for a given value and the funds are approved in advance of an autoload issuance.

2.2.3.2 Balance Protection

The balance protection feature replaces the value that was on the card when it becomes lost, stolen, or damaged. The balance protection can also leave the member agencies at risk of losing fare revenue. If a card with balance protection is lost or stolen, the risk of the card being used before being "hot listed" (or negative listed) needs to be covered. Agencies must be comfortable that these liabilities present acceptable risks.

2.2.3.3 Strategies for Overcoming Risk Factors

The risk of adopting features such as autoload and balance protection can be further defined by developing cost models that quantify these features in terms of cost versus economic benefit. Both of these features are as much an agency benefit as a patron benefit. For example, patrons who understand that balance protection can alleviate the concern of losing a card's stored value are more likely to embrace the fare payment system. This may, in turn, increase transaction volume and shift more fare collection to electronic media and away from cash, thus resulting in cost savings.

A similar case may be made for autoload, whereby the adoption of the feature lowers the use of traditional vending equipment, resulting in lower maintenance and cash-handling costs. The risk of autoload to the participating agencies may be further mitigated through the adoption of the pre-funded model. However, the pre-funded autoload transaction is a more complicated and less patron-convenient transaction given that it may be a two-step process.

2.3 Patron Impact Issues

The rollout of an interoperable smartcard-based fare payment system introduces technologies and policies that are likely to be new and unfamiliar to the transit patron. The business case for the fare payment system depends heavily on the level of acceptance by the patrons. For these reasons, the implementation needs to consider three key areas affecting the patron:

- Technology,
- New processes, and
- Convenience.

2.3.1 Technology

Most transit ridership has not been exposed to smartcard technology, which is a new medium for payment. Patrons already familiar with magnetic media and stored value of pass products will find the conversion less of an inconvenience. When introducing a new fare payment system, resistance to change must be anticipated and mitigation measures must be implemented. Worldwide experience has proven that transit users embrace contactless smartcard technology because of its ease of use. A few riders are hesitant to use the card because of concerns about privacy resulting from a lack of understanding of how the data are used. Additionally, features such as autoload, which benefit both the cardholder and the participating agencies, require educating the ridership on the benefits provided.

2.3.2 New Processes

Depending on the type of service model implemented, cardholders who require assistance with their cards may be required to call a separate service center and not the transit agency. Although this approach can provide an efficient and consistent level of service across a region for card-related issues, it can create confusion for cardholders. The decentralized customer service approach often minimizes this confusion to the cardholder because the patron would continue to call the agency. However, an agency would probably have to increase customer service staffing levels. A compromise of these approaches may lie in having the cardholder call the agency directly and then having the agency forward the call to a central service center. This would allow for a centralized customer service and maintain the convenience of agency contact for the cardholder.

2.3.3 Convenience

Based on the experience in San Francisco and Washington, DC, patrons in other regions will most likely embrace a regional interoperable system once they understand the increased convenience this type of fare payment system offers. The challenges of the new technology and process are minimized once riders gain an increased understanding of its use. Other changes, such as a business decision to allow the balance on a card to go negative in either value or rides, will, at the beginning, contribute to cardholder confusion.

2.3.4 Strategies for Overcoming Patron Impacts

Global experience indicates that transit riders quickly see the benefits of switching from cash or magnetic and paper fare media to contactless smartcards. However, to make the transition less disruptive, transit systems must either develop and implement a comprehensive patron education and marketing program to ease the transition to the interoperable smartcard system or adopt a slow, gradual rollout approach similar to SmarTrip. A comprehensive education program is ongoing and provides accurate information. Examples of education materials used include

- Fact sheets, bulletins, newsletters, and websites;
- Public meetings hosted by the transit agencies;
- Presentations to targeted groups;
- Advertisements on vehicles, radio, or television;
- Direct mailings;
- Local publications;
- Clear and simple instructions placed on the card; and
- Supplemental staff at high-traffic locations as customer service ambassadors.

Transit systems may consider offering cardholder benefits, such as loyalty programs, to increase smartcard penetration. A loyalty program is a promotional program in which benefits, such as discounted fares, are credited to a cardholder's card for using the system. Interoperable systems can significantly increase card use by restricting the purchase of certain fare products only to the smartcard. For example, one of the agencies in San Francisco's TransLink plans to restrict its monthly pass purchases to TransLink cardholders only. This concept can also be applied to the issuance and acceptance of transfers.

2.4 Equipment Design Issues

One of the primary challenges posed by existing equipment designs is to find a way to procure interoperable equipment from multiple vendors in a competitive manner. The goal is to build a fare payment system that conforms to open standards or specifications, uses existing infrastructure, offers flexibility to scale, and adds functionality as needs develop. Thus, open standards and specifications will enable the participating agencies to add equipment and functionality competitively and use the open platform to establish new opportunities for partnerships with non-transit applications.

A secondary challenge for the member agencies is to determine the degree to which legacy systems are either upgraded and integrated into the new interoperable fare payment system or replaced with new equipment. The cost to replace may be less than the cost of upgrading and integrating legacy systems.

The age of legacy systems and their incumbent technology are key factors in the cost of upgrade. Each agency's legacy equipment will need to be reviewed to determine whether it can be upgraded to the new technology and industry standards of the interoperable system. A useful tool to help determine the best approach is the preparation of a comprehensive value analysis. The value analysis balances the life cycle cost to acquire and maintain the new equipment against the cost to upgrade and maintain the legacy equipment for the useful life of the fare payment system. In addition to the capital cost of new equipment and normal operating and maintenance cost, key components of the value analysis need to include

- Useful service life of equipment and systems,
- Life expectancy of the equipment,
- Cost of spares or replacement devices,
- Residual value of legacy equipment,
- Expected reliability, and
- Operational improvements and customer convenience.

2.5 Transit Industry Issues

This section discusses the issues that exist within the transit industry that may impede efforts to adopt a common smartcard specification. Chapter 3 identifies the components and information that need to be exchanged to achieve interoperability. A smartcard specification needs to define items such as data elements, objects, API, and an APDU command set for an interoperable fare payment system. The issues for discussion are categorized as follows:

- Business justification,
- Supplier behavior, and
- Supplier compliance with available standards.

2.5.1 Business Justification

One of the primary goals of interoperability is to provide transit agencies with the ability to multi-source their equipment procurements. The ability to access multiple suppliers for equipment and system purchases increases competition in the market place, usually resulting in lower pricing. However, in today's market, many smartcard-based fare payment implementations are based on proprietary system architectures that do not conform to common interface protocols. This situation may inhibit any attempt to implement regional interoperability among transit providers.Furthermore, the challenge and the cost of adopting an agreed-on standard after a proprietary system development may be prohibitive and may even prevent post-deployment regional-interoperability efforts.

Another goal of interoperability is to provide the transit patron with a seamless means to pay for travel across multiple transit systems. This goal has already been achieved at regional levels using systems and equipment incorporating varying degrees of proprietary design. For a standard to be relevant, it needs to be universally adopted by the institutions that it benefits. Without a critical mass supporting a standard or specification, the standard or specification becomes ineffective. The strong business case for compliance does not materialize in the initial stages of adoption. However, as adoption progresses, economies of scale begin to materialize.

2.5.2 Supplier Behavior

Proprietary solutions are used to create barriers to entry and lock transit agencies into long-term contracts. Standards and common open specifications can remove the barriers created by proprietary technologies, thus allowing transit agencies more choice and making interoperable fare payment systems possible. Proprietary solutions were developed long before standardization discussions began.

Once proprietary technology hurdles have been removed as a barrier to market entry, suppliers need new ways to distinguish themselves from competitors. Frequently, suppliers may attempt to accomplish this by lowering price, providing better service, adding features, or improving the reliability of their equipment and systems. From the supplier perspective, loss of pricing power is clearly undesirable. Therefore, attempts to impose a common standard or specification on the equipment suppliers probably will be resisted.

2.5.3 Supplier Compliance with Available Standards

Even with a clear business case, other incentives may be necessary to achieve universal acceptance of a standard. One strategy would be to link standard conformance to capital-funding grant approval. In this scenario, FTA funds for smartcard implementations could only be available for projects that agree to conform to a common standard. However, this strategy can only be applied to new projects. Such an approach would require the governance of a large body of funding such as the FTA. A slightly different approach to this strategy, one that focuses on rewarding an adopting agency versus imposing a penalty, is to make special funding available to agencies that elect to adopt the standard.

CHAPTER 3

Findings of Peer Review of Interoperable Smartcard Programs

This chapter compares the interoperability of programs currently implemented or under development. The research identified similarities and differences in the system features, the data exchange, and the policies for selected peer agencies, and begins to establish benchmarks and best practices for developing interoperable smartcard systems for transit.

Establishing the benchmarks and identifying best practices is based on conducting a detailed survey of agencies that have implemented or are in the early stages of implementing a regional smartcard fare payment system. Most agencies surveyed are U.S. and Canadian transit operators, because the legislation under which U.S. and Canadian transit agencies operate limits the commercial opportunities for innovative business arrangements such as establishing corporations and issuing shares for participation in a business similar to those in Singapore, Hong Kong, or Europe. Fully implemented regional smartcard fare payment systems in Asia and Europe have been operating longer than any in the United States and Canada. Because the international projects continue to serve as benchmarks throughout the world, they have also been included in the survey.

The research focused on identifying the information exchanged between participating agencies. The survey data are intended to provide a benchmark for comparing the data elements critical to achieving fare payment interoperability. These critical elements are identified in Chapter 4. Key policies affecting interoperability are also part of the survey, because establishing policies that tie agencies participating in an interoperable fare payment system together is equally important to technology decisions. Moreover, the findings and current trends both within and outside the transit industry are compared. Particularly, adding non-transit services (or becoming interoperable with non-transit services) affects the data elements to be exchanged.

The primary sources of information were transit agency personnel and project managers who have or have had direct project involvement. Secondary sources of information consisted of a literature review (particularly websites and project documentation). The research team's direct involvement through engagements with the planning, design, and implementation of many of the systems served to substantiate the information provided by primary and secondary sources.

The regional (interoperable) fare payment systems reviewed in this chapter are

- SmarTrip—Greater Washington, DC, Metropolitan Area, Maryland, Northern Virginia (www.wmata.com/riding/smartrip.cfm)
- TransLink—San Francisco Bay Area (www.mtc.ca.gov/projects/translink/translnk.htm)
- Chicago Card—Chicago, IL (www.chicago-card.com)
- Central Puget Sound Regional Fare Coordination (RFC) Project—Seattle, WA (http://transit.metrokc.gov/prog/smartcard/smartcard.html)
- Go-To Card—St. Paul-Minneapolis, MN (www.mvta.com/tafsinformation.html)

- Orlando Regional Alliance for Next Generation Electronic Payment System (ORANGES)—Central Florida (http://www.pbsj.com/what/Core/ITS/projects/ORANGES/)
- Go Ventura—Ventura County, CA (www.goventura.org)
- Transit Access Pass (TAP)—Los Angeles County, CA (www.mta.net)
- Compass—San Diego County, CA (sdcommute.com)
- EZ-Link—Singapore (www.ezlink.com.sg/index.html)
- Octopus—Hong Kong (www.octopuscards.com/eng/customer/apply.jsp)
- Oyster—London (tube.tfl.gov.uk/content/ticketsoyster/asp)

This chapter is organized as follows:

- Section 3.1 presents an overview of the above programs with respect to their smartcard, reader, and hardware design. It also discusses their business policies and related data elements.
- Section 3.2 identifies the commonalities in the information shared among agencies participating in the listed interoperable programs.
- Section 3.3 discusses current trends and new developments being considered or pursued within the smartcard programs, including
  - Payment for parking, bridges, and highway tolls;
  - Applications for financial institutions and retail; and
  - Expanded security and biometrics features.

3.1 Survey of Interoperable Agencies

Surveys were conducted to gather current data on the following elements of each interoperable system:

- Physical Elements—Physical characteristics of the cards and communication protocols;
- Data Elements—“Essential” and “optional” data elements required for financial settlement between participating operators; and
- Security Elements—Security architectures and the security devices used.

For data gathering purposes, the security element information was included in the data elements portion of the survey.

The physical-layer results of the survey are presented in Table 7. The data-layer results of the survey are presented in Table 8. The optional data results of the survey are presented in Table 9.

3.1.1 SmarTrip

In May 1999, the Washington Metropolitan Area Transit Authority (WMATA) introduced the SmarTrip card based on Cubic Transportation Systems’ (CTS) proprietary Go CARD technology. WMATA has issued approximately well over 1 million SmarTrip cards for Metrorail, Metrobus, and station parking fare payment. Cardholders add value to their SmarTrip cards at Metrorail vendors or at Metrobus fareboxes. Metrorail vendors also vend magnetic tickets for non-SmarTrip cardholding customers; these tickets can only be used in the rail system.

An implementation that will expand the SmarTrip functionality to surrounding transit providers is under way. Additional smartcard-enabled equipment, including vending devices, fareboxes, and readers will be deployed in support of the regional program. An integral feature of the SmarTrip program will be the implementation of the Regional Customer Service Center (RCSC). The RCSC will provide services to all SmarTrip participants and operators in the DC, Maryland, and Northern Virginia regions. The RCSC will consist of the customer service center,

Smartcard Interoperability Issues for the Transit Industry

Table 7. Survey results: physical layer.

Physical-Layer Features	Washington, DC, SmarTrip	San Francisco, TransLink[10]	Chicago, Chicago Card	Seattle, RFC[10]	Minneapolis, Go-To Card	Central Florida, ORANGES	Ventura County, Go Ventura	LA County, TAP[10]	San Diego, Compass[10]	London, Oyster	Hong Kong, Octopus	Singapore, EZ-Link
1. Is the card ISO 14443 compliant?	No[1]	✓	No	✓	✓	✓[5]	✓	No[6]	✓	✓	No	No[7]
2. Is the reader ISO 14443 compliant?	No[2]	✓	No	✓	✓	✓	✓	✓	✓	✓	No	✓[8]
3. Does the reader modulate between Types A and B?	No[2]	✓	No	✓	✓	✓	No	✓	✓	✓	No	No
4. Is the command set ISO 7816 compliant?	No	✓[9]	No	No	No[4]	✓	N/A	No	No	No	No	No
If yes, which APDUs do you use and how many?	DNA	N/A	DNA	DNA	DNA	N/A	N/A	DNA	DNA	DNA	DNA	DNA
If no, what do you use?	PRO	DNA	PRO	PRO	PRO	DNA	N/A	PRO	PRO	PRO	Felica	PRO
5. List the type of card security used.	DES	DES[3]	PRO	N/A	PRO	PRO	3DES	PRO	PRO	PRO	3DES	3DES

Notes:
[1]Currently, Cubic's Go CARD is used, which is not compliant, but they are taking steps toward using a compliant card.
[2]The current reader for rail (Cubic's Go CARD reader) is not compliant, but they are procuring a system of buses that will use Cubic's Tri-Reader, which is compliant and would modulate between Types A and B.
[3]The card security is a variation of 3DES.
[4]The cards are not compliant, but the system could be compliant if compliant cards are used.
[5]The card type is Mifare Type A, which is compliant for Parts 1 and 2, but not fully compliant for Part 4.
[6]The most commonly used card (Cubic's Go CARD) is not compliant.
[7]Compliant with Part 1 only.
[8]Compliant with Part 2, Type B only.
[9]As allowed by ISO 7816, a subset of APDU commands has been implemented.
[10]Full project rollout has not ocurred. Listed information is "as planned."

Key
✓ = Yes
DNA = Does Not Apply
PRO = Proprietary
N/A = Not Available
DES = Data Encryption Standard
3DES = Triple DES

Table 8. Survey results: data layer.

Data-Layer Features	Washington, DC, SmarTrip	San Francisco, TransLink	Chicago, Chicago Card	Seattle, RFC	Minneapolis, Go-To Card	Central Florida, ORANGES	Ventura County, Go Ventura	LA County, TAP	San Diego, Compass	London, Oyster	Hong Kong, Octopus	Singapore, EZ-Link
1. What types of cardholder data are exchanged?												
-Card ID #	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
-Card Issuer ID #	✓	✓	No	✓	✓	✓	✓	✓	✓	✓	✓	✓
-Patron Profile Code (Age/Disability)	✓	✓	No	✓	✓	✓	✓	✓	✓	✓	✓	
-Patron Language	No	N/A	No	No	No	No	No	No	No	No	N/A	No
2. Do you have product data?												
-Fare Product ID #	✓	✓	✓	✓	✓[3]	✓	✓	✓[3]	✓[3]	✓[3]	N/A	✓
-Fare Product Validity Period	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3. Do you collect journey data?												
-Agency ID #	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	✓
-Date/time of specific transaction	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
-Entry/exit location of patron	✓	✓	✓	✓[7]	No	✓	✓	✓	✓	✓	✓	✓
4. Do you process and send configuration/mgt. data?												
-Autoload	✓	✓	No	✓	✓	✓	No	✓	✓	✓	✓	✓
-Hotlist	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
-Others?	No	✓[1, 4]	✓[2]	✓[1, 4]	No	No	✓[5]	No	No	No	No	✓[4]
5a. What types of security algorithms do you use?	3DES	DES	DES	3DES	3DES	3DES	N/A	3DES	3DES	3DES	DES	3DES
5b. How many key sets?	One	N/A	N/A	One	One	Two [6]	N/A	One	One	One	N/A	One

Notes:

[1]The ability to block products

[2]Hot list goes to aging list if the card is not used in 2 months

[3]This number is based on a set of data elements that when complete forms a unique number

[4]Device hotlist

[5]Remote loads, configuration data to buses, future data (such as fare change)

[6]One key set for the smartcard and second key set for the transponder.

[7]Entry or Exit (not both) captured depending on agency implementation

Key
✓= Yes
PRO = Proprietary
N/A = Not Available
DES = Data Encryption Standard
3DES = Triple DES

Table 9. Survey results: optional data.

Optional Data Results	Washington, DC, SmarTrip	San Francisco, TransLink	Chicago, Chicago Card	Seattle, RFC	Minneapolis, Go-To Card	Central Florida, ORANGES	Ventura County, Go Ventura	LA County, TAP	San Diego, Compass	London, Oyster	Hong Kong, Octopus	Singapore, EZ-Link
1. Are the following data types exchanged?												
-Pretax/employer-based transit benefits	✓	✓	✓	No	✓ [3]	No	No	UC	UC	No	N/A	No
-Pretax/employer-based parking benefits	Yes	No	No	No	✓ [3]	No	No	UC	N/A	No	✓	No
-Bridge/highway tolls	No	No	No	No	✓ [3]	✓	No	No	No	No	No	No
-Loyalty programs	Yes	✓	✓	✓	✓ [3]	✓ [4]	No	UC	No	No	N/A	No
-Multiple purses	UC	✓	No	No	✓ [3]	✓	No	✓	No	No	✓	No
-Universities	No	No	✓	✓	✓ [3]	No	No	UC	No	No	✓	No
-Retail	No	No	No	No	✓ [3]	No	No	No	No	No	✓	Future
2. What other data are exchanged that might be unique?	Nil	✓[1]	✓[2]	✓[8]	Nil	✓[5]	✓[6]	UC	Nil	Nil	✓[7]	Nil

Notes:

[1]Transaction/purse sequence numbers serve to identify gaps in data

[2]The back-end system does not carry any value so the server will charge the patron's account, and when the threshold goes below 10 dollars, an email is sent to the patron. Also, there is a bonus program that provides 1 dollar back for every 10 dollars spent on the card.

[3]For this system, all these data types could be exchanged; however, to date they have not been used

[4]Members of the field operation test are provided incentives to participate in the form of discounts

[5]A smartcard transponder can be used to pay for parking or bus fare

[6]Automatic passenger counting

[7]Access to recreational facilities; access to gated communities

[8]Non-fare counting data (e.g., wheel lift and bike rack use)

Key

✓ = Yes

N/A = Not Available

UC = Under Consideration

POS devices and network, walk-in centers, and WMATA's data network concentrator. ERG Group received the contract award in July 2003 to install and implement the RCSC. CTS also received a contract in July 2003 to supply POS devices and the data network concentrator and to make upgrades to existing systems to support the regional program. CTS and ERG are working with WMATA to integrate their respective systems.

Upon full implementation, the SmarTrip program will include the following regional bus and rail participants:

- WMATA Metrorail-heavy rail;
- Maryland Transit Administration (MTA)-light rail;
- Virginia Railway Express (VRE)-commuter rail;
- MARC-commuter rail;
- Baltimore Metro—rail;
- Annapolis Transit—bus;
- Arlington Regional Transit (ART)—bus;
- MTA Bus;
- WMATA Metro Bus;
- Corridor Transit Corporation—bus;
- Fairfax City CUE—bus;
- Alexandria DASH—bus;
- Fairfax Connector—bus;
- Frederick Transit—bus;
- Harford County Transportation Services—bus;
- Howard County Transit—bus;
- Loudoun County Transit—bus;
- Potomac and Rappahannock Transportation Commission (PRTC)/OmniRide—bus;
- Montgomery County Ride On—bus; and
- Prince George County-TheBus.

3.1.1.1 Fare Policies

The following fare policies and customer features define the SmarTrip program:

- Card Fee—$5 card purchase fee;
- Fare Products—Bus and rail fares, parking;
- Fare Categories—Full fare, senior/disabled, peak, off-peak, distance; and
- Other Features—Balance protection/fare replacement, negative balance.

3.1.1.2 Transit Benefit Program

As of September 2000, SmarTrip cardholders could receive direct deposited transit benefits on their SmarTrip cards using the SmartBenefits program. In the Washington region, employers may participate with Metrochek, a fare card voucher program provided as an employee benefit by more than 2,500 public and private employers. In the past, employers were burdened with having to distribute paper Metrochek fare cards and vouchers. The SmartBenefits program allows employers to access a secure website where the benefit is transferred electronically to the employee's SmarTrip card. SmarTrip cardholders then claim their transit benefits from specific WMATA rail ticket vending machines (TVMs) located in each station.

3.1.1.3 Loyalty Program

With WMATA's planned Fair Fares loyalty program, cardholders will pay the lowest possible fare based on their card usage. This allows a cardholder to receive the benefit of an unlimited ride pass without having to actually purchase the pass. A counter on the card will log the rides, and if the cardholder takes the required number of rides in a day, the card is subsequently treated as an unlimited-use day pass. This feature is similar for weekly, bimonthly, and monthly passes.

3.1.2 TransLink

The Metropolitan Transportation Commission (MTC) and San Francisco Bay Area transit agencies are implementing TransLink, a regional fare payment system for public transit in the Bay Area. TransLink cardholders can use a single smartcard for bus, train, light rail line, and ferry services provided by multiple operators throughout the Bay Area.

In May 1999, MTC awarded a DBOM contract to Motorola/ERG. In addition to the TransLink cards, ERG will supply the following devices:

- Add-value machines (AVMs);
- Handheld card readers (HCRs);
- Smartcard interface devices (CIDs) for vehicles and platforms;
- Wireless data transmission system (for zone-based fares and data transfer);
- Ticket office terminals (TOTs);
- Retail POS devices; and
- Central system networking and related equipment.

ERG is providing a full range of cardholder customer services and financial clearing and settlement among agency participants. Customer services include a live operator help desk, 24-hour automated customer service, registration for autoload and balance protection, and card distribution services.

The TransLink card is an ISO 14443 Type B smartcard containing both contact and contactless interfaces. TransLink cardholders place their card within range of a CID on board a vehicle or at a station platform. The CID automatically deducts the correct fare, calculating transfers and appropriate senior, disabled, and youth discounts. The contact interface is used at AVMs to load e-cash value or transit fare products to the card. A planned on-street parking meter payment implementation will also use the contact interface.

A 6-month pilot program (TransLink Phase I) was successfully conducted in 2002 with six transit operators implementing TransLink on their systems. The Phase I pilot served as a demonstration and test period and included the following transit agencies:

- Alameda County Transit (AC Transit)-bus;
- San Francisco Bay Area Rapid Transit District (BART)-heavy rail;
- Caltrain-commuter rail;
- Golden Gate Transit (GGT)-ferry and bus;
- San Francisco Municipal Railway (Muni)-light rail; and
- Santa Clara Valley Transportation Authority (VTA)-bus and light rail.

Phase I also included the integration of BART's legacy faregates with TransLink CIDs. Although the formal evaluation period is complete, the pilot system continues to operate in the interim between Phase I and Phase II.

The Phase II rollout will expand TransLink service throughout the original six operators' systems and also expand the capabilities to other transit operators in the region. Included in the expanded Phase II BART service is the integration of TransLink functionality with BART's recently installed CTS faregates. To achieve this level of integration, ERG is providing CTS with an API. The API provides the TransLink business rules to the CTS faregate reader software that will be used when a TransLink card is presented to the reader. A similar integration of BART, VTA, and Caltrain TVMs is also planned.

Transit agency board decisions culminating in September 2003 have affirmed Phase II, or full regional deployment of TransLink. GGT and AC Transit will be the first agencies to offer full operational availability to their patrons in mid 2006, followed by BART and Muni in late 2006. TransLink will become available on the remaining 16 operators in 2007 and 2008.

3.1.2.1 Fare Policies

The following fare policies and customer features define the TransLink Program:

- Card Fee—Phase I Demonstration-free. Phase II—$5 card deposit proposed;
- Fare Products—Multiple transit products, including e-cash, passes, and transit ride products (electronic ticket-books), inter-operator transfers;
- Fare Categories—Adult, youth, and senior/disabled; and
- Other Features—Balance protection, autoload, and negative balance.

3.1.2.2 Transit Benefits Program

Employees of participating employers can elect to have their transit benefits loaded directly onto their TransLink card via autoload.

3.1.2.3 Loyalty Program

No loyalty programs are planned.

3.1.3 Chicago Card

As part of an effort to make fare payment easier, more reliable, and flexible, the Chicago Transit Authority (CTA) in August 2000 conducted a 6-month smartcard-based fare payment pilot program. CTA's pilot, designed to test the feasibility of smartcard technology and to gauge customer acceptance, involved the distribution of 3,500 contactless smartcards used at designated sites and rail stations. CTA's existing fare collection system, purchased from CTS in 1997, was already configured for smartcards. In addition, CTA integrated the farebox, manufactured by GFI Genfare, with the bus farecard machine (BFM). The CTS BFM processes both magnetic tickets and smartcards.

In September 2001, following a successful pilot, CTA awarded a contract to CTS to increase the card base to 300,000 over a 3-year period. In late 2002, CTA announced the systemwide launch of the Chicago Card, a stored-value smartcard that can be used as fare payment on CTA bus and rail vehicles and Pace buses. The devices used for their system include

- Turnstile faregates,
- Transit card vending machines, and
- Fareboxes.

Customers may add value to their Chicago Card only at TVMs at CTA rail stations and some offsite locations such as grocery stores and currency exchanges. Registration and balance protection of the Chicago Card is available to customers.

In January 2004, CTA launched Chicago Card Plus, an account-based smartcard program that supports stored-value and 30-day passes. An added feature and requirement of the Chicago Card Plus is the automatic reloading capability that allows customers to charge their credit card for a user-determined amount each time the account balance falls below the $10 threshold. Chicago Card Plus customers can also direct their transit benefits to their card accounts. Chicago Card Plus customers cannot add value to cards at TVMs. Orders for Chicago Card and Chicago Card Plus are accepted on line, by phone, by mail, or in person at CTA headquarters.

Both the Chicago Card and Chicago Card Plus provide pass-back privileges, which allow up to seven customers to board the same bus or enter the same rail station using one card. A full fare or transfer, as appropriate, is deducted from the Chicago Card or Chicago Card Plus account each time the card is presented to the reader. Customers with a 30-day pass also enjoy pass-back privileges and can pay for additional riders using a single Chicago Card Plus card under certain conditions. The first rider travels under the 30-day pass while pay-per-ride charges apply to the additional riders.

The Chicago Card and Chicago Card Plus are based on the proprietary contactless GO-CARD format developed by CTS.

3.1.3.1 Fare Policies

The following fare policies and customer features define the Chicago Card and Chicago Card Plus program:

- Card Fee—$5 purchase and replacement fee;
- Fare Products—Chicago Card-stored-value only; Chicago Card Plus-account-based pay-per-ride, 30-day pass;
- Fare Categories—Full fare only (reduced farecard for seniors is planned); and
- Other Features—Fare replacement/balance protection, automatic account replenishment (Chicago Card Plus only), negative balance (Chicago Card only), Internet loads and card management (Chicago Card Plus only).

3.1.3.2 Transit Benefits Program

Participants of the Regional Transportation Authority (RTA)/CTA Transit Benefit Program can have their pretax benefit automatically applied to their Chicago Card Plus account. The employer establishes an online account linked to their employee accounts and submits the pretax payroll deduction for posting directly to the account.

3.1.3.3 Loyalty Program

Both Chicago Card and Chicago Card Plus users receive a 10-percent bonus each time their accounts are reloaded with $10 or more.

3.1.4 Central Puget Sound Regional Fare Coordination (RFC) Project

Seven transportation agencies supporting approximately 130 million annual boardings are collaborating to plan and implement a smartcard-based regional fare payment system that enables customers to use one farecard on multiple systems throughout the four-county Central Puget Sound area. The Central Puget Sound RFC Project will consolidate hundreds of existing fare media onto one smartcard to streamline the management of fare transactions and facilitate cross-jurisdictional and multi-modal trip-making in the Puget Sound region. The smartcard system will replace all current fare media. In the future, fares will be paid only via smartcard or physical cash. ERG was awarded a contract in April 2003 to design, implement, and provide operational support service for the regional smartcard-based fare collection system. Participating agencies include

- King County Metro Transit-bus;
- Community Transit-bus;
- Kitsap Transit-bus and passenger ferry;
- Pierce Transit-bus;
- Everett Transit-bus;
- Washington State Ferries-ferry; and
- Sound Transit-commuter rail, express bus, and light rail (under construction).

The RFC Project, which plans to use both reusable and disposable Mifare ISO 14443 Type A contactless smartcards, is scheduled for revenue beta testing in 2006 and full revenue operation in 2007 and will include the following devices:

- TVMs;
- Customer service terminal (CST);
- Fare transaction processor (FTP) on-board, handheld portable, and standalone;
- Central data collection system; and
- Driver display unit (DDU).

Customers will be able to load value to their RFC card at TVMs, customer service offices, and retail outlets, or by mail, phone, or autoload, and via the Internet. In addition to transit fare payment, the RFC Project is considering opportunities to use the card for parking payment and transit employee identification and building access.

3.1.4.1 Fare Policies

The following fare policies and customer features define the RFC program:

- Card Fee—Planned: no fee during conversion period, card fee (e.g., $3 to $4) after the introductory period concludes;
- Fare Products—E-cash, fixed-period passes, and transit ride products (electronic ticketbooks), intra/inter-operator transfers;
- Fare Categories—Planned: Adult, youth, senior/disabled, and operator employee; and
- Other Features—Planned: Balance protection/fare replacement, autoload, and Internet sales.

3.1.4.2 Transit Benefit Program

A transit benefit program is planned that will allow cardholders to load pre-tax and employer-sponsored transit benefits to their RFC cards.

3.1.4.3 Loyalty Benefits Program

A “frequent rider” program to reward riders with free rides is being considered.

3.1.5 Go-To Card

Metro Transit, which serves the Minneapolis/St. Paul area, is developing the Go-To Card, a smartcard-based fare payment system. The goal of the Go-To Card project is to modernize an aging fare collection system and to speed passenger boarding. In January 2002, Metro Transit awarded a contract to CTS to implement the Go-To Card system in the seven-county Minneapolis/St. Paul metropolitan region. The card will be accepted on the Twin Cities bus and the Hiawatha light-rail line. During December 2003 and the first half of 2004, Metro Transit performed hardware and software testing. Full public rollout has been scheduled for early 2006.

The equipment procured includes rail and bus validators, TVMs, and a central system. The ticket machines for this system are unique in that they are programmed with four languages—English, Spanish, Hmong, and Somali. TVMs vend magnetic-stripe tickets and add value to smartcards. Cardholders can also load value to their Go-To Card at ticket stores, participating retail locations, and via an interactive voice response (IVR) system. Internet loads are also planned.

The Go-To Card system uses a MiFare ISO 14443 Type A smartcard that will be integrated into the following equipment:

- TVMs,
- Platform and onboard card validators,
- Handheld read/write devices,
- Retail POS terminals, and
- Central system.

38 Smartcard Interoperability Issues for the Transit Industry

3.1.5.1 Fare Policies

The following fare policies and customer features define the Go-To Card program:

- Card Fee—$5 initiation fee (waived in first 90 days if card is registered);
- Fare Products—e-cash, 31-day pass, 10-ride book (schools only);
- Fare Categories—Adult, reduced (youth and senior), and mobility; and
- Other Features—Balance protection/fare replacement, reverse autoload if attempts to collect autoload fail.

3.1.5.2 Transit Benefits Program

Metro Transit plans to integrate the Metropass employer-sponsored transit benefit program.

3.1.5.3 Loyalty Benefits Program

Metro Transit has no loyalty benefit programs available.

3.1.6 Orlando Regional Alliance for Next Generation Electronic Payment System (ORANGES)

ORANGES is the first project in the nation that involves toll payment, transit fare payment, and parking payment via a single smartcard, and processing all transactions through a single source. The program is also unique in that it combines the capability for both stored-value payment from the card and account-based payment such as those used in traditional electronic toll collection applications. In the toll application, participants have a choice of using a transponder in which the inserted card enables drive-through automatic toll payment, using a “touch-and-go” process to pay with their cards directly at devices in non-express lanes.

The ORANGES project began in April 2001; it had been selected through a competitive grant process administered by the FTA. A 1-year field operational test (FOT) with 1,000 volunteers started in August 2003 and concluded in July 2004. An evaluation report was completed in 2004.

The participating agencies include

- Orlando-Orange County Expressway Authority (OOCEA),
- Central Florida Regional Transportation Authority (LYNX), and
- City of Orlando Parking Bureau.

These agencies are using equipment and systems supplied by Ascom Transport Systems, Efkon, Jafa Technologies, and McGann Software Systems. Transend International (formally Touch Technologies, Inc.) acted as systems integrator providing and operating the clearinghouse system. Cards are supplied by Gemplus.

During the testing phase, the smartcard could only be used at select locations, including

- SR 408 East-West Expressway-Holland East toll plaza;
- LYNX Bus-Lines 13 and 15; and
- City of Orlando Parking Bureau-three garages (Central Boulevard, Library, and Market Street).

Each agency issued their own cards from a common stock; however, other agencies’ cards were accepted by all through the use of the common e-cash purse. Interoperability between agencies was achieved by sourcing all the technology from the single vendor team.

3.1.6.1 Fare Policies

The following fare policies and customer features define the ORANGES program:

- Card Fee—FOT-free. Phase II-$5 card deposit proposed;
- Fare Products—e-cash for tolls and parking, 7-day and 30-day transit passes;

- Fare Categories—Adult, student, and senior/disabled; and
- Other Features—Balance protection, auto replenishment/auto renewal, toll account number for account-based payment.

3.1.6.2 Transit Benefits Program

None are available.

3.1.6.3 Loyalty Programs

Discounts were provided as incentives for volunteers to participate. These discounts included a 15-percent discount for the LYNX transit customers, a 50-percent discount off hourly and daily parking fees for customers using specific garage parking, and a free EPASS transponder for the Expressway Authority smartcard transponder users.

3.1.7 Go Ventura

The Ventura County Transportation Commission (VCTC) awarded a contract to ERG Group in May 2000 for its regional smartcard program Go Ventura. Installations began in July 2001 with full project rollout achieved in January 2002. The Go Ventura regional smartcard system has been in service since January 2002 and is accepted on all six of the County's bus operators:

- South Coast Area Transit (SCAT)-bus;
- Simi Valley Transit-bus;
- Thousand Oaks Transit-bus;
- Camarillo Area Transit (CAT)-bus;
- Moorpark Transit-bus; and
- VISTA (Intercity Service).

The Go Ventura program uses ISO 14443 Type B contact and contactless smartcards, where the contact mode is used to load value to cards at the sales office terminals and the contactless mode is used to deduct fares boarding the buses. Cardholders can load value to their card on board buses (except Simi Valley Transit and SCAT), via the Internet, at sales outlets, by phone, or by mailing a check to the customer service center.

The Go Ventura system also allows Cal State University Channel Islands (CSUCI) to brand and provide smartcards usable for unlimited trips throughout the County bus system. Along with smartcard usage statistics, the system incorporates automatic passenger counting and provides sophisticated statistical analysis of system use. Go Ventura cards are issued to social services clients from various agencies within Ventura County. The system is scheduled to be upgraded next year following 5 full years of successful service.

3.1.7.1 Fare Policies

The following fare policies and customer features define the Go Ventura program:

- Card Fee—No charge. $5 for card replacement;
- Fare Products—e-cash, monthly passes;
- Fare Categories—Full fare, student, and senior/disabled; and
- Other Features—Balance protection/fare replacement.

3.1.7.2 Transit Benefits Program

None are available.

3.1.7.3 Loyalty Programs

Cardholders receive a 10-percent discount for using their e-cash to board the system.

3.1.8 Transit Access Pass (TAP)

The Los Angeles County Metropolitan Transportation Authority (Metro) along with nine other municipal operators is introducing the TAP program. TAP is a smartcard-based regional fare payment system for multi-modal, public transit in the Los Angeles area. The TAP program will use two different smartcards. The proprietary contactless Go CARD supplied by CTS will be used for general public fare sales, while an ISO 14443 Type A MiFare card integrated with an HID access module will be used as the transit employee card. The HID portion of the card provides access to Metro building doors, stairwells, and elevators, while the Mifare portion interfaces with fare collection equipment to provide validation at fareboxes on buses or at validators at rail stations.

In March 2002, Metro awarded the TAP contract to CTS with responsibility for supplying:

- TVMs;
- Standalone validators (SAVs) for platforms and stations;
- Handheld validators (HHVs) for inspection;
- POS devices;
- Fareboxes; and
- A central data collection system (CDCS)

As a subcontractor to CTS, GFI will provide bus fareboxes with integrated smartcard readers as well as revenue equipment. There will also be more than 800 third-party supplier locations throughout Los Angeles County equipped with POS terminals that will allow customers to purchase and add value to their cards.

The program is in the system-testing stage, with the central computer installed and supporting more than 200 fareboxes on buses at one of Metro's operating divisions. TAP will be gradually introduced across Metro's fleet of more than 2,500 buses and four rail lines following the successful pilot test at the first division. TAP will also be installed on the Metro Orange Line, a dedicated right-of-way bus rapid transit line under construction in the San Fernando Valley. Municipal operators will follow with TAP equipment installation in 2005. Although several other municipal operators are finalizing their plans to participate, these are among the confirmed TAP participants:

- Metro-bus, light rail, heavy rail;
- Foothill Transit-bus;
- Montebello Municipal Bus Lines;
- Torrance Transit-bus;
- Santa Clarita Transit-bus;
- Antelope Valley Transit-bus;
- Culver City Bus;
- Norwalk Transit-bus;
- Long Beach Transit-bus; and
- Los Angeles Department of Transportation (LADOT)-bus.

Metrolink, the commuter rail system connecting Los Angeles County with five neighboring counties, is also undergoing fare collection system upgrades to prepare for interfaces to TAP.

3.1.8.1 Fare Policies

The following fare policies and customer features define the TAP program:

- Card Fee—Fee amount undecided;
- Fare Products—Planned-Multiple transit products including e-cash, passes, and transit ride products (electronic ticket-books);

- Fare Categories—Adult, student, senior/disabled/Medicare, and operator employee; and
- Other Features—Balance protection, autoload, secure access.

3.1.8.2 Transit Benefits Program

Employer and county programs are under consideration. The employer program has been scheduled to become operational in the first quarter of 2005.

3.1.8.3 Loyalty Program

A fair fares or best fare loyalty program is under consideration.

3.1.9 Compass

The San Diego Association of Governments (SANDAG), teamed with eight San Diego-area transit operators, is leading the implementation of a smartcard-based fare payment system for the San Diego Region (SDR). The Compass card will be used as fare payment by bus, light rail, and commuter rail customers on the following systems:

- North County Transit District (NCTD);
- San Diego Transit Corporation (SDTC);
- San Diego Trolley, Inc. (SDTI);
- Chula Vista Transit (CVT);
- County Transit Systems;
- Direct Access to Regional Transit (DART);
- National City Transit (NCT); and
- MTS Contract Services South Bay.

The vision for the project is the result of regional goals that the transit agencies set out to achieve beginning in year 2000, which were to

- Simplify the use of transit,
- Remove “barriers” to using transit,
- Deliver improved passenger amenities,
- Unify the procurement of AFC equipment, and
- Automate San Diego’s existing manual revenue collection processes.

After considering various technologies and approaches, SDR agreed that a regional fare payment system based on smartcard technology would allow them to achieve their new directives, including to

- Simplify transit fare payment for customers,
- Improve and enhance agency revenue data collection, and
- Provide regional clearing and settlement.

In September 2002, the Metropolitan Transportation Development Board (MTDB) awarded two separate contracts for the AFC system. (Compass management responsibility has since been transferred to SANDAG.) One contract is with GFI Genfare for bus fareboxes and revenue equipment. The second is with Cubic Transportation Systems (CTS) for the smartcard and back office systems, including

- TVMs;
- Handheld card readers (HCRs);
- Onboard and platform CIDs;
- Ticket office terminals (TOTs);

- Card issuance machines (CIMs); and
- The central system (NextFare).

As part of their parallel contracts, CTS and GFI integrated their onboard systems and interfaced the GFI farebox to a new CTS driver-control unit (DCU). The CTS smartcard reader resides in the GFI Odyssey farebox or stands beside existing fareboxes that will remain on some contracted suburban operators. The entire system is designed to communicate over the NCTD/MTS-provided network, which includes fiber-optic lines to each station and between operator sites.

The program is being implemented in two phases. Phase I is 95-percent complete as of November 2004 and includes the deployment of bus DCUs, fareboxes, and a limited function central system. Phase II includes the deployment of the remaining system components (i.e., DCUs and smartcard reader kits for contracted bus agencies, commuter rail and trolley equipment, HCRs, full customer services, and smartcards). Phase II is in the final design review phase. The Compass system will be operated entirely by following full system deployment.

The Compass system will use an ISO 14443 Type A Mifare contactless smartcard capable of supporting expanded functionality beyond transit applications. As such, SDR is considering commercial opportunities for the Compass card such as on-street metered parking, use in coffee houses, and several opportunities at the new downtown Petco baseball park. For now, however, SDR is focused on achieving the goal of a transit-application deployment in 2005.

3.1.9.1 Fare Policies

The following fare policies and customer features define the Compass program:

- Card Fee—Fee amount undecided ($5 being considered);
- Fare Products—Monthly passes initially, then multiple transit products, including e-cash, passes, ticket books, and day passes;
- Fare Categories—Adult, youth, senior/disabled, and operator employee; and
- Other Features—Balance protection/fare replacement and autoload. Internet enrollment and fare product purchases (future capability).

3.1.9.2 Transit Benefits Programs

None are available.

3.1.9.3 Loyalty Programs

None are available.

3.1.10 Octopus

In 1994, Creative Star Ltd. (now called Octopus Cards Ltd. or OCL) was established to oversee the development and implementation of a smartcard system for transit fare payment. OCL is a joint venture among six major transport operators in the Hong Kong region. After a 3-year test and trial period, OCL launched the Octopus smartcard program. The Octopus card, a stored-value smartcard based on Sony's Felica card technology, is accepted on virtually all of Hong Kong's transportation systems, including rail, ferries, buses, coach (shuttle) services, taxis, and tramways. The Octopus card may also be used to pay for parking at garages and car parks and on-street metered parking. The Octopus card is the first and largest multipurpose, contactless smartcard-based payment system in the world with nearly 11 million cards in circulation used in over 8.3 million daily transactions totaling HK$56.7 million. More than 95-percent of the population aged 16 to 65 uses an Octopus card.

In April 2000, the Hong Monetary Authority authorized OCL as a deposit-taking company. The authorization allows the Octopus card to be used for non-transit payment. Payment at 7-Eleven convenience stores, the first non-transport-related application, was introduced in October 2000. The Octopus card can now be used for payment at fast food restaurants, supermarkets, self-service kiosks and vending machines, conferences and exhibitions, recreational facilities, schools, theaters, and telephones, and for access control.

The equipment used in the Octopus system includes

- Multipurpose octopus processor (MOP);
- MiniMOP;
- Parking access and payment system;
- The Octopus central computer;
- Faregates;
- POS devices; and
- A central clearing center.

3.1.10.1 Fare Policies

The following fare policies and customer features define the Octopus program:

- Card Fee—HK$50 deposit, HK$7 card-refund handling fee, HK$20 bank switching fee;
- Fare Products—Multiple transit products including e-cash, passes and transit ride products (electronic ticket-books), inter-operator transfers;
- Fare Categories—Adult, children, senior, and student; and
- Other Features—Balance protection, autoload, and negative balance. Alternatives such as Nokia phone covers, watches, and key chains are available in place of the standard card media.

3.1.10.2 Transit Benefits Programs

None are available.

3.1.10.3 Loyalty Programs

In 2002, Octopus launched loyalty programs in connection with retail applications. Discounts with retail participants and transit operators vary widely.

3.1.11 EZ-Link

Following on the heels of Hong Kong's Octopus card, EZ-Link is Singapore's smart-card-based transit and non-transit payment system. The EZ-Link card is a contactless smartcard that supports stored value and ticket products, including period passes. Visitor EZ-Link cards are available and provide access to tourist attractions in addition to supporting public transit payment. The EZ-Link card is accepted on all mass rapid transit (MRT), light rail transit (LRT), and buses, as well as at non-transit participants, such as movie theaters, schools, libraries, and bowling centers. There are more than 5 million cards in circulation today with more than 4 million daily financial transactions.

EZ-Link Pte. Ltd. (EZL), a subsidiary of the Land Transport Authority [Land and Transport Authority of Singapore (LTA)], was formed in January 2002 and is responsible for selling, distributing, and managing EZ-Link cards as well as clearing and settling the card transactions generated in transit and non-transit applications.

EZL appointed Transit Link Pte. Ltd. as the agent to manage the day-to-day use of EZ-Link cards on public transportation. Transit Link is a consortium composed of SBS Transit Ltd., Singapore MRT Ltd. (SMRT), and Trans-Island Bus Services, Ltd. (Tibs). Transit Link sells and distributes EZ-Link cards, as well as provides customer service to cardholders.

The EZ-Link card is based on Sony's Felica card technology. Devices used in the systems include onboard validators, faregates, ticket offices, AVMs, and general ticketing machine (GTMs). The GTM provides written and video instructions available in English, Malay, Mandarin, and Tamil, but no audio instructions.

3.1.11.1 Fare Policies

The following fare policies and customer features define the EZ-Link Program:

- Card Fee—$5 (S) card deposit;
- Fare Products—e-cash, passes, park-and-ride tickets;
- Fare Categories—Adult, children, senior, and student; and
- Other Features—Autoload/auto top-up.

3.1.11.2 Transit Benefits Programs

None are available.

3.1.11.3 Loyalty Programs

EZ-Link offers both transit and non-transit loyalty programs, including incentives on auto top-up transactions and fast food purchases. Up to 15 loyalty programs can be supported on each card, while the EZ-Link back office can accommodate up to 225 separate loyalty programs.

3.1.12 Oyster

The Prestige Project was conceived to improve revenue collection and information management about journey patterns across the London Transport, now Transport for London (TfL) network. On the London Underground, the amount of ticketless travel, estimated to be approximately £45 million annually, needed to be reduced. The solution was to install faregates throughout the system and use smartcard technology to expedite the throughput of passengers. On the bus network, there was need for common ticketing and accounting across a deregulated market of different bus operators and for ensuring a fair apportionment of revenue on "net" contracts. Smartcard technology also offered the opportunity to adopt the "cash-less bus" resulting in faster boarding and reduced potential for fraud.

In 1998, a 17-year contract was awarded to TranSys—a consortium of companies composed of Electronic Data Systems, Ltd (EDS), Cubic Transportation Systems (CTS), International Computers Limited (ICL), and WS Atkins—to design, develop, deliver, and maintain a transit fare payment smartcard system for the London region. Oyster was introduced in a trial program that began November 2002 with 80,000 ISO Type A MiFare smartcards used by the London Underground and bus employees. In June 2003, a phased rollout began when monthly and annual season pass holders could obtain an Oyster card. In January 2004, Oyster was expanded to include stored value (Pre-Pay) on the London Underground and Docklands Light Railway (DLR). As of October 2004, more than 2.1 million Oyster cards have been issued for fare payment on the following transit providers:

- London Underground (The Tube)-255 stations;
- London Bus-8,000 buses;
- Tramlink light rail;
- DLR; and
- National Rail-28 stations.

The five transit modes combined serve more than 8.5 million passengers a day. The Oyster-enabled equipment installed throughout the London region includes

- Faregates,
- Onboard validators,

- HCRs,
- Ticket machines,
- Ticket office machines, and
- Back office and central system equipment.

Oyster's plans include expanding beyond transit by adding an open e-purse to the card and moving outside London by integrating with other railways in the United Kingdom.

3.1.12.1 Fare Policies

The following fare policies and customer features define the Oyster program:

- Card Fee—£3 for pre-pay, 7-day, and bus passes, all others free;
- Fare Products—e-cash, passes;
- Fare Categories—Adult, senior/disabled freedom pass, employee; and
- Other Features—Balance protection, station-specified recharge, and Internet loads.

In addition to TVMs and ticket offices, Oyster cardholders can add value to their card via telephone and Internet and at participating retail outlets.

3.1.12.2 Transit Benefits Programs

A voucher program provides an Oyster card to employees of employers who participate in the program. The employer covers the cost of the Oyster card. The employer is then reimbursed through interest-free employee payroll deductions.

3.1.12.3 Loyalty Programs

A loyalty program was launched that deducts 2003 adult single fares for trips taken in 2004 on the Tube and DLR. Plans include "Pre Pay Capping," which will establish a maximum amount a traveler pays on any one day.

3.2 Findings

The single commonality for all regional fare payment systems implemented is the proprietary nature of the design. Most contactless smartcards issued are proprietary (i.e., either Sony Felica card in Asia or CTS Go CARD in The United States and Canada). All of the interfaces to the back office system are considered proprietary. The security architecture is unique to each supplier. The lack of open specifications is the primary barrier to interoperability and the use of a transit payment card for non-transit applications across the world. Suppliers continue to refuse to publish the interface documentation necessary to allow broad participation in an interoperable smartcard system. The only way interoperability has been achieved is by forcing the use of a single smartcard fare payment system supplier across a region.

3.2.1 Commonalities and Differences

Critical information necessary to achieve transit fare payment interoperability may be grouped into the following elements:

- Physical Elements-Mechanical and electro-physical characteristics of the contactless smartcard;
- Data Elements-Minimum information stored on the card that allows fare calculations to be conducted;
- Application Elements-Transit-specific data elements that facilitate transit operator-specific data needs for special services or reporting;

- Security Elements-Methodology used to secure the data on the card from unauthorized access and manipulation; and
- Optional Data Elements-Information required to increase the utility of the card for other uses than fare payment.

The findings of the survey are discussed within the context of the interoperability elements. In order to achieve interoperability, all five elements have to be defined and complied with by all participants in a smartcard system. This rule applies to both transit and non-transit participants.

3.2.1.1 Physical Elements

To achieve physical interoperability, a common set of physical characteristics for the smartcard needs to be defined, particularly if physical manipulation is required, such as insertion into a slot or automatic dispensing. The most common physical specification is conformance to ISO 14443 Part 1 contactless interface standard. Though not fully ISO 14443 Type A or Type B compliant, virtually all projects profiled use ISO 14443 Part 1 conforming cards.

3.2.1.2 Data Elements

Tables 7, 8, and 9 make clear that, with few exceptions, the agencies profiled exchange the following data:

- Card ID number,
- Card issuer identification,
- Patron profile code,
- Fare product ID number,
- Fare product validity period,
- Agency identification,
- Date and time of specific transaction,
- Entry and/or exit location of patron,
- Hotlist number, and
- Transaction value.

The exceptions result from the level of functionality required by the fare payment system, whether the card includes a stored-value purse or just passes. These data are the minimum required to process inter- and intra-agency fare payment transactions. The data elements accommodate existing fare structures and transfer agreements through the use of a common fare media—the contactless smartcard.

3.2.1.3 Application Elements

A standard "application elements" definition for transit does not exist today in a published specification available to the public. Although interoperability exists within smartcard implementations, the application is proprietary and specific to the region's implementation. As an example, although the CTA Chicago Card application and the WMATA SmarTrip application use the Go CARD platform, the SmarTrip application is not supported within the CTA system, nor is the Chicago Card application supported within the WMATA system. Similarly, although the San Francisco TransLink application and the Go Ventura application use the MV5000 series platform, the two applications are not interchangeable. Therefore, despite interoperability within specific regional implementations, there is no non-proprietary, open standard application definition that provides interoperability across a single supplier.

However, applications such as SmarTrip, TransLink, and Chicago Card have integrated their employee benefits program with their card technology and therefore exchange of such data between operators is possible. The data exchange of these benefits is at the discretion of the transit properties. Other agencies, such as in San Diego and Los Angeles, are considering this capability for future implementation. This integration is not fully automated and usually requires manual input by the employer or smartcard system operator.

3.2.1.4 Security Elements

The security architecture varies across each implementation. The research found that most projects use either a variation of the Data Encryption Standard (DES) or a variation of the Triple Data Encryption Standard (3DES) as a cryptographic algorithm within their card and device tier. To achieve interoperability, at a minimum, the cryptographic security algorithms used for communication between the card and reader will need to be defined. In addition to the algorithms, the use of symmetric cryptography will require the exchange of key data to achieve interoperability.

In general, each region has unique keys for accessing the data on its cards. To achieve higher order interoperability, a mechanism needs to be established that allows cards with keys from different regions to be accessed in a single system. Key management is one of the most significant barriers to higher order interoperability because of the unique way each supplier handles security keys. All systems may use the same key. However, if the single key is compromised, then all keys need to be exchanged, which is time consuming and costly.

3.2.1.5 Optional Data Elements

The survey indicates that the use of optional data elements for increasing the utility of the card beyond transit fare payment is not typically available. The most common uses beyond transit fare payment include

- Identification for access control (e.g., to agency facilities or university campus services);
- Transit and non-transit loyalty programs;
- Bridge and highway toll payment;
- Non-transit retail payment; and
- Parking payment.

The approach to implementing optional card features varies widely and will be affected by the systems and equipment design of the participants. Most specifications require the system supplier to be able to add these capabilities in the future. Because of the card design, at a minimum, the cards will need to be exchanged if the capability was not demonstrated during the design review. Moreover, if the transaction data need to be transferred to or through the transit central clearinghouse, costly software modifications will likely be required.

3.2.2 Current Trends and New Developments

A trend for interoperable smartcard programs is using the stored-value purse for non-transit payments, such as payment for parking and bridges and highway tolls. Since the inception of transit smartcard programs, it has been envisioned that the transit card will be used with financial institutions, for retail payment, and/or for secure access control.

European and Asian transit smartcard systems are more mature than U.S. and Canadian systems. Since U.S. and Canadian programs are only now beginning to be rolled out, the use of the card is limited to transit. However, the vision of most U.S. and Canadian agencies is to expand the utility of the card with other applications.

The following two sections summarize the current trends and new developments in Asia and The United States and Canada. Given that Oyster only recently rolled out and where proliferation beyond transport payment has not started, the discussion on the United States and Canada contained in Section 3.4 would apply.

3.3 Asian Contactless Smartcard Trends

3.3.1 Octopus

Several programs already have integrated non-transit applications into their functionality. The Octopus card is accepted extensively throughout Hong Kong at more than 200 different non-transit locations. Currently, the Octopus card can be used at the following types of non-transit locations:

- Parking lots and garages;
- Secure access facilities;
- Retail stores (e.g, fast food chains, convenience stores, supermarkets, personal care stores, bakeries);
- Self services (e.g., vending machines, photo booths, pay phones, photocopiers);
- Movie theaters;
- Recreational facilities (e.g., swimming pools, race tracks, amusement parks); and
- Schools (e.g., food service).

Additionally, the Octopus card can be used to control access to residential properties, offices, schools, and parking lots.

3.3.2 EZ-Link

Similar to the Octopus card, the EZ-Link card in Singapore is accepted for payment by non-transit merchants such as hotels, fast food restaurants (e.g., McDonald's), cafes, cinemas, school food services, libraries, and a bowling alley. The EZ-Link card can even be used to enable Muslims to contribute their annual alms, or zakat, through their EZ-Link cards during Ramadan.

3.3.3 Finding

These programs use the capabilities of the transit application and the settlement functionality of the central system. Non-transit participants and merchants are treated the same as a transit agency, from the perspective of transaction processing.

3.4 U.S. and Canadian Contactless Smartcard Trends

3.4.1 TransLink

As the full rollout of TransLink progresses, the City of San Francisco has decided to expand the use of the TransLink card with the Department of Parking and Traffic (DPT) for payment at parking meters. The city recently purchased 25,000 new meters designed to accept smartcards. Development work to enable the meters to accept the TransLink card and include DPT as a participant in clearing and settlement is well under way with a planned demonstration program to begin in mid-2005.

3.4.2 SmarTrip

Customers of Washington's Metrorail may use their SmarTrip card to pay for parking at station parking facilities. WMATA is conducting pilots with financial institutions where the SmarTrip chip is embedded in an ATM card. There is no direct connection between the debit card information and the data stored on the SmarTrip chip.

3.4.3 ORANGES

In addition to fare payment for transit services, participants in Central Florida's ORANGES project may use their smartcard to pay for downtown parking at two garages and for expressway tolls. The smartcard has a stored-value purse and the capabilities to store toll account data and prepaid multi-day bus passes. To facilitate toll payment, select participants were provided with a smartcard-enabled transponder that eliminated the need to stop at the tollbooth.

3.5 Summary

As these programs demonstrate, there is no clear technical or business model for creating interoperability across multiple industries. Each opportunity uses the unique characteristics of each system. The information to be exchanged with the interoperable partners is developed as the project matures. Defining the information for non-transit opportunities is beyond the scope of this study and needs to be developed to address the specific needs of the participants. However, the core information required for interoperability across multiple transit agencies can be effectively used beyond transit to non-transit participants.

Transit smartcard projects are still in the early stages of development, particularly in the United States and Canada. Interoperability is still viewed primarily as a regional issue. Issues associated with interoperability beyond fare payment, though explored, have not been at the forefront when developing smartcard fare payment systems. This situation is attributable to the high cost of developing a system with the capabilities to be used for more than fare payment. Another factor contributing to this situation is the current competitive environment. Suppliers use technology to protect their market position. Even the most prominent programs in Asia have not achieved large-scale market penetration beyond transit fare payment as evident by the small average retail transaction amount of less than US$10.

As a result of the challenges experienced by the global community of transit agencies, significant standards development efforts are under way—including in the United States and Canada, Europe, and Australia.

Table 10 gives the names and contact information for the people interviewed for each of the systems profiled.

Table 10. Interviewees for each system.

Location	Project	Contact Name	Contact Title	Telephone Number
Washington, DC	SmarTrip	Doug Deckert	Project Manager	202-962-2457
San Francisco	TransLink	Scott Rodda Jennifer Cheng	Program Manager Project Manager	510-817-3252 510-817-3251
Chicago	Chicago Card	Chung Chung Tam	Client Representative	312-255-1818 ext. 5709
Seattle	RFCS	Candace Carlson Margaret Walker	Project Manager Supplier	206-684-1562 905-890-2794 ext. 222
Minneapolis	Go-To Card	Mike Tensfeldt Jim Alexander	Supplier Project Manager	858-810-1308 612-349-7467
Central Florida	ORANGES	Doug Jamison Tom Delaney	LYNX Project Manager Project Consultant	407-254-6071 407-647-7275 ext. 4121
Ventura County, CA	Go Ventura	Steve DeGeorge	Project Manager	805-642-1591 ext. 103
Los Angeles County, CA	TAP	Jane Matsumoto	Project Manager	213-922-3045
San Diego	Compass	James Drieisbach-Towle Brian Monk	Project Manager Supplier	619-557-4502 858-614-4481
Hong Kong	Octopus	Joseph Lee	Supplier	416-495-3339
London	Oyster	Richard Thomas Brian Monk	Client Bus. Mgr. Supplier	44 020 7918 6019 858-614-4481
Singapore	EZ-Link	Margaret Walker	Supplier	905-890-2794 ext. 222

CHAPTER 4

Findings of Key Information to be Exchanged Between Agencies

This chapter identifies the key information to be exchanged between public agencies in order to implement an interoperable smartcard-based fare payment system. Using the Interoperability Model introduced in the Introduction, the subsequent research reviews and analyzes relevant technology standards and specifications and outlines the essential data elements required for two or more smartcard payment systems to exchange data to enable financial settlement for rides between different agencies.

The culmination of the policies established between participating agencies are the business rules embedded in the terminals (smartcard read-write devices). As discussed in the Introduction, the business rules allow the proper fare to be deducted from the card and the associated transaction record to be generated and transferred to higher levels in the fare payment system clearinghouse.

This chapter identifies the minimum data elements that will be used to generate the information to be exchanged between the card and card read-writer (terminal), and transferred to the clearinghouse for processing. This chapter consists of the following sections:

- Industry Interoperability Analysis—Identifies available standards and specifications developed to address interoperability;
- Description of Required Data Elements—Identifies and describes the data elements required for interoperability; and
- Gap Analysis—Discusses the differences between the available standards and specifications and the required data elements.

4.1 Industry Interoperability Analysis

A detailed literature review of relevant documents was conducted to identify standards and specifications that address interoperability. These standards and specifications have been developed with the same intention as this research effort. In order to conduct the gap analysis, it is important to define the difference between a standard and a specification:

- Standards are maintained by nationally or internationally recognized governance bodies such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), or the International Organization for Standardization (ISO), or by an individual organization such as the American Public Transportation Association (APTA) or Europay, Mastercard, or Visa (EMV).
- Specifications address industry or very specific user needs that usually augment a standard.

The documents reviewed include specifications and standards developed both in the United States and internationally. Particular focus was given to technology, data, and control standards, and interface specifications from the smartcard and transit industries that attempt to address the issue of interoperability. Table 11 lists documents reviewed contributing to interoperability, describes the organizations promulgating the standards or specifications, and describes the scope. Table 12 lists additional literature, potentially related to interoperability.

4.2 Description of Required Data Elements

This section discusses the data required to complete a fare payment transaction. The information exchange required for an interoperable farecollection system is a limited subset of the informational capabilities of these systems. The results of the survey described in Chapter 2 validate that interoperability can be accomplished by defining the following four critical layers:

- Physical Layer-Includes the form factor of the card itself (particularly relevant for dual interface [contact/contactless] card deployments), electrical and radio frequency characteristics, and basic communications and transmission characteristics for Type A and Type B cards;
- Data Layer-Defines the essential data elements for the card, the reader, and the back-office system;
- Application Layer-Includes the card file structure ("card application") as well as how data on the card are stored and accessed; and
- Security Layer-Includes overall security approach (symmetric or asymmetric) and key management throughout the system.

Figure 9 illustrates the critical layers mapped against the minimal data elements.

This section of the report addresses each layer, focusing on what is required for interoperability.

4.2.1 Physical Layer

At the most basic level, before any information can be exchanged, there must be a physical interface that supports communication. The starting point for this commonality is the ISO, which created standard definitions for communication protocol for smartcards. Smartcards can be contact (i.e., the interface of the card must touch the reader), contactless (i.e., the reader creates a radio field to activate and communicate with the card), or both. ISO 14443 defines the standards for contactless smartcards, and ISO 7816 defines the standards for contact smartcards.

Given that ISO 14443 focuses on standardizing aspects of the communication channel between a contactless card and a reader, the next level of commonality focuses on how an application would interact within the communication channel. The obvious selection for standardizing application interaction would be ISO 7816 Part 4 for application commands. These application commands, normally referred to as APDUs, are an application-based protocol that can be used within the ISO 14443-established communication channel. Although ISO 7816 Part 4 defines the template for each of these APDU commands, the precise implementation of these commands and their specific command options must be defined to ensure interoperability. Agencies implementing disparate options will have difficulty communicating properly. However, supplier interoperability that enables multiple suppliers to supply equipment into the system requires definition at the physical level. Because ISO 14443 and ISO 7816 exist as recognized international standards, they are the logical common denominator for the physical elements.

The key information required to ensure interoperability within the physical element are quite simple from a system perspective. The interoperability of fare media requires the exchange of information in the following areas:

- Fare media communication protocol and
- Application communication protocol

Table 11. Description of primary references.

Organization	*Document Title*	*Description*
Calypso	Specification for Contactless Smart Cards and Card Readers	The Calypso standard is a privately owned European licensable specification that describes the transaction between a contactless card and card reader. The specification offers a standardized approach that is supplier independent and provides the following benefits to transit operators: • Multi-modal (management of different interconnected transit systems) • Interoperable (enables sharing between different transit operators) • Multi-application (supports other card applications beyond transit ticketing) Calypso is also available to all industrial partners (card manufacturers, chip manufacturers, systems integrators, etc.) through a license agreement. This facilitates open development according to the Calypso standards.
CEN	ENV 1545 1545-1–Codification of data elements for public transport 1545-2–ID Card systems 1545-3–Tachograph-related data elements 1545-4–Driving license-related data elements 1545-5–Freight ID-related data elements 1545-6–Vehicle-related data elements CWA FINREAD Parts 1–8 CWA13987: Smart Card Systems: Interoperable Citizen Services: User-Related Information Part 1–Definition of User-Related Information Part 2–Implementation Guidelines Part 3–Guidelines for Creating, Operating, and Maintaining an Interoperable Card Community CEN/ISS Application Interface for Smartcards Used as Secure Signature Creation Devices, Part 1–Basic Requirements	The European Committee for Standardization (CEN) is the European counterpart to the ISO, charged with planning, developing, and adopting European standards. The organization develops and maintains standards for over 16 broad areas of business. A sample of the CEN specifications are listed below: • CEN ENV 1545 addresses public transit ticketing data elements. • CEN Workshop Agreement (CWA) FINREAD is a set of technical specifications for a secure card reader connected to a PC to carry out, essentially but not exclusively, payment and global financial as well as e-commerce transactions on the Internet. • CEN Workshop Agreement (CWA) 13987 addresses user-related information for interoperable citizen services within smart card systems
EMV 2000	Integrated Circuit Specification for Payment Systems, Version 4.0	EMV 2000 is an integrated circuit specification that ensures single terminal and card approval processes are developed at a level that will allow cross payment system interoperability through compliance with the "EMV" specifications (Europay Mastercard Visa Integrated Chip Card Standard).

(continued on next page)

Smartcard Interoperability Issues for the Transit Industry

Table 11. (Continued).

Organization	*Document Title*	*Description*
Global Platform	Global Platform Card Specification, Version 2.1.1	Global Platform is an international smartcard association, responsible for creating and advancing interoperable technical specifications for smartcards, acceptance devices, and systems infrastructure. Formed in 1999, it is made up of a cross-industry member base comprising over 50 organizations.
ISO	ISO 14443 ISO 7816	The International Organization for Standardization (ISO) is a 148-member country body charged with developing worldwide standards. ISO standards include ISO 14443 (parts 1-4), the standard that governs contactless smartcards, and ISO 7816 (parts 1-6), the standard that describes integrated circuit cards with contacts.
ITSO	Interoperable Public Transport Specification	The International Ticketing SmartCard Organization (ITSO), founded in 1998, is a collaboration between various UK passenger transport authorities addressing the lack of suitable standards for interoperable smart card ticketing. ITSO was formed to build and maintain a specification for secure end-to-end interoperable ticketing transactions, utilizing relevant ISO and emerging CEN standards.
MTC	San Francisco Bay Area TransLink Project–Conformed Statement of Work, June 1999	The Metropolitan Transportation Commission (MTC) is the transportation planning, coordinating, and financing agency for the nine-county San Francisco Bay Area. MTC is responsible for administering the Bay Area's TransLink smartcard project. A data message and format specification owned by MTC and participating operators defines data elements in the system.
PANYNJ	Regional Interoperability Standard (RIS)	The Port Authority of New York and New Jersey (PANYNJ) Regional Interoperability Standard (RIS) identifies and defines the required operations and data elements between a contactless smartcard and card interface device.
RKF	RKF Travel Card Travel Card Specification Requirement Specification, Version 2.00 Technical Requirements Specification Implementation Specification Details Type 1, Version 2.00 Implementation Guide RKF Type CL-1	The Resekortisforeningen I Norden (RKF) is an association of transit operators in Denmark, Norway, and Sweden. The purpose of the RKF travel card is to facilitate one travel card within the public transport in the Nordic countries. The RKF Travel Card Technical Requirement Specification identifies requirements for selected IC-card technologies for the RKF travel card.
WMATA	Washington, DC SmarTrip Regional Customer Service Center Contract Book and Draft SmarTrip Interoperability Regional Specification	The Washington Metropolitan Area Transit Authority (WMATA) is developing the SmarTrip Interoperability Regional Specification (SIRS) that defines the interface between agency equipment and the third-party service provider of the SmarTrip Regional Customer Service Center (RCSC).

Table 12. Additional literature reviewed.

Organization	Document Title
American Pubic Transit Association (APTA)	Business Issues Guidelines for Regional Transportation Payment Systems and Clearinghouse (draft) Work Package #4 Functional Interface Description (draft)
Applied Security Technologies	Security Standards for Smartcards Smartcard Lifecycle– Security Guidelines
e-Government Interoperability Framework (e-GIF)	Government Data Standards Catalogue Volume 1–General Principles Volume 2–Data Standards The e-Government Interoperability Framework (e-GIF) mandates the adoption of XML and the development of XML schemas as the basis of the government interoperability and integration strategy. In addition, the Government Data Standards (GDS) catalogue specifies the rationale, approach for using XML schema, and other interchange processes.
	Part 1–Framework Part 2–Technical Policies and Specifications Version 5.1
eEurope Smart Card (eESC)	Open SmartCard Infrastructure for Europe Volume 2–Contactless Technology Volume 9–Referenced Standards e-Europe Smart Cards (eESC) is an initiative developed by the European Commission to further the development of smart cards across Europe and promote the following objectives: Interoperability Multi-application cards Secure transactions User acceptance Accessibility
National Institute of Science and Technology (NIST)	Government SmartCard Interoperability Specification, Version 2.1
Smart Card Alliance	Transit and Retail Payment: Opportunities for Collaboration and Convergence
Transit Cooperative Research Program (TCRP)	Report 10–Fare Policies, Structures, and Technologies
	Report 32–Multipurpose Transit Payment Media
TCRP–Research Results Digest	Developing a Recommended Standard for Automated Fare Collection of Transit
	Multipurpose Fare Media: Developments and Issues
	Coordinated Intermodal Transportation Pricing and Funding Strategies

4.2.1.1 Fare Media Communication Protocol

ISO 14443 was established as the standard from which contactless smartcards establish a communication protocol with contactless smartcard readers. Within ISO 14443, there are four parts:

- Part 1: Physical Characteristics-Defines the physical and electrical specification for smartcards in a standard credit card format.
- Part 2: RF Power and Signal Interface-Defines two types of RF modulation scheme known as Type A and Type B.
- Part 3: Initialization and Anti-collision-Defines the initial communications when the smartcard is brought into the RF field of the smartcard reader. Also defines the anti-collision scheme to allow multiple cards to enter the field simultaneously—

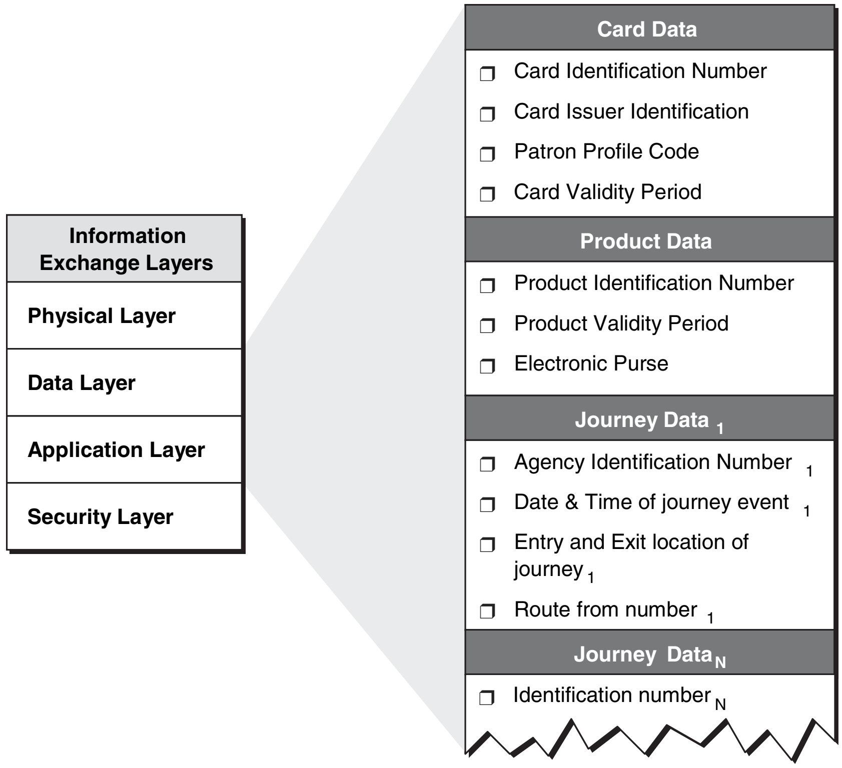

Figure 9. Critical interoperability elements matrix.

determining which card to select for communication. Type A uses bit-wise anti-collision, Type B uses slotted anti-collision.

- Part 4: Transmission Protocol-Defines the communication protocol and framing for data exchange. Because of its transparency, it can encapsulate any application command, which permits a variety of functionality and flexibility.

4.2.1.2 Application Command Protocol

ISO 7816 was established as the standard from which contact readers and smartcards were to enable application interaction. Although ISO 7816 establishes the framework for application commands, the data and parameters contained in each of these ISO commands can be exclusive to an application and are not defined by ISO. One objective of this report is to identify the subset of ISO 7816 commands to use for a transit application and then define the data and parameters that will be contained within these commands for transit interoperability. In the ISO 7816 standard, there are six parts, of which only Part 4 applies to this discussion. In Part 4 of ISO 7816, the following subset of application-related commands is provided:

- SELECT FILE—Selects files, directories, or applications on the smartcard file system for read and update operations.
- READ BINARY—Retrieves data from a transparent (non-record-based) file on the smartcard.
- WRITE BINARY—Writes data to a transparent (non-record-based) file on the smartcard.
- UPDATE BINARY—Modifies existing data within a transparent (non-record-based) file on the smartcard.
- READ RECORD—Retrieves data from a record-based (non-transparent-based) file on the smartcard.
- WRITE RECORD—Writes data to a record-based (non-transparent-based) file on the smartcard.

- UPDATE RECORD—Modifies existing data within a record-based (non-transparent-based) file on the smartcard.
- EXTERNAL AUTHENTICATE—Used with GET CHALLENGE to authenticate the terminal to the smartcard.
- INTERNAL AUTHENTICATE —Used to authenticate the smartcard to the reader device.
- GET CHALLENGE—Used with the EXTERNAL AUTHENTICATE to authenticate the terminal to the smartcard.

Despite the existence of the ISO 7816 standard, some suppliers have implemented smartcard application commands that use the distinct advantages of their own specific platforms and thus offer an advantage to their particular product lines and barriers to entry for other suppliers. This defeats the purpose of interoperability between suppliers. Therefore, it is critical to require and then examine the card application requirements that will lead to the definition of the application commands in a manner that complies with the ISO standard.

4.2.2 Data Layer

The key essential data elements of a regionally interoperable system include information for front-end components (e.g., the smartcard and the smartcard reader) as well as information for back-office systems (e.g., the data collection equipment). Starting with a superset of all data from the four primary reference interoperability specifications (i.e., RIS, ITSO, CEN, and RKF) a conceptual model was created. All data elements were tested against the working definition of interoperability. This information is summarized in the following two questions:

- Does this data element enable multiple transit agencies to offer a common smartcard application for transit-fare payment?
- Would the lack of this data element prevent multiple transit agencies from offering a common smartcard application for transit-fare payment?

If the answer to both of these questions was yes, the data element was considered essential. This information is categorized as follows:

- Cardholder information (information unique to the card itself);
- Fare information (information regarding a particular fare product); and
- Transaction information (information about the particular trip).

During the development phase of this project, additional essential data elements may be identified. Such discoveries are expected in iterative prototype development, and we will update this paper with these elements should it be necessary.

Table 13 depicts the data fields defined in the four primary standard specifications (RIS, ITSO, CEN, and RKF) for each of the three categories (card/holder information, fare information, and transaction information). Each of these standards has many other types of data beyond these three categories; however, only the data for the three categories relevant to data element interoperability have been included. Table 13 does not suggest that ALL of the included data fields in each specification in the three categories are required. In fact, the opposite is true, and the subset of fields that must be standardized for minimal interoperability are identified following this table. Table 14 defines the data elements listed in Table 13 based on the RIS.

Of the data elements listed, most are not required to be exchanged between agencies for interoperability to work. Many elements are exchanged between the agencies for business

Table 13. All data fields available in selected categories.

CARD/HOLDER INFORMATION			
RIS v. 1.0	**ITSO v. 1.2**	**CEN v. 1.0**	**RKF v. 2.0**
Card/Transit Information			
PICCTestUse	NA	NA	NA
OpsMaintenanceUse	NA	NA	NA
CountryID	NA	Country ID	NA
PICCValidityPeriod	ValidUntil (VUT)	NA	CardValidityEndDate
RegionID	NA	NA	NA
IssuerID	ITSOOperatorsIDNumber	ApplicationIssuerID	CardProvider
TransitExpirationDate	ITSOShellExpiryDate	Base data type of EndDate	NA
KeySetIdentifier	KeyVersionCode	MACKeyID	MACKeyIdentifier
ManufactureID	MID or CSN	NA	ManufacturerData
TransitPICCID	IssuerIdentificationNumber	NA	CardSerialNumber
IssuingDeviceID	ISAMID	Base data type of DeviceID Base data type of SerialNumbers	Base type of Device
Holder Information			
ProfileBirthDate	DateOfBirth	BirthDate	Base data type of DateTime
ProfileStartDate	NA	StartDate	Base data type of DateTime
ProfileExpireDate	ExpiryDate	EndDate	Base data type of DateTime
ProfileLanguage	Language	LanguageID	DialoguePreferences Language
UserRegistered	NA	NA	
ProfileCode	CustomerProfile	EntitlementType DiscountLevel PassengerClass	DiscountCounter DiscountLevel DiscountType PassengerType
DepositPaid	ShellDeposit	NA	Deposit
PICCHolderGender	IDFlags	NA	PassengerType
PICCHolderDescription	NA	NA	NA
CardHolderDescription	PersonID	UserData BirthName Forename Surname HolderName Employee CompanyName Birthplace	NA

reasons or to accommodate policies such as allowing the agencies to gather information to better run their businesses. The following are the essential elements that need to be exchanged for interoperability:

- Card/Holder Information is primarily information associated with an individual card and cardholder. This information is required in transaction data to allow the back-office systems to validate, process, and deliver the necessary data for clearing and settlement between agencies. It also allows the reader to validate the transaction and perform the service (allow entrance or exit) to the patron. The essential card/holder data elements are
  - *Card Identification Number*—Uniquely identifies the card within the interoperable system. One purpose of the card ID is to ensure the integrity of a card's total value in the system.
  - *Card Issuer Identification Number*—Uniquely identifies the issuer of the card within the system. The card issuer ID is required in order to perform inter-system funds settlement.

Table 13. (Continued).

FARE INFORMATION			
RIS v. 1.0	**ITSO v. 1.2**	**CEN v. 1.0**	**RKF v. 2.0**
Stored Value Information			
AutoSubscribe	ValueATPAFlags	NA	AutoloadLoad Status
ValueExpires	EndDate	NA	EndDate
RemValueSign	NA	NA	NA
RemValue	Value	Balance	Value
ExpRecurDate	NA	Date	NA
RecurringAutoloadType	NA	NA	NA
AutoThreshold	Threshold	NA	NA
SVThreshloadLoadAmount	TopUpAmount	NA	AutoloadValue
SVRecurringLoadAmount	NA	NA	AutoloadValue
CurrencyCode	ValueCurrencyCode	NA	CurencyUnit
CIDTransactionNumber	TransactionSequenceNumber	NA	Device Transaction Number
CIDID	SAMID	Base data type of DeviceID Base data type of SerialNumbers	Device
Pass/Transfer Information			
AutoloadSubscribed	TYP9Flags	NA	NA
PaymentType	AmountPaidMethodOfPayment	NA	NA
LocationEncodingType	NA	NA	NA
RemTripRidesTransfers	CountUsesAvailable	NA	NA
ExpDate	ExpiryDate	Base data type of EndDate	Base data type of DateTime
ExpTime	NA	EndTime	Base data type of DateTime
RenewedInAdvance	NA	NA	NA
AutoThreshold	NA	ThresholdAmount	NA
ProdID	TransactionType	AuthorizedProduct	ContractSerial Number
LocationEncoding	ValidFrom / ValidTo	NA	Place
CIDTransactionNumber	TransactionSequenceNumber	NA	DeviceTransaction Number
CIDID	SAMID	Base data type of DeviceID Base data type of SerialNumbers	Device

(continued on next page)

- *Patron Profile Code*—Represents the discount allowance, if any, for the individual bearing the card. Without the patron profile code, discounts for special fares such as for those with disabilities or for students could not be supported.

- Fare Information describes the fare product being used. It is required for the fare equipment and the back-office systems to validate and process fare payment transactions. Fare information, at a minimum, consists of the following:
  - *Fare Product Identification Number*—Uniquely identifies the logical fare product used in the transaction to enable appropriate clearing and settlement. Even in a system where only the e-purse is used as the form of payment, the e-purse must be uniquely identified.
  - *Product Validity Period*—Identifies the time and/or date period that the product is valid.
  - *Transaction Value*—Identifies the fare amount if a stored value e-purse is to be used.
- Transaction Information is a concatenation of card, fare, and specific transaction information. It is normally referred to as the transaction data for a specific patron's journey. This is the primary information used by back-office systems to validate and process fare payment transactions for establishing end-of-day net-settlement positions. When the day's transactions are processed and net-settlement positions established, funds will either be sent to or received

Table 13. (Continued).

TRANSACTION INFORMATION			
RIS v. 1.0	**ITSO v. 1.2**	**CEN v. 1.0**	**RKF v. 2.0**
Add Value History Information			
LoadType	ValueAPTAFlags	NA	NA
ValueExpires	EndDate	NA	NA
AgencyID	IssuerID	ProductOwner	NA
Date	DateTimeStamp	Date Time	Base datatype of DateTime
Time	DataTimeStamp	NA	Base datatype of DateTime
RecurringAutoloadType	NA	NA	NA
SVTransaction	Value	NA	NA
SVTransactionNegative	NA	NA	NA
RegionID	NA	NA	NA
LocationID	NA	LocationData	Place
CIDTransactionNumber	TransactionSequenceNumber	ReceiptFlag	TransactionNumber
CIDID	SAMID	Base datatype of DeviceID Base datatype of SerialNumbers	Device
Transaction History Information			
TransactionType	TransactionType	NA	NA
In_Out	NA	NA	NA
ProdID_or_RegionID	TransactionType	ProductID	ContractSerialNumber
AgencyID	SAMID	ServiceOperator	Basetype of CardProvider
LocationID	NA	LocationData	Place
DateStamp	DateTimeStamp	Date	Base datatype of DateTime
TimeStamp	DateTimeStamp	Time	Base datatype of DateTime
TransactionLinked	NA	NA	NA
TransferStartTime	NA	Time	Base datatype of DateTime
TransValue	ActualAmount	FareDeducted	MoneyAmount
TransValueSign	NA	NA	NA
TransferCode	NA	NA	NA
Special	NA	NA	NA

from partner agencies, as determined by these settlement positions. Transaction information, at a minimum, consists of five data elements presented above and three additional data elements described below:

– *Agency Identification Number*—Uniquely identifies the agency that provided the service for this transaction. The agency ID is necessary for the proper settlement of funds.
– *Date and Time* of the specific transaction—Date and time information is required to uniquely identify transactions for reporting and troubleshooting.
– *Entry and/or Exit Location* of the patron—Entry and/or exit information is required for fare calculation in distance-based or zone-based fare structures.

4.2.3 Application Layer

A standard "application data element" definition does not exist today in an open, accessible form in the transit industry. However, from an information exchange perspective, the application layer for a smartcard and reader is primarily the software and/or data structure on a smartcard and reader that allows for the exchange and capture of data that will be used for clearing and settlement. The captured data are ultimately transferred from the reader through the agency's system hierarchy to another system (partner agency or central system) for clearing and settling that transaction.

Table 14. Definition of RIS data elements.

Card/Transit Info	
Field	**Description**
	Indicates the test or revenue PICC
OpsMaintenanceUse	Indicates the revenue or operations/maintenance
CountryID	Numeric value that identifies the country in which this PICC was issued
PICCValidityPeriod	Card validity period in years
RegionID	Numeric value that identifies the metropolitan region of a country in which this PICC was issued and intended for the majority of its use. There are 256 possible regions that can be defined on a PICC within each country
IssuerID	Designates the card and ticketing application of issuing nation, state/region, or agency
TransitExpirationDate	Represents the transit application's expiration date
KeySetIdentifier	Represents a logical pointer to a key set that is contained on a PICC to support the transit application. (Note: The actual physical location of the keys, as well as access to the keys, is protected and managed by the specific PICC's operating system)
ManufactureID	Represents the manufacturer ID code
TransitPICCID	Represents the unique printed serial number assigned by the PICC manufacturer based upon instructions of the ordering regional clearinghouse
IssuingDeviceID	Indicates the PICC issuing/encoding device containing the CID ID
ProfileBirthDate	Represents birth date of the customer to assist with identifying the customer's eligibility for discounts and recording demographics (Format ddmmyy)
ProfileStartDate	Provides the date this profile becomes valid for use (Format ddmmyy)
ProfileExpireDated	Provides the expiration date of this customer profile and associated discount if applicable (Format ddmmyy)
ProfileLanguage	Enables an automatic language of preference to display on smart PICC devices [e.g., PCD (reader), faregate, vending machine, touch-pads at non-transit outlets, etc.]. Different regions can assign other languages, but if a customer travels to a different region and the language code is not supported in the standard, a patron can always select English as a default

(continued on next page)

The need to access the application data elements in an interoperable equipment independent fashion is another objective of this research project. The objective is to develop an implementation of a transit application using a standard API to serve as a proof of concept of interoperability between the smartcard readers and the transit application software. The application layer should use ISO/IEC 7816-4 to address the need for a standard approach. Chapter 7 contains the details of the standard approach.

4.2.4 Security Layer

Security for interoperable fare collection systems should be implemented at multiple layers of the overall system. Security may be as simple as implementing a security mechanism

Table 14. (Continued).

Card Holder Information	
Field	**Description**
ProfileBirthDate	Represents the birth date of the customer to assist with identifying the customer's eligibility for discounts and recording demographics (Format ddmmyy)
ProfileStartDate	Provides the date this profile becomes valid for use (Format ddmmyy)
ProfileExpireDate	Provides the expiration date of this customer profile and associated discount if applicable (Format ddmmyy)
ProfileLanguage	Enables an automatic language of preference to display on smart PICC devices [e.g., PCD (reader), faregate, vending machine, touch-pads at non-transit outlets, etc.]. Different regions can assign other languages, but if a customer travels to a different region and the language code is not supported in the standard, a patron can always select English as a default
UserRegistered	Indicates that the cardholder has registered prior to card issue
ProfileCode	Numeric code that represents a patron's specific discount and/or demographic profile if appropriate and available. Although standard profile codes and demographic codes should be recognized by different participating regions for consistency, the criteria defining the profiles may not be consistent between regions and at times may be region specific. As such, profile codes should be processed according to intra-regional and inter-regional policies, or default to adult full fare
DepositPaid	Indicates that the deposit has been paid
PICCHolderGender	PICC holder gender description
PICCHolderDescription	Provided for future assignment at the national, state, or regional level
CardHolderDescription	Provided for additional PICC holder description such as full name, weight, or other PICC holder required information to gain access to a site, facility, transit system, or building
AutoSubscribe	Represents the autoload subscription indicator for this load
ValueExpires	Indicates that this is a Single Load SV product that expires on the date indicated by ExpRecurDate
RemValueSign	Value designates a positive or negative balance
RemValue	Provides remaining currency value
ExpRecurDate	Provides the date that this product expires or last recurring load date (Format ddmmyy)
RecurringAutoloadType	Used to differentiate SV Recurring Autoload types

between the card and reader or implementing multiple security mechanisms in parallel at each layer in the fare payment system architecture. These mechanisms may include one or a combination of the following:

- Security on each component of the system;
- Security between each component of the system (i.e., card and reader); and
- Security extending throughout the system.

Security protections may be implemented at the component, application, and network perspective. The most common areas of protection are

- Ensuring that the fare products on the smartcard are not changed by an unauthorized entity,
- Authenticating the use of a card and application within the system, and

Table 14. (Continued).

Stored Value Information	
Field	**Description**
AutoloadThreshold	Indicates when the T-Purse will be threshold-loaded and a funds charge transaction will be sent to the customer's bank.
SVThreshholdLoadAmount	Indicates value to add for a threshold autoload
SVRecurringLoadAmount	Indicates value to add for a recurring autoload
CurrencyCode	Provides the currency of the value of this product. The currency code is considered fixed and permanent where indicated and consistent for all regions that recognize and adhere to this transit smart PICC Regional Interoperability Standard. The fare collection system conforming to these specifications will recognize the defined currency and deduct the equivalent of that currency from the T-purse
CIDTransactionNumber	Represents the LSB of the Event Identifier assigned by the issuing machine's CID
CIDID	Represents the issuing machine CIDID, used to identify the encoding equipment
AutoSubscribe	Represents the autoload subscription indicator for this load
ValueExpires	Indicates that this is a Single Load SV product that expires on the date indicated by ExpRecurDate
RemValueSign	Value designates a positive or negative balance
RemValue	Provides remaining currency value
ExpRecurDate	Provides the date that this product expires or last recurring load date (Format ddmmyy)
AutoSubscribe	Represents the autoload subscription indicator for this load
ValueExpires	Indicates that this is a Single Load SV product that expires on the date indicated by ExpRecurDate
RemValueSign	Value designates a positive or negative balance
RemValue	Provides remaining currency value
AutoloadSubscribed	Provides the autoload type
PaymentType	Represents the payment code. Indicates the manner in which revenue is collected or returned
LocationEncodingType	Describes the type of location validity encoding depicted by LocationEncoding Field
RemTripRidesTransfers	Indicates the number of remaining transit trips/rides/ transfers (maximum number of trips = 255)

(continued on next page)

- Ensuring that the transaction data are unaltered when transferring within an agency and between agencies.

The appropriate security mechanisms will depend on several factors. At a minimum, these factors are

- Assessment of the functionalities and capabilities of a specific system element and its components,
- A risk and risk mitigation cost model for the element,
- A risk assessment and threat analysis performed by the region and its agencies of the specific system element and its relevance upon the overall system, and
- The complexity of encryption algorithms and key management structure.

Table 14. (Continued).

Pass/Transfer Info	
Field	**Description**
ExpDate	Indicates the expiry date for the product
ExpTime	Indicates the time this product expires. Time in minutes past midnight
RenewedInAdvance	Indicates that this product has been renewed in advance of its expiry date
AutoThreshold (N/A for Transfers)	Code representing the time in advance that a threshold load will occur
ProdID	Product code specifically owned by the transit agency of use. The code is defined by the transit agency within the region and posted to the PICC when the customer buys the product either at any add-value vending machine, ticket booth, or other device in the future. There are 255 possible product codes for each Agency of use. These codes are not fixed and permanent and can be changed by the owning transit agency within the region via tables/fare rules. The code is captured by the faregate reader and used for accounting, demographic reporting, and other downstream fare collection system processing
LocationEncoding	Represents the valid locations indicator
CIDTransactionNumber	Represents the LSB of Event Identifier assigned by the issuing machine's CID
CIDID	Indicates the issuing machine CIDID used to identify the Encoding equipment
LoadType	Represents the payment type code. Indicates how revenue was collected or returned
ValueExpires	Represents the expiry indicator. Indicates that this is the load of a Single Load SV product
AgencyID	For agency-specific SV purses, this is set to the relevant Agency ID The Agency ID for the Regional T-Purse is set to 0
Date	Indicates the purchase date (Format ddmmyy)
Time	Indicates the purchase time in minutes past midnight
RecurringAutoloadType	Used to differentiate SV Recurring Autoload types
SVTransaction	Indicates the value added or deducted inclusive of any bonus for cash, bank card, directed autoload, or threshold autoload transactions
SVTransactionNegative	0 = Positive, 1 = Negative
RegionID	Provides the value of the regional ID
LocationID	Represents the unique location of the device within the regional system.

Based on the research team's experience, technology and system suppliers make products as secure as the procuring agency specifies them to be. For any IT system, a threat and vulnerability analysis is the first step in determining the security features required to mitigate the security risk.

The objective of this discussion is to define security and provide a framework for establishing a smartcard fare payment system security policy that meets system needs cost effectively. As discussed, a smartcard fare payment is an automated data-collection system, thus an information systems security framework applies. The Information Security Handbook defines security as three components:

- *Confidentiality of information* is ensuring that any information exchanged between two or more parties remains private to the authorized entities.

Table 14. (Continued).

Add Value History Info	
Field	**Description**
CIDTransactionNumber	Represents the LSB of the event identifier assigned by the issuing machine's CID
CIDID	Represents the issuing machine CIDID used to identify the encoding equipment
TransactionType	Denotes the type of transaction
In/Out	Indicates in or out of "paid area" for closed systems
ProdID Or RegionID	Provides the product ID for in-region product use or region ID for out-of-region T-Purse use
AgencyID	Represents the service providing agency/agencies for the associated product
LocationID	Represents the unique location of the device within the regional system
DateStamp	Indicates the date of transaction (Format: ddmmyy)
TimeStamp	Indicates the time of transaction. Time in minutes past midnight when transaction occurred (Format: mmm [0–1339])
TransactionLinked	Provides linkage to previous transaction
TransferStartTime	Indicates the transfer start time for the journey and used to determine transfer validity. Time in minutes past midnight. Set to Time of Use if not applicable
TransValue	Indicates the value of the SV transaction, where applicable
TransValueSign	Value designates a positive or negative transaction value
TransferCode	Provides the transfer service code
Special	Indicates the bits reserved for agency-specific usage

- *Integrity of information* is to guarantee that changes to information due to entering and editing errors, faulty data transmission, and unauthorized modifications are detected and if possible corrected.
- *Availability of information* is to balance availability to those allowed access against information-protection measures.

Figure 10 identifies the most common breaches in security and provides an overview of the associated effects. To determine the level of security required for a transit smartcard fare payment system, the methodology presented in Figure 11 provides a systematic approach to assessing the threats and associated risks.

The methodology consists of the following key activities:

- Analyzing business processes to provide the basis for identifying weak links and vulnerabilities to fraud and exploitation;
- Assessing threats to identify how the smartcard fare payment system may be misused, which depends on card use. The most common forms of misuse are
  - Counterfeiting—Creation of a duplicate card,
  - Misrepresentation—Using someone else's access authorization or card,
  - Alteration—Unauthorized modification of data, and
  - Collusion—Circumventing procedures and technology through illegal arrangements;

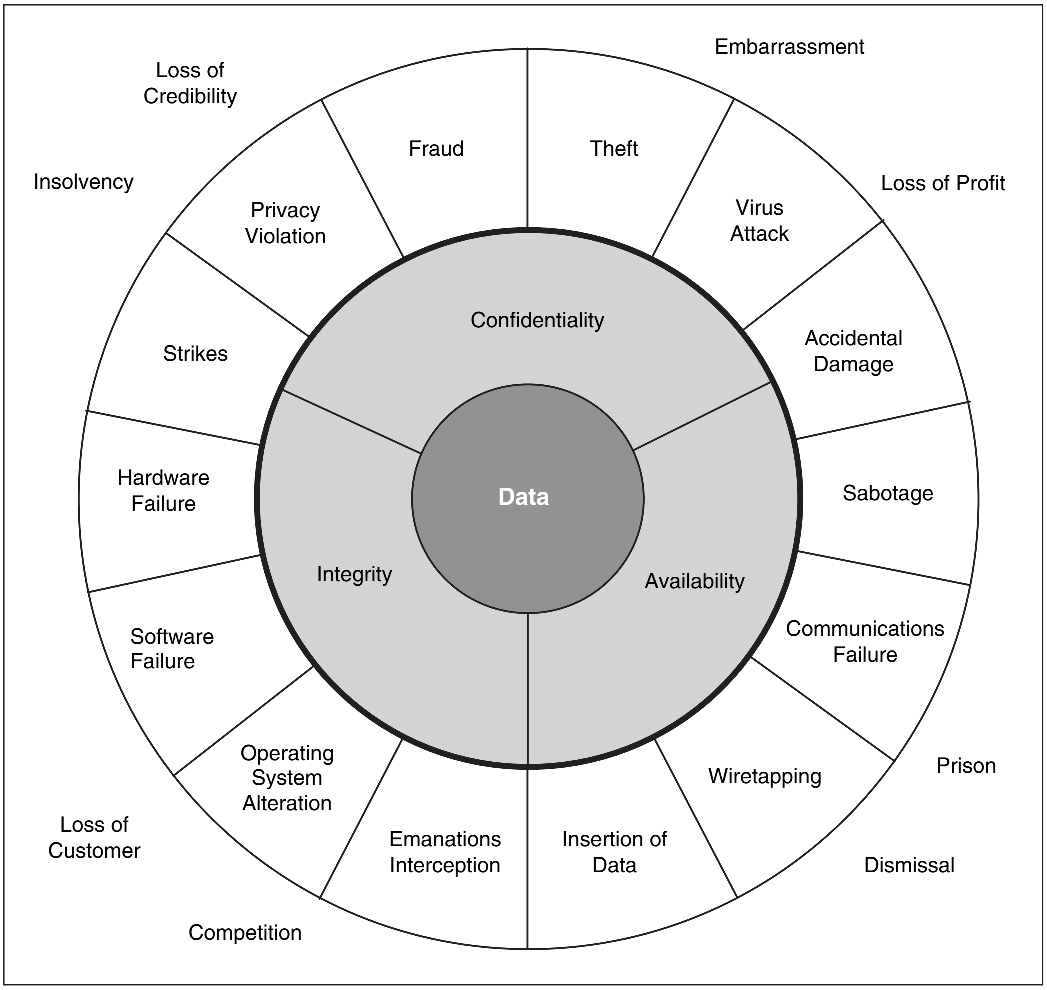

Figure 10. Data security breaches and impacts.

- Assessing technology to identify inherent vulnerabilities that present system risks. According to the orange book, vulnerabilities include
  - Modification,
  - Unavailability,
  - Data corruption, and
  - Data exposure;
- Analyzing risks and developing options to provide the basis for conducting the cost-benefit analysis. The objective of this activity is to develop a set of logically sequenced metrics that identify countermeasures and risk mitigation strategies as follows:
  - Threat vulnerability and countermeasures and
  - Security versus risk and mitigation measures; and
- Conducting cost-benefit analysis to determine the most cost-effective solution for the perceived risks

Security in a smartcard fare payment system is achieved by combining the following three basic elements:

- *Encryption*—This is the transformation of data that is only readable through the use of a secret key.

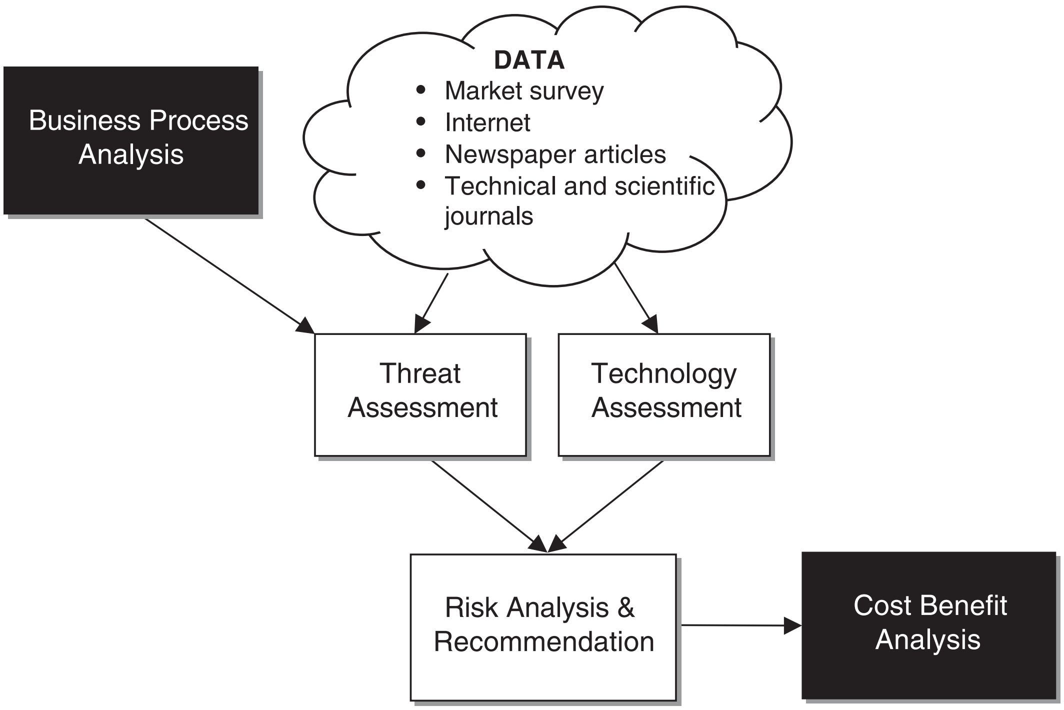

Figure 11. Threat and risk assessment.

- *Authentication*—This is the process of ensuring the message received is the message sent and preventing message modification.
- *Non-repudiation*—This guarantees that the message sender cannot deny having sent the message.

Combining these elements is a function of the business processes, system design, and the exposure associated with the risks. The smartcard fare payment system security is analyzed during the system design-review process.

The research team's findings indicate that a uniform security approach to support interoperability has not yet been developed. As an example, the transit industry has not yet adopted the use of standard Federal Information Processing Standards (FIPS), compliant security algorithms, or keys. The current lack of a standard has not hindered regional systems because a single supplier can provide an end-to-end fare payment system; however, multi-supplier interoperability will require the adoption of a uniform security protocol for smartcard-based fare collection systems. At a minimum, the cryptographic security algorithms used in a regional system between a card and reader will need to be defined and shared to enable the opportunity for interoperability of cards and readers or the readers will need to accommodate multiple algorithms. In addition to the algorithms, the use of symmetric cryptography will require the exchange of key data for interoperability.

4.3 Gap Analysis

Critical gaps exist in current smartcard deployments in the United States and Canada. ISO 14443 and 7816 remove some barriers to interoperability, but even when combined with the minimal essential data set identified through this research, they alone are not enough to achieve full interoperability.

68 Smartcard Interoperability Issues for the Transit Industry

Interoperability is accomplished through proprietary solutions at the application and security layers. Proprietary elements are embedded even into data elements governed by standards. For true supplier-independent interoperability, public domain standards, code, APIs, or some combination thereof will need to be openly available.

Smartcard technology has introduced new features to both the transit patron and the transit agency. Some of these features, such as autoload, are popular with both the patrons and the agencies. Despite the popularity of these features, they are not critical to fare payment interoperability. However, a transit application that does not accommodate data fields for the more popular features is less likely to be embraced by the transit industry. Optional services that are emerging as key factors of smartcard acceptance for patrons and value creation for transit agencies include the following:

- The use of a credit card- or bank account-backed autoload feature is a convenience to both patrons and agencies. However, because it is a convenience feature, autoload elements should be part of the optional, rather than essential data set.
- Balance protection and the ability to change a card status to "ineligible" is a similar popular feature for protecting the incorrect use of monetary value in the smartcard e-purse. As with autoload, the elements associated with this feature should also be optional.
- IRS-defined tax benefits for transportation and commuter parking are gaining momentum and are expected to conform as they are controlled by Treasury regulations. However, because the requirements to support a transit-related tax-benefits program may be complex, the elements associated with this feature should also be optional.
- Audit mechanisms for recording transaction history on the card, as well as for tracing transactions throughout the system, are beneficial but vary across implementations. Two ways in which smartcard-based fare payment implementations CURRENTLY perform transaction auditing are
  - *Audit Registers*-As part of the transaction stream, require that separate and distinct data elements be identified for transaction auditing.
  - *Transaction Transmission*-Where elements of the previous transaction are sent concurrently with the current transaction thereby minimizing the possibility for lost or incomplete transactions.
- A minimum level of system auditability may be achieved without having to define separate and distinct data elements. From a regional perspective, the selection of a standard audit mechanism is key to interoperability within that particular region.

As these features proliferate, it becomes increasingly important to expand the interoperable capabilities as needed to accommodate one or more of these features. Many of these functions have become "de facto standard" requirements for nearly all smartcard fare payment systems, although these functions are not required to achieve interoperability.

CHAPTER 5

Findings of Data Flows Between Agencies

This chapter identifies the data that need to reside on a smartcard and the information that needs to be exchanged between participating agencies. There are two types of information flows in an interoperable smartcard system:

- Institutional Information-Related to the business rules and policies that provide the guidelines for participation in the smartcard system. The institutional information is discussed in detail in Chapter 2.
- Transaction Processing Information-Consists of the following data as depicted in Figure 12:
  - Resides on the card,
  - Flows between the card and reader,
  - Flows between the reader and agency,
  - Flows between the agency and clearinghouse, and
  - Flows between clearinghouses.

To prepare the transaction-processing information flows, the following tasks must be completed:

- Development of a conceptual fare payment system architecture,
- Identification of the data types, and
- Analysis of the data flows.

5.1 Development of Conceptual Fare Payment System Architecture

A smartcard fare payment system architecture consists of the following five functional tiers:

1. Card or Data Input Tier-Data repository for holding the value required to acquire the services desired;
2. Device Tier-Reads the card and conducts the transaction according to the business rules embedded in the software;
3. Station or Local (Garage or Depot) Tier-Manages the assigned devices and consolidates and transfers the transactions to the next tier;
4. Agency Tier-Manages the transfers of device configuration data and the transactions with the central system and may also be used as the agency interface with the central system for system management and reporting; and
5. Central System Tier-Primarily responsible for clearing and settlement; the database also supports the card services operation.

This five-tier model is referenced for most of the standards development efforts in the United States and Canada, particularly the APTA Universal Transit Farecard Standards UTFS). Figure 13 illustrates the five tiers of an interoperable regional smartcard fare payment system.

Figure 12. Figure data flow logic.

Depending on agency size and the supplier's system design, the functionality of the station/local tier and the agency tier can be consolidated into a single server or workstation (computer). A typical smartcard fare payment system is an off-line system; data are stored at each tier and periodically forwarded to the next tier or to the central system. In contrast, credit and debit card transactions are conducted on line; the transaction is authorized before approval.

5.2 Identification of the Data Types

The following two types of data flow among the five tiers:

- Configuration Data-Includes all data a device needs to conduct a secure and appropriate fare payment transaction and
- Usage Data-Primarily consists of the transaction records associated with each device, but includes any recorded alarms or events.

All data transferred between each tier in the system architecture may be categorized as configuration or usage data. Configuration data are generally transferred to the device tier at the start of operation. For buses, start of operation may occur when a driver logs on before pulling out of the depot. On a gated rail system, start of operation may begin before trains begin the morning rush hour.

Usage data are transferred at the end of an operating cycle and at a predetermined cut-off time. Usage data need to be transferred to the central system in sufficient time to allow processing and settlement to be completed according to agency requirements.

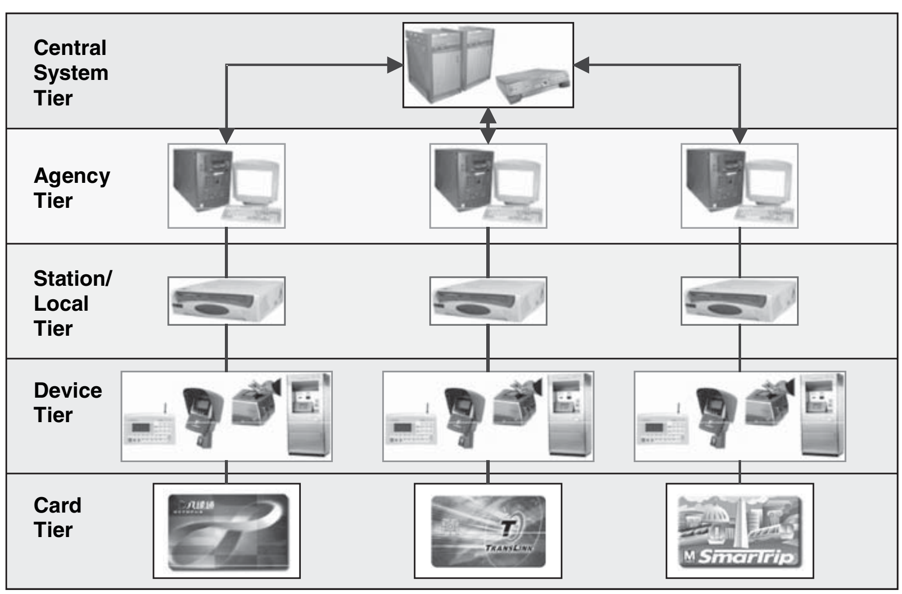

Figure 13. Conceptual smart card system architecture.

Table 15. Configuration and usage data matrix.

Configuration Data	Description/Examples
Business Rules	Fare Policies and Transfer Rules
Software Version Control	Software in Device, Valid Device in System
Hot List	Bad Cards
Action List	Prepaid Autoload
Localization Rules	Rules that Apply to Specific Services Such as Express Bus
Device Configuration	Ensure Bus Device is for Bus
Security Keys	Keys to Unlock Data on Card for Write Function
Usage Data	**Description/Examples**
Fare-Payment Value	Amount Deducted from Card
Fare-Payment Type	Stored Value, Monthly Pass
Add Value	Amount Added to Card
Autoload	Amount Automatically Loaded
Event	Pass-Back Disabled to Conduct Multiple Transactions
Alarm	Bad Card, Hotlisted Card Detected

Table 15 provides an overview and examples for each type of data that flows through a smartcard fare payment system.

5.3 Analysis of Data Flows

Because of the performance requirements of transit operations, the smartcard does not perform any calculations with the exception of dynamic encryption. Dynamic encryption occurs as the data are transferred between the card and reader. The card-based microprocessors are not fast enough to conduct card-based fare calculations at this stage of technology development while passengers are boarding a bus or passing through a faregate. In the transit environment, the smartcard serves as a secure data repository for fare value.

5.3.1 Data on the Smartcard

Table 16 lists the minimum data required on the card to clear and settle transactions for an interoperable smartcard payment system. This also assumes that the physical and security layers are compatible. A detailed discussion of the information exchange layers between the card and reader is provided in Section 4.2. These minimum data requirements are based on analysis conducted as part of the design-review process for projects such as TransLink.

5.3.2 Operation Data Flows

The operation data flows provide the basis for identifying the functionality that the API will need to accommodate. The API functional requirements will be identified in Appendix A. Figure 14a shows the data flows that occur during normal system operation and identifies the tiers relevant for each data element. Figure 14b provides a functional description of each tier and identifies where the data elements reside in the system architecture flow.

Table 16. Minimum data required on card.

Card Data	Product Data	Journey Data
Card Identification Number Card Issuer Identification Patron Profile Code Card Validity Period	Product Identification Number Product Validity Period Electronic Purse	Agency Identification Number Date and Time of Journey Event Entry and Exit Location of Journey Route Number

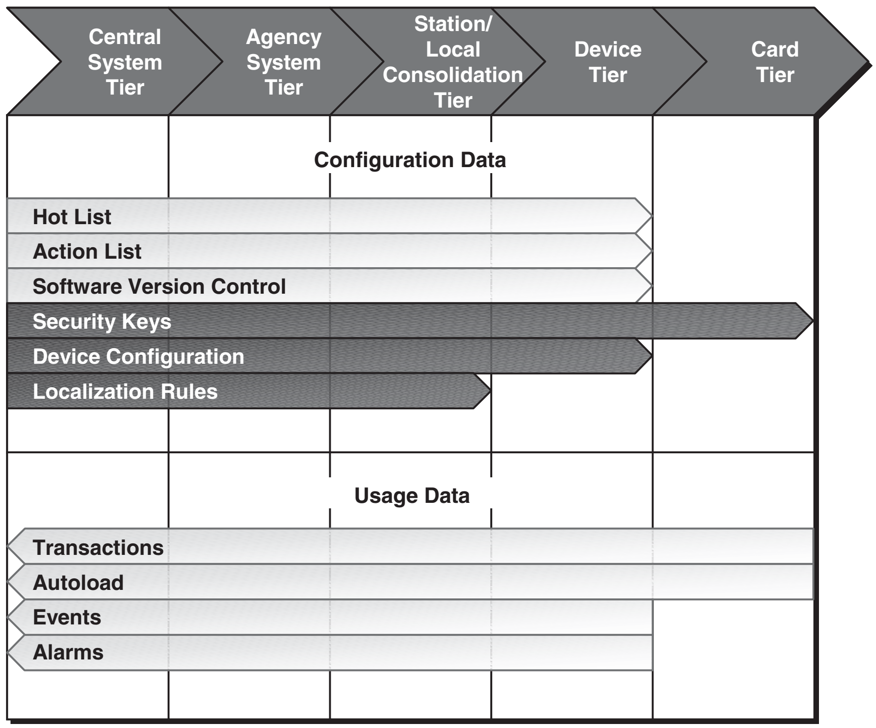

Figure 14a. Data flow analysis.

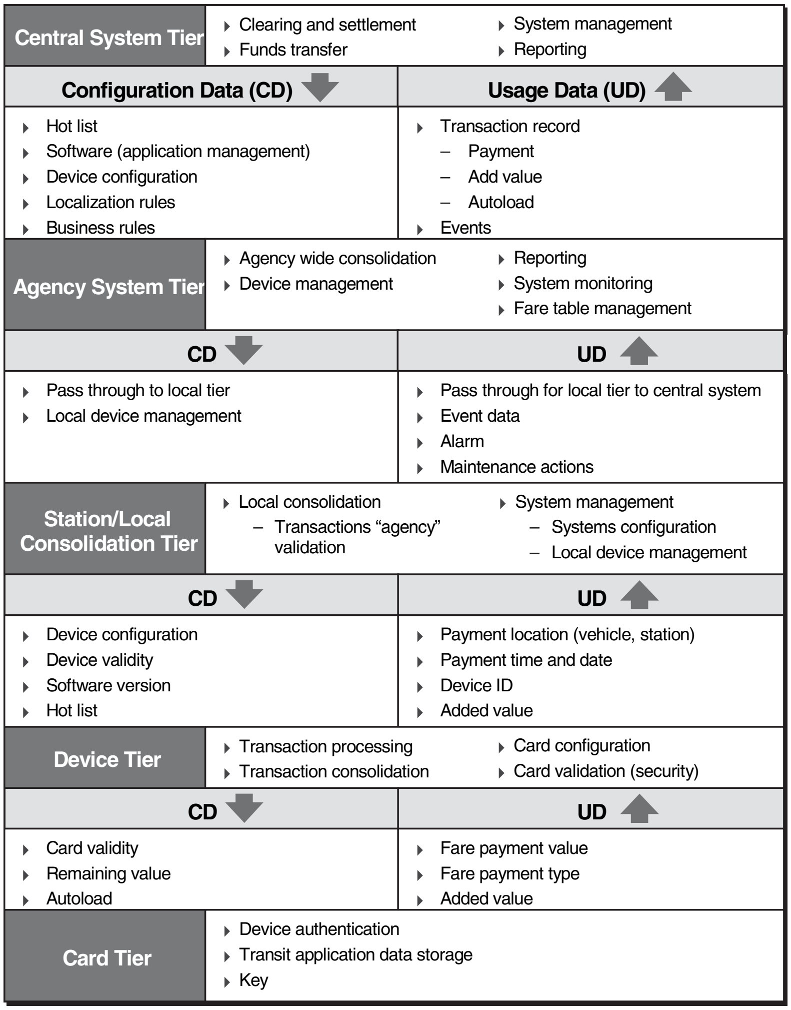

Figure 14b. Functional data flow matrix.

CHAPTER 6

Findings of Data-Management Policies and Issues

This chapter is to examine critical issues and policies related to data management. A smartcard fare payment generates a transaction record every time a card is processed at a read-write device, with the exception of designated terminals that only provide remaining value information to the patron. These transaction records are an asset that has significant value and thus needs to be managed. A data-management policy provides the guidelines for the participants in an interoperable smartcard system for managing this data asset.

At a minimum, a data-management policy should address the following:

- Scope of the data-management policy;
- Definition of the data types,
  - Data location,
  - Ownership and access rights, and
  - Data-protection measures;
- Identification of the stakeholders and their roles and responsibilities; and
- Other requirements-privacy.

A data-management policy is a document updated as stakeholder needs change. Similar to business rules, which may range from a one-page document (e.g., the business rules for TransLink) to a detailed set of requirements (e.g., the business rules for the Seattle RFC), data-management policies' length and level of detail will vary according to stakeholder needs.

Figure 15 illustrates a process for developing and maintaining a data-management policy.

6.1 Scope of the Data-Management Policy

The scope and purpose of the data-management policy identifies to whom it applies, and the limitations of the data involved. In general, the data-management policy for an interoperable smartcard fare payment system will apply to all agencies participating and accepting the smartcard for payment, the contractors supplying systems and services, and any non-transit participants. The data are generally limited to those generated during the fare payment operation.

The scope and purpose of the data-management policy does not necessarily need to be updated unless organizational structural changes occur in the program. Because of the long-term nature of smartcard projects and the effort required by agencies to set up program-management structures, organizational structures are fairly stable once established.

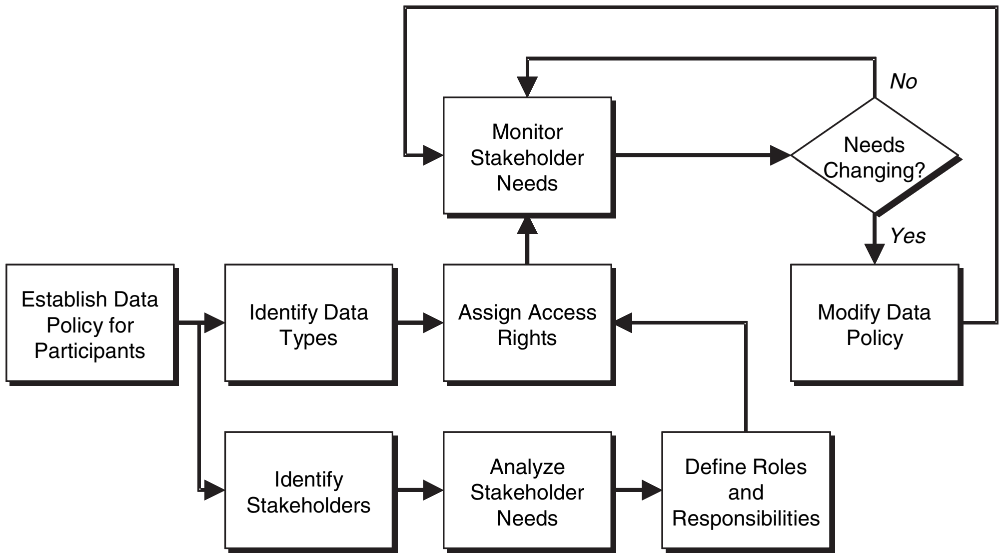

Figure 15. Data-management policy development and maintenance process.

6.2 Definition of the Data Types

Smartcard systems capture detailed transaction and revenue data. Rules must be established for governing who has access to what data, particularly in environments where multiple private operators compete for ridership, because this type of data is generally considered confidential. The data sharing and information access policies also drive the security architecture of the interoperable smartcard system.

Two categories of data are associated with a smartcard fare payment system:

- Transaction Data-Consists of the transactions generated as the smartcard system is used for payment or validation of ride privileges or when value is loaded to cards and
- Operations Data-Consists of all non-transaction data collected while the smartcard system is operating.

As discussed in Chapter 1, transit agencies take ownership of the service levels offered to riders. This situation precipitates an environment of defending control of all data generated for a specific agency's operations.

6.2.1 Data Location

In a multi-agency environment, most operational data associated with each agency will be stored separately, primarily because of the differences in operations. Certain data, such as card holder identity on personalized cards, may be shared by multiple agencies because such data are loaded after card issuance. For example, a card issued by a university for identification purposes may contain a transit application that uses the identity information collected and encoded on the card by the university; this is used for transit-balance protection services. Given the current state of the technology, the fields and format of such data must, however, be established and coded at the time of card manufacture.

Long-term goals of transit agencies in cities such as Washington, San Francisco, Seattle, and London include the future integration of other applications onto cards issued initially for transit service. Although development efforts are under way for card-operating systems (i.e., applications may be dynamically loaded onto cards in a secure manner after they have been issued to customers,) no such system is commercially available at a marketable price. Until systems permitting the dynamic loading of applications are further developed and tested, adding an application to an existing smartcard system will only be possible with the manufacture and issuance of new cards.

6.2.2 Data Ownership and Access Rights

Substantial value is associated with data related to customer characteristics. The data referred to in this discussion include all types generated and collected in operating the fare payment system—both related to customers (transit riders) and the agency. Any contract for a smartcard fare payment system must define the following clearly:

- Rights and Responsibilities—Associated with data generated through processing transactions; with the process of issuing, loading, and reloading transit-only cards; and with whether or not the transit application resides on a card with other applications.
- Data Management—Assurance that any card-holder or card-activity data and financial and operational data from an agency are held securely so that they can be accessed by and released to only those authorized.
- Confidentiality and Privacy Issues-Associated with personal (card holder) data created during fare payment system operations; data that can be linked to an individual card holder at any time are to be considered confidential and should not be released in any manner without card holder consent.

For an agency-owned system, data ownership follows existing rules and regulations as they apply to public agencies. Some data, such as capital and operating expenditures, are subject to the Freedom of Information Act. However, personal data generated during fare payment systems operations should be excluded and only released in the most compelling circumstances to the proper authorities. For example, in the Hong Kong program, most cards issued are anonymous—approximately 10 percent are personalized (registered). If customers are not reasonably confident that privacy is protected they will be unlikely to accept this new form of fare media.

When a smartcard fare payment system is bank-sponsored, consortium-owned data ownership ultimately becomes a cost issue. Data ownership is an intangible benefit for which quantifying a value to a particular organization is difficult. The value of the data depends on how the data will be used by the capturing entity. In the most aggressive scenario, such data may be sold outright to an organization interested in targeting customers riding transit or using a specific transit mode.

Regardless of the ownership model, data ownership has to be defined before entering a contractual relationship. However, data ownership requirements cannot be finalized until a fare payment system concept is complete. The fare payment systems concept defines what data are generated and where in the system. During fare-systems operations, the fare payment system may generate temporary files, which a contractor may argue are proprietary and are an integral function of the application software. A contractor may argue that the agency has no right to the files. Therefore, data ownership becomes a subject of negotiation once fare payment system services and equipment requirements have been finalized.

6.3 Identification of Stakeholders and Their Roles and Responsibilities

As the smartcard program progresses and the system design is established, the location of the data at the different tiers in the architecture becomes evident. The stakeholder will vary depending on the location of the data and how and where it is generated. Each stakeholder that needs to have access to the data in the system will be required to meet responsibilities associated with the data's specific role.

The stakeholders of an interoperable smartcard system have different needs and those needs will affect the level of access to data required. Table 17 identifies the stakeholders, their needs, and the types of data they require.

6.4 Other Requirements—Privacy

Consumer privacy is a growing concern in the smartcard industry. There is no universal law in the United States governing the use of personal information. The U.S. government has encouraged the different industries to self-regulate the use of personal information. Each system should be analyzed on a case-by-case basis for the personal data collected through the normal course of business to determine if an individual's right to privacy is at risk. If a regional farecard program is used beyond transit, this will likely complicate the already complex privacy issues inherent in this type of identity-based system. When marketing value is placed on information by a participant in the smartcard program, such as a financial institution, guidelines and policies should be established regarding the collection and use of such data.

In today's business environment, information about customers has an intrinsic value. In contrast to the European Union, no universal laws in the United States govern personal information. However, there are sectoral laws for industries such as the financial services and medical industries, and for federal, state, and local government. Because laws specifically address financial privacy, financial institutions distinguish privacy as follows:

- Informational Privacy—Defined as the "claims of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."
- Financial Privacy—Defined as the "rights of individuals to control the collection, storing, use, and dissemination of information concerning their personal financial affairs by their financial products and services."

Table 17. Stakeholder data-access matrix.

Stakeholder	Data Needs	Access Requirements
Government	Funding Competing obligations	Consolidated Performance-Related Data
Transit Agency	Operating system Service efficiency Funding	Financial Data Ridership Data Customer-Support Data
Customer	Customer service Ease-of-use Efficient access to information	Transaction Summaries Card Configuration Remaining Value
Other Transportation	Highway and bridge tolls Taxi	Revenue User Profiles
Non-Transportation	Private operators FTA Merchants	Ridership/Sales Revenue

To determine if a smartcard fare payment system may be at risk of invading an individual's right to privacy, the system's data needs to be analyzed to determine the personal identifiable information that is collected in the normal course of business. If it is determined that an individual's right to privacy is at risk, then the Privacy Alliance (a group of more than 80 global corporations and associations who work together toward on-line privacy for individuals) recommends taking the following steps to minimize the exposure to potential litigation:

- Adopt and Implement a Privacy Policy—Any organization engaged in electronic-funds transfer has the responsibility to adopt and implement a policy to protect the privacy of personally identifiable information
- Adopt a Notice and Disclosure Policy—Policy must be available before or at the time the personally identifiable information is requested or collected
- Provide Choice and Obtain Consent—Individuals must have a choice on how the personally identifiable information may be used or have the opportunity to opt out of such use
- Ensure Data Security—Appropriate measures must be taken to ensure that personally identifiable information is reliable and protected from loss, misuse, and alteration
- Ensure Data Quality and Access—Reasonable steps must be taken to ensure that data are accurate, complete, and timely

6.5 Current Trends

The trend for managing smartcard-related data is to adopt the most conservative approach:

- Each agency owns the transaction data generated in its system.
- Any transaction record related to an adjoining agency's service, such as a transfer, is to be made available only to the respective agency involved in the transaction.
- Only ridership reports required by the FTA, through other inter-agency agreements, or through other public sources, may be available to all participants.
- Financial and revenue data are to be reported on an aggregated basis, and each agency controls the distribution of its financial and revenue data.

As interoperable systems become more common and economic benefits begin to materialize as a result of wider sharing of data, transit agencies may begin to cede the tight control common in the industry today.

CHAPTER 7

Findings of Proof of Concept Using Standard API

The importance of contactless smartcards to transit is that these devices serve as secure and convenient vessels for holding the application data elements. The application data elements represent the information required by the AFC system to properly assess fares to passengers and construct transaction records. As discussed in Section 4.2.3, the application layer is the mechanism used to retrieve and update the application data elements on the card. The primary responsibility of the transit software application is to implement an application layer to allow this data exchange to occur. The less time and effort that needs to be spent in conforming the execution of the application layer to the proprietary interface of a smartcard reader, the greater the benefit for transit.

The objective of this chapter is to show the concept of how hardware independence can be forwarded through the use of a proposed standard smartcard reader API. Currently, contactless smartcard readers typically either have their own proprietary API to communicate between the reader and the application software or merely a framing protocol that must be implemented by a software application. This situation limits a prewritten application from adapting transparently to another type of smartcard reader. In the case of a mass-transit application, when an agency has purchased smartcard-based automatic fare collection (AFC) equipment and needs to upgrade or change its smartcard technology, the agency has to rewrite the application software to communicate with new hardware. By standardizing the smartcard reader API for transit applications, any additional investment in modifying application software to upgrade card reader equipment can be reduced or eliminated.

7.1 Use of Standard API in Proof of Concept

To prove this concept, the research team developed a contactless smartcard reader API and an AFC simulator. With experience gained from working with several proprietary readers, the team developed a set of API functions essential to contactless smartcard reader operation. The specification of the API functions is listed in Chapter 6 and will be referred to as the standard API in this report. A subset of the standard API functions was used in the AFC simulator to communicate with the smartcard reader. The team also selected two commercially available readers, the ASK LDB 215 reader and the OTI Saturn 5000 reader, for testing with the AFC simulator. Given that both of these readers use proprietary APIs from their respective manufacturers, the development of conversion layer software was required in order for the readers to work with the AFC simulator. The conversion layer was designed to convert the proprietary reader API functions to the standard API functions, allowing the AFC simulator to function with smartcards that are compatible with the ASK LDB 215 reader and the OTI Saturn 5000 reader. The simulator is designed with a feature that allows the operator to choose a reader

Exhibit 1. AFC simulator code segment.

```
if(Reader == "ask"){
  reader_dll = LoadLibrary("TCRP"); // load converted API of ASK
  readerConf.nDevice = 0x01;
  readerConf.nCommType = 0x02;
  card.nTimeout = 0x19;
  updatePTR(reader_dll, 1);
  if(whichReader == 1)
          reader1 = 1;
}
else if(Reader == "oti"){
  reader_dll = LoadLibrary("OTISaturn5k"); // load converted API of OTI
  readerConf.nDevice = 0x02;
  readerConf.nCommType = 0x01;
  readerConf.cUsbName = "";
  readerConf.nComPort = 0;
  readerConf.nID = 0;
  card.nTimeout = 25;

  updatePTR(reader_dll, 2);
  if(whichReader == 1)
reader1 = 1;
}
```

from a list of readers at run time to demonstrate the interoperability of the AFC simulator by using the standard API.

Exhibit 1 is a code segment and an excerpt from the source code of the AFC simulator. It shows how the simulator loads the code that implements the standard API as a dynamic library when a reader is selected at run time. The simulator loads the API for the chosen reader and configures the reader settings. The module that is loaded is the conversion layer with the standard API functions embedded so that the simulator application can make the same function calls, regardless of which reader has been selected.

Exhibit 2 is a code segment that loads the standard smartcard reader API functions from the conversion layer software. These functions are used throughout the simulator to communicate with the selected reader.

Standardizing the API not only provides the ability of interchangeable readers but also simplifies the structure of application software. Any smartcard application developed through the use of a standard API can communicate through driver software to any reader that complies with the API. Through the use of one set of common communication functions, the business rules of the application software can be performed through one common process for all the readers. Unlike using the standard API, an application developed by using a proprietary API has to implement different ways of communicating to the readers for one set of business rules when the application is required to communicate with multiple types of readers or when the application must now support the upgrade of a reader.

Exhibit 3 shows the differences in the implementation of an application using the standard API and the proprietary API.

Exhibit 2. Standard smartcard reader API.

```
readerOpen = (int (*)(PCD*))GetProcAddress(reader_dll, "OpenReader");
readerClose = (int (*)(PCD*))GetProcAddress(reader_dll, "CloseReader");
readerPoll = (int (*)(PICC*, PCD))GetProcAddress(reader_dll, "Poll");
readerTransmit = (int (*)(Command_Frame, Response_Frame*,BYTE,PCD))
            GetProcAddress(reader_dll, "TransmitToCard");
```

Exhibit 3. Standard API compared to proprietary API.

```
Implementation Process of Using Standard API for Multiple Devices

Load the driver with standard API.
Initiate the communication with the reader.
Configure the application data unit.

If opening reader is successful
{
        Poll for a card

        If a card is found
        {
            Perform a set of business rules.
        }
}
Else if opening reader is failed
{
        Error Message.
}

Unload the driver.
```

```
Implementation Process of Using Proprietary API for Multiple Devices

Load the driver with proprietary API.
Initiate the communication with the reader.

If the reader is type 1
{
  Configure the application data unit for type 1 reader.
  If opening reader is successful
  {
        Poll for a card
        If a card is found
        {
            Perform a set of business rules.
        }
   }
   Else if opening reader is failed
  {
        Error Message.
   }
}
Else if the reader is type 2
{
  Configure the application data unit for type 2 reader.
  If opening reader is successful
  {
        Poll for a card
        If a card is found
        {
            Perform a set of business rules.
        }
   }
  Else if opening reader is failed
  {
        Error Message.
   }
}
Else if  … … …
Unload the driver.
```

One potential development aspect of this project was the proposal of a new APDU specific for transit applications. The impetus for this work was the uncertainty of the suitability of the ISO/IEC 7816-4 Interindustry Command Set for transit applications. The 7816-4 Command Set was developed for contact smartcards and was not widely supported initially by manufacturers of equipment for the contactless interface. When the research topic was being developed this was a legitimate concern, however, since then there has been a dramatic shift in contactless smart cards toward support for the 7816-4 Command Set and away from proprietary commands. This is good news for transit, because the cards are moving toward interoperability. In addition, work has been performed in testing a proof of concept, the Regional Interoperability Specification for Electronic Fare Payment (RIS) that shows the 7816-4 Command Set can work well and within a reasonable timeframe for transit. A custom APDU for transit is no longer necessary or desirable, based on the utility and usability of the ISO/IEC 7816-4 Command Set and the movement among smartcard manufacturers to support that standard command set. Table 18 shows the transaction times of fare tickets with AFC simulator using 7816-4 commands within projected execution time.

Table 18. Transaction timing charts.

Activity	**DESFire with ASK LDB 215**	**DESFire with OTI Saturn 5k**	**UltraLight with ASK LDB 215**	**UltraLight with OTI Saturn 5k**
Select App	47 ms*	16 ms	N/A	N/A
KEY Authentication	94 ms	32 ms	N/A	N/A
Read Data	47 ms	16 ms	47 ms	55 ms
Write Data	47 ms	16 ms	47 ms	55 ms
Write Transaction Record	62 ms	16 ms	N/A	N/A
Commit Record	47 ms	16 ms	N/A	N/A
Process	**T-Purse Transaction Activities**	**DESFire with ASK LDB 215**	**DESFire with OTI Saturn 5k**	
1	Polling	100 ms*	390 ms	
2	Select Application / Product	47 ms	16 ms	
3	Authenticate purse's KEY	94 ms	32 ms	
4	Read Data	47 ms	16 ms	
5	Write Data	47 ms	16 ms	
6	Authenticate record's KEY	94 ms	16 ms	
7	Write Transaction Record	62 ms	16 ms	
8	Commit Record	47 ms	16 ms	
	Total Transaction Time (without polling time)	438 ms	144 ms	
Process	**Trip-Based and Time-Based Transaction Activities**	**DESFire with ASK LDB 215**	**DESFire with OTI Saturn 5k**	
1	Polling	100 ms*	390 ms	
2	Select Application / Product	47 ms	16 ms	
3	Authenticate KEY	94 ms	32 ms	
4	Read Data	47 ms	16 ms	
5	Write Data	47 ms	16 ms	
6	Write Transaction Record	62 ms	16 ms	
7	Commit Record	47 ms	16 ms	
	Total Transaction Time (without polling time)	344 ms	112 ms	
Process	**Trip-Based and Time-Based Transaction Activities**	**UltraLight with ASK LDB 215**	**UltraLight with OTI Saturn 5k**	
1	Polling	100 ms*	390 ms	
2	Read Data	68 ms	16 ms	
3	Write Data	52 ms	16 ms	
4	Write Transaction Record	52 ms	16 ms	
	Total Transaction Time (without polling time)	172 ms	48 ms	

*** ms = milliseconds**

7.2 Development of AFC Simulator

The simulator is designed to perform the AFC functions such as processing the fare tickets based on the type of tickets, the issuing agencies, validation periods, reading and updating purse balances, and issuing the fare tickets. Three types of fare tickets (i.e., trip-based, time-based, and purse) can be processed with the simulator. The data structure design of each type of ticket is based on the minimum data requirement of transit fare ticket and is a set of common data derived from an analysis of the four primary standard specifications: Regional Interoperability Standard for Electronic Transit Fare Payments (RIS), ITSO, CEN, and RKF. Table 19 shows the data fields of the card.

The data structure has been implemented on both a Philips Mifare DESFire smartcard and Philips Mifare UltraLight smartcard. Because of the differing capabilities of the operating systems of each card, the fare ticket's data structure is implemented differently on each type of card. The DESFire Card Operating System (COS) supports a file structure, and the data structure of the fare ticket on this card is implemented as a file system with a security key on each file. Accessing and updating the card's information requires authentication of the security key. Because of the secure file system feature, the electronic purse fare product is implemented on this card. Trip-based pass and time-based pass products have also been implemented on the DESFire card for use as reusable fare tickets. Figure 16 shows the file structure of fare tickets on Mifare DESFire card.

The Philips Mifare UltraLight COS supports a memory block architecture to store the data. The fare ticket's data structure is implemented as a block, and can be configured to be irreversible when the card is issued from the AFC simulator. Since the fare ticket information on this card

Table 19. Data fields of fare tickets.

Card Holder Information	Fare Ticket Information	Transaction Information
Unique Card Number	Ticket Type	Date and Time
Name	Balances	Type of Transaction
Birth Date	Validity Period	Transaction Amount
Profile Code	Issued Agency	Original Balance
Card Validity Period	Electronic Purse	

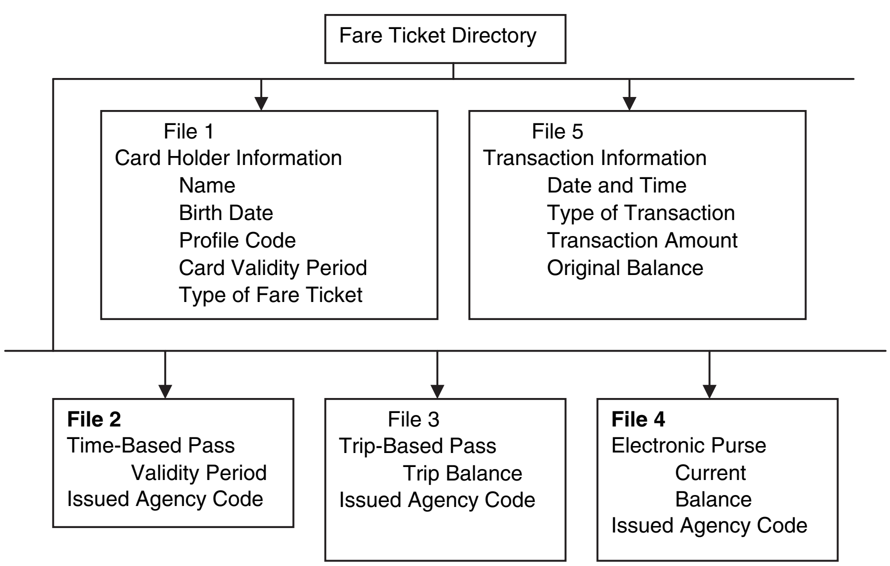

Figure 16. File structure of fare ticket on Mifare DESFire card.

cannot be changed once it is written, the card can be issued as a one-time used-fare ticket. The trip-based and time-based pass products on this card are designed to be used up to the maximum number of trips issued or within a period of time that has been written to the card. Because of the lack of data security, the electronic purse should not be implemented on this card. Information sensitive to the privacy of the cardholder or issuing agency should not be implemented on this card because the data can be read without requiring any authentication. In the AFC simulator, the irreversible data setting was disabled to limit the consumption of UltraLight cards during demonstration.

Figure 17 shows the simulator program flow. Business Rule application during transaction processing with the Mifare DESFire is shown in Figure 18. Business Rule application during transaction processing with the Mifare UltraLight is shown in Figure 19. An overview of the software architecture for the simulator is displayed in Figure 20.

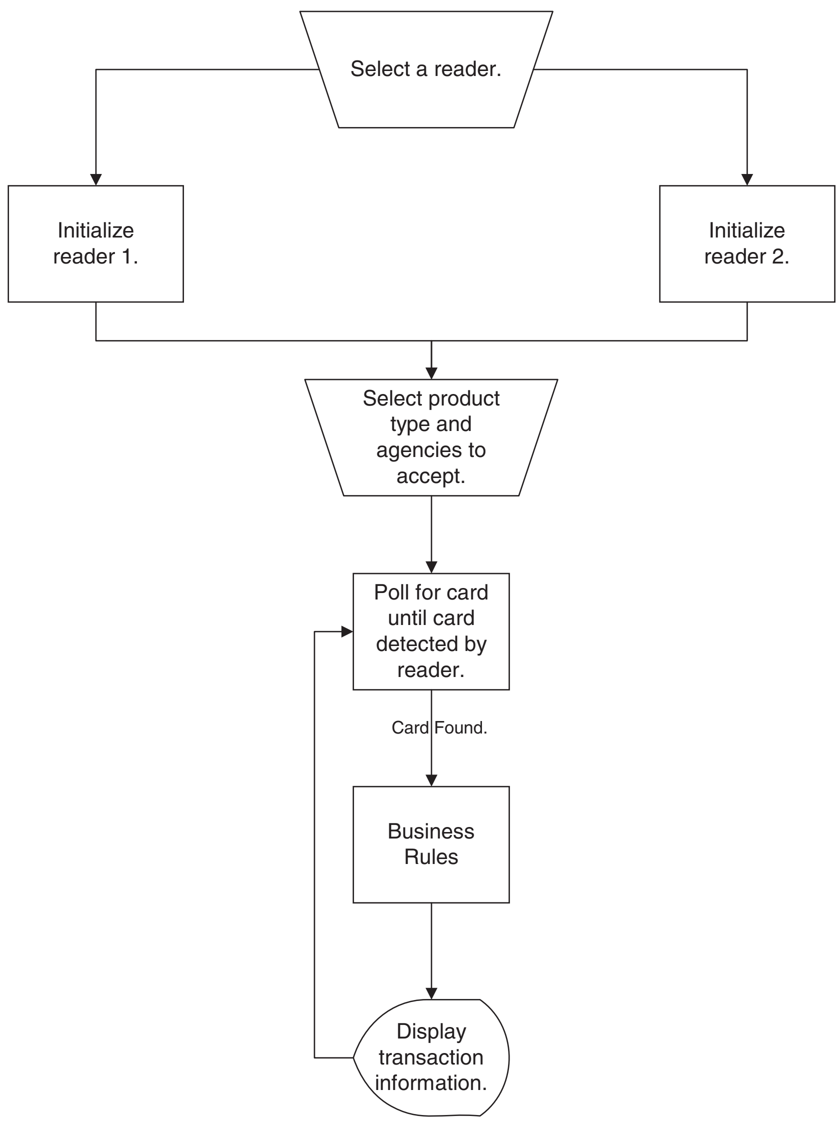

Figure 17. Simulator program flow chart.

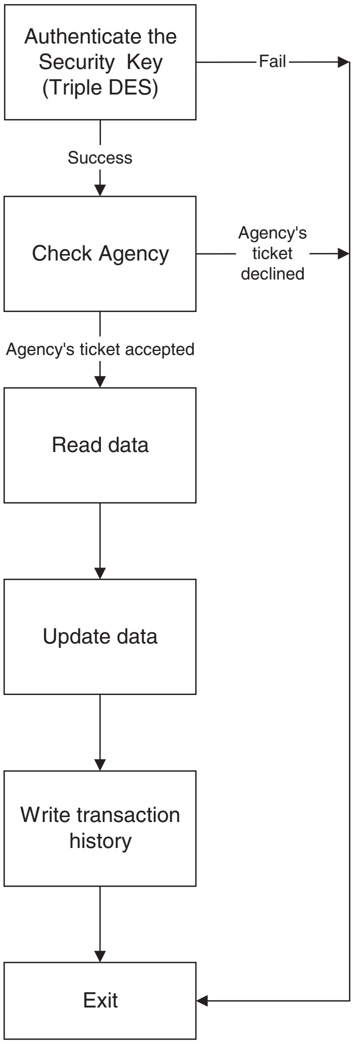

Figure 18. Business rules for Mifare DESFire

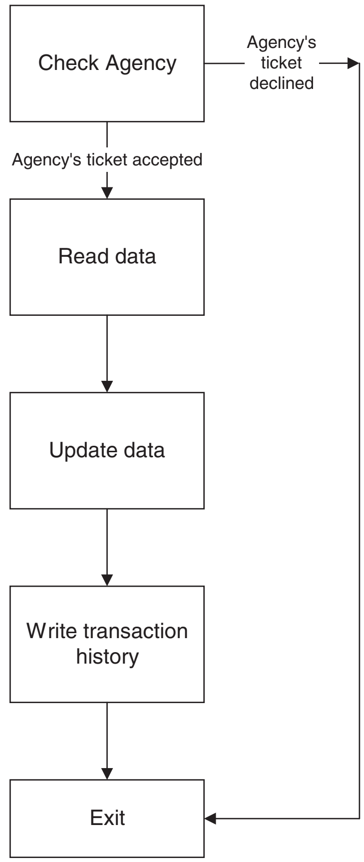

Figure 19. Business rules for Mifare UltraLight.

7.3 Demonstration

The following steps are required to run the simulator:

- Hardware Requirement
  - ASK LDB 215 contactless smartcard reader (RS-232 serial support) or OTI Saturn 5000 contactless smartcard reader (USB support)
  - Philips Mifare DESFire and Mifare UltraLight contactless smartcards
- Installing the simulator
  - Double click on "TCRP Installer.msi".
  - Follow the Acumen Setup Wizard instructions and click "Next". The simulator is named "TCRPSimulator.exe".
- Running the simulator
  - Connect a reader to the computer.
  - Run the simulator by clicking "TCRPSimulator.exe".
  - Click "Issue PICC" tab to issue a fare ticket on the smartcard.
  - Click "Monitor" tab for simulation.

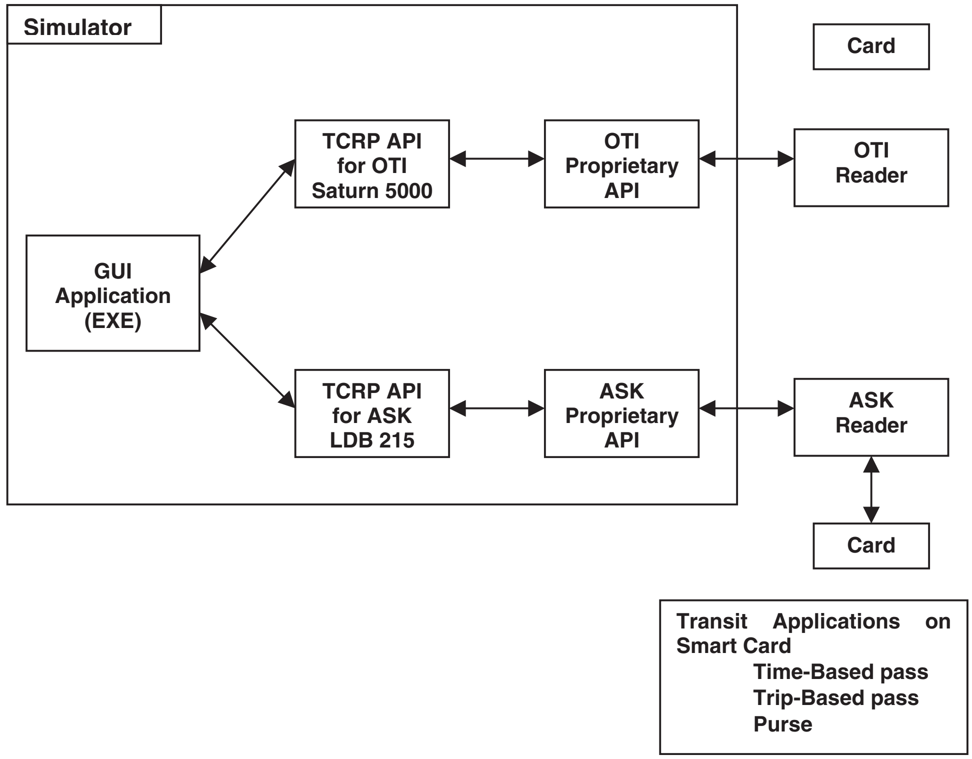

Figure 20. Simulator's components layout.

– Select a reader.
– Select agencies to accept its fare tickets.
– Click "Poll" button to start polling a fare ticket at the selected reader.

- Present the smartcard at the selected reader.
- The transaction information will show on the simulator.

7.4 Conclusion

Creating a standard contactless smartcard reader API for transit applications is feasible. Analysis of more contactless smartcard readers is needed to develop a broader and more scalable standard API.

CHAPTER 8

Conclusions

The best approach to take when determining the management and organization for a smartcard-based AFC environment will be determined by the existing capabilities of the region. If the region has an agency of good size with a significant level of experience in large-volume smartcard-based fare collection operations, then logically that agency should become the lead agency in developing a fare collection approach for the region. If an existing governing body presides over the transit agencies in the region and has a strong engineering support staff, then logically that governing body should lead the regional fare collection effort. If neither of these previous conditions exists, then the project should be led by a management committee that represents each of the agencies in the region.

Regarding implementation and operations, the best approach depends on the composition of the agencies in the region. If the region has a lead agency, it may make sense for that agency to become the central provider and integrator for operational services to the other agencies. Thus, the non-lead agencies outsource this function to the lead agency. This is a practical approach because the non-lead agencies lack the experience and depth to perform these functions and with this approach they do not need to commit resources to develop the core competency or expertise in this area. The lead agency simply builds on what it already does well and is compensated for this effort. If a region is run by a regional planning organization or a management committee, then a centralized approach is the obvious method. This approach is likely to be the result of the regional planning organization or management committee creating a specification of business rules derived from the fare policies of the regional agencies. The specification can now be put out to open bid where third-party contractors can propose solutions for program implementation. Regardless of the approach taken, agencies or management committees are best served by employing transit consultants to assist in their planning and implementation efforts. An agency will seldom possess the same level of in-house expertise as does the consulting firm.

Regardless of the management approach adopted, a fundamental step is the creation of a participant agreement acceptable to all participants. This agreement should be viewed as extensible to new participants in the region in the future. Another basic consideration should be an analysis of external factors influencing electronic fare payments. For example, if contactless bankcards have been introduced and are held by many patrons in a region, then perhaps the acceptance of contactless bankcards would be a system design imperative.

It is always good practice to verify the results of system integration incrementally. Thus, a phased approach is the most responsible method of deploying a regional smartcard-based fare collection program. One approach for phasing this deployment would involve supplementing the Card Interface Device (CID) equipment into fare collection and issuing smartcard fare media initially to agency employees only. This would allow for real live data and statistics to be compiled for system-validation purposes with less risk than a full public deployment. Another strategy would be to introduce only a few fare products initially. This approach also limits the complexity of the system analysis and can give an ideal opportunity to uncover weaknesses or problems in the new system.

A contracting strategy balances the costs of management of vendor(s) versus the costs of equipment and services provided by vendor(s). Although a single vendor approach is the easiest to manage, the cost of products and services may not be as competitive, because very few single respondents can supply the complement of equipment and services for a regional smartcard-based fare collection system. Multiple vendors may provide a more competitive contract process, but the management is more complex and costlier. Given the many individual schedules that must be coordinated, the multiple vendor contract approach may lead to a longer elapsed time between the project inception and deployment when compared with the single procurement contract model. The decision to use multiple vendors may also be determined by the size of the agency and the scale of the deployment. The larger the project, the higher the degree of complexity required to manage the overall project.

Financial management issues, such as settlement of payment and funds pool management, should be decided by a finance committee set up by the region. The decision of whether clearing and settlement should be centralized is the decision of the committee. A centralized clearinghouse is the easiest approach; however, the overhead required to operate the clearinghouse may be a barrier. A decentralized approach, where agencies must have relationships with each other for reimbursement and transfer privilege, requires greater effort on the part of any given agency to maintain these multiple relationships. This method, however, might be the most financially practical solution. The adoption of one approach over another is best indicated by the level of inter-agency use by patrons. More specifically, if an agency has predominantly single-agency transactions, then centralized clearing is inefficient.

Current deployments of smartcard-based fare collection systems throughout the world demonstrate that there is no clear technical or business model for creating an interoperable environment. Every system studied shows some attempt of using currently available standard features for smartcard-based systems, but these implementations are mainly proprietary because of waivers granted with respect to the use of these standards. For example, most smartcards comply with the ISO/IEC 14443 standard; however differences in the implementation of minute details, such as response timing, can preclude the interoperation of cards and readers. Not all of the readers used in these projects are fully ISO/IEC 14443 compliant, nor do they all support both Type A or B smartcards, and only one agency has implemented a full ISO/IEC 7816-4 command set to define the communication between the card and the reader in a standard manner. With regard to security, smartcard applications, interfaces, and back-end systems, the implementations involve a mixture of schemes, all of which are mainly proprietary. The current system implementations show they can be the first step in effectively moving the transit industry toward interoperability. The next challenge for smartcard-based systems should be to adopt standards in order to move toward this goal. If transit systems make full compliance to ISO/IEC 14443 and ISO/IEC 7816-4 a procurement requirement from equipment integrators, the problem of smartcard hardware interoperability could, to a large degree, be solved.

Almost all current national and international transit implementations of smartcard-based fare collection systems are proprietary. To reach true interoperability and a competitive environment for smartcard-based fare collection solutions, transit must insist on using standards throughout all tiers of the system. Doing so will result in greater availability of multi-source vendors to supply products and services at a greater cost savings to agencies. As standards such as ISO/IEC 14443 and ISO/IEC 7816 become more ubiquitous, transit fare collection components must be built on them. It is projected that form factors for contactless fare media will be expanding from just cards to soon include watches, fobs, and cell phones. Other contactless applications on the horizon include banking, retail, and building access. Transit must keep standards a priority and look for new form factors and cooperation with other potential issuers like banks or retailers.

Limited-use smartcards, also known as memory logic cards, have restricted capabilities and are a low-cost solution for transit agencies. On this class of card, the processor provides read/write and limited or no security for these operations. These cards are best suited for applications that do not require a great deal of data or high security, such as a one-trip ticket or daily pass. At a minimum, these cards should adhere to the ISO/IEC 14443 specification parts 2 through 3. [These parts define the radio frequency power and signaling interface scheme, of which there are two (Type A and B), and define the initialization and anti-collision procedures.] This class of smartcard typically offers a very small amount of memory, on the order of 48 bytes, and they are only suited to applications with limited memory requirements. At this time, no limited-use cards support the ISO/IEC 7816-4 commands and only implement proprietary commands. Although this precludes the transparent substitution of limited-use cards from one vendor to the product of another vendor, the low cost of these devices is likely to determine their use in emerging AFC systems, despite their inherent lack of interoperability.

Full-featured smartcards, which contain a microprocessor, are more expensive, but offer greater capabilities than the limited-use smartcards. These cards are best suited for long-term use, because they offer greater storage capacity, the capability of storing of multiple applications, and a higher security model. These cards should not only offer the same ISO/IEC 14443 Parts 2 through 3 requirements of the limited-use cards, but also be Part 4 compliant. (ISO/IEC 14443 Part 4 defines the transmission protocol and framing for data exchange.) As memory storage size on smartcards increases, the value of a robust transmission protocol will become more evident. The fully featured smartcard should also adhere to the entire APDU set defined in Part 4 of the ISO/IEC 7816 specification, which standardizes a command set used for data exchange between the reader/writer unit and the smartcard. Adopting ISO/IEC 7816 Part 4 and 3DES as the standard security level would standardize the security process for the smartcards. This would solve a major problem with current smartcard implementations, where most security schemes are proprietary. Requiring these ISO specifications would virtually turn smartcards into a commodity item and increase the number of smartcard sources available and increase vendor competition.

The reader/writer device, also known as a proximity coupling device (PCD) or CID, should also adhere to standards. The difference between a PCD and a CID is that a PCD is a "dumb" device, commanded by a host controller device such as a single board computer in a faregate or TVM. It is the primary job of the PCD to pass instructions and data between the host controller and a smartcard. Conversely, a CID is a self-contained unit constructed with an embedded processor and code to implement the instructions and business logic and is connected directly to the components responsible for the radio frequency (RF) generation and modulation. A PCD can be an interchangeable device, no matter what model or manufacturer; however, it is also a slower solution for smartcard transactions because of its additional layer of communication to an external host processor. The CID model offers faster smartcard transaction times, but also makes a change in reader/writer deployment more difficult, because a rewrite of the logic will probably be required. In an interoperable environment, both the PCD and CID must be able to work with both Type A and B smartcards as defined in the ISO/IEC 14443 Part 2 specification. Also, the CID must be able to add at least two SAMs in its design. The SAM allows a safe method for both deploying secret key information for authentication and encrypting the data transmitted during a secure smartcard transaction.

A common data model is also critical to achieve interoperability for smartcard-based systems. A minimum set of data elements common to all systems must be defined and used. This set of data should consist of information about the cardholder, including card identification number, card issuer identification, patron profile code, and card validity period, and information about the products, including product identification number, product validity period, and fare amount for electronic purse transactions. This set of data should also contain information about the journey, such as agency identification number, date/time of journey event, entry and exit location of journey, and route number.

Also, adopting a regional data standard that meets the minimum data element set, such as the RIS or the Universal Transit Farecard Standards (UTFS), is highly desirable and essential if intraregional operability between regions is desired. The RIS and UTFS also offer other data items that can be used within other agencies. Another benefit of adopting a published data model standard is that it is easily understood and allows for competitive vendor selection for implementation and further system expansion and maintenance.

The data standard adopted by transit should have broad capabilities to allow for many types of electronic fare payments. If it is broad and flexible enough, it can allow non-transit applications such as parking, bridge and highway tolls, retail, access control, movies, and school services, to share a common purse with transit applications. The RIS has been designed in such a manner and should serve as a preferred path for future implementations based on a stored-value/transit application model. This can be used in addition to the acceptance of bankcards directly.

A standard approach for security on both hardware components and data flow throughout the system tiers must be defined and established for smartcard-based fare collection systems. Hardware and communications channels should be as secure as messages between a front-end device and the bank clearinghouse [e.g., the Verifone security model for personal identification number (PIN) pads]. In the PIN pad model, if a hardware device is ever tampered with or altered in order to "sniff" messages, the unit becomes permanently inoperable. The same level of security should be applied to PCDs and CIDs. For the software layer, there must be a standard proposal to generate a signature for a transaction; this ensures data integrity and fully encrypts the data stream to provide data confidentiality. Current public algorithms such as SHA1 for signatures and DES/3DES for encryption would be solid choices for this approach.

A standard API was developed for this project and was designed to prove that a software layer with a common command set could be created to work between a host application and different manufacturer/model PCD/CID, which then interface with a smartcard. All smartcards for this project must be at least ISO/IEC 14443 Parts 2 to 3 compliant. Today, virtually no PCD/CID offers a common way to poll (search for) or query/update an ISO/IEC 14443 Part 2- to 3(4)-compliant proximity integrated circuit card (PICC) in the generated RF field. All PCDs/CIDs offer either a very small subset of the ISO/IEC 7816 Part 4 commands or their own proprietary commands. This API proved that the commands supplied by the manufacturer for each of the PCDs/CIDs selected for the project can be translated into a common set of newly defined commands, thus forming a seamless layer between the host application and the PCD/CID. If this API is instituted by the PCD/CID manufacturers as a driver or maintained as a TCRP dynamic load library (DLL) module, the API would ensure that any TCRP-compliant PCD/CID could be interchanged without any affect on the system.

Since the inception of this project, technology and industry requirements have changed and the need for the API has diminished. The transit industry is moving from the PCD model toward the CID model, where the business logic is integrated in the device. The CID today is capable of higher processing power and becoming a central component of fare collection device (e.g., faregates and TVMs), thus a generalized programming strategy seems more inapplicable than it did at the outset of this project and the API itself may not be the most efficient mechanism moving forward; however, it may prove of great value in the incremental modernization of legacy systems or early proprietary smartcard implementations.

Transit must compel the use of standards as a part of all future procurement efforts to foster the interoperability of smartcard-based AFC systems. Anything short of full compliance to ISO/IEC 14443 and ISO/IEC 7816-4 should no longer be acceptable for transit applications. New and emerging AFC programs must accept and embrace an agreed-on standard data format defining the data elements to be held on the smartcard. The RIS or UTFS are flexible systems ideally suited for this use. If transit agencies collectively resolve to make using these standards a high priority in system development and procurement projects, the cause of smartcard interoperability in transit AFC systems will be greatly advanced.

APPENDIX A

Set of Functionality for a Standard API

The API proposed under this work is intended to standardize the implementation aspects associated with contactless smartcards as a fare media for mass transit applications.

A.1 API Functions

This section describes the functions that will be provided by the API and the associated parameters, return values, and pre/post conditions for each function.

Table A-1 presents the API-provided CloseReader function used to close an open interface to a particular contactless smartcard reader.

Table A-2 describes the API-provided GetDriverCap function used to return information about the driver capabilities for the API-compliant driver. This would include information about the API version supported and any support for optional API instructions.

Table A-3 describes the API-provided GetPCDProp function used to retrieve a list of properties associated with the actual hardware reader defined by a particular reader ID. This command serves as a configuration interrogation utility.

Table A-4 describes the API-provided GetPCDStatus function used to retrieve the current status of the PCD. This command can be used to verify the current condition of a particular reader.

Table A-5 describes the API-provided OpenReader function used to initialize and open an interface to a particular contactless smartcard reader.

Table A-6 describes the API-provided Poll function used to instruct the reader to initiate probing of the field for contactless card(s). The behavior of the Poll will be defined by the options defined in the xPICC parameter.

Table A-7 describes the API-provided RetrieveFirmware function used to extract currently installed firmware from a reader supporting this type of download. It is intended to function as a standard firmware extraction utility for retrieving an image to be used in a potential restoration.

Table A-8 describes the API-provided SendFirmware function used to send an updated firmware to a reader supporting this type of upload. It is intended to function as a standard firmware mounting utility.

Table A-9 describes the API-provided SetPCDProp function used to set attributes associated with the actual hardware reader defined by a particular interface ID in PCDProp. This command serves as a configuration-setting utility.

Table A-1. TCRPAPI: CloseReader.

Syntax	int CloseReader (PCD* xPCD);	
Data Type	**Field Name**	**Description**
PCD*	xPCD	Pointer to the PCD structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	The function returns 0 if successful. Otherwise, it returns 2008.	

Table A-2. TCRPAPI: GetDriverCap.

Syntax	int GetDriverCap (DriverCap* xCap);	
Data Type	**Field Name**	**Description**
DriverCap*	xCap	Pointer to the DriverCap structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Function returns 0 if successful. Otherwise, returns 2008.	

Table A-3. TCRPAPI: GetPCDProp.

Syntax	int GetPCDProp (PCDProp* xPCDprop);	
Data Type	**Field Name**	**Description**
PCDProp*	xPCDProp	Pointer to the PCDProp structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Reader properties and attributes will be set to PCDProp structure if the function execution is successful.	

Table A-4. TCRPAPI: GetPCDStatus.

Syntax	int GetPCDStatus (PCD* xPCD);	
Data Type	**Field Name**	**Description**
PCD*	xPCD	Pointer to PCD structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Outgoing command status is set to nPCDstatus of PCD structure will be set to current status of a reader. The information shall indicate the type of reader, its communication type, and target reader identification number.	

Table A-5. TCRPAPI: OPENREADER.

Syntax	int OpenReader (PCD* xPCD);	
Data Type	**Field Name**	**Description**
PCD*	xPCD	Pointer to PCD structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	The function returns 0 if successful. Otherwise, it returns 2008. Device Identifier will be assigned in PCD structure if successful. (It will be assigned to zero if device identifier is not supported.)	

Table A-6. TCRPAPI: Poll.

Syntax	int Poll (PICC* xPICC, PCD xPCD);	
Data Type	**Field Name**	**Description**
PICC*	xPICC	Pointer to the PICC structure
PCD	xPCD	PCD structure
Return Value	0	Successful execution
	2008	Failed execution
	2002	Timeout
	2088	No precise diagnosis
Precondition	The OpenReader function should be executed successfully prior to Poll function.	
Return Code(s)	If there is no card in the field, nPICCTYPE is set to 0x00 in PICC structure. If a card is found in the field, its serial number is assigned to the byte array of nPICCUid and the length of the serial number is assigned to nPICCUidLen in PICC structure. If the card in the field is ISO 14443-4 compliant, bISOPart4 is set to true in PICC structure.	

Table A-7. TCRPAPI: RetrieveFirmware.

Syntax	int RetrieveFirmware (Firmware* xFirm int nID);	
Data Type	**Field Name**	**Description**
Firmware*	xFirm	Pointer to Firmware structure
int	nID	Interface ID of the communication target.
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Function returns 0 if successful. Otherwise, it returns 2008.	

Table A-8. TCRPAPI: SendFirmware.

Syntax	int SendFirmware (Firmware* xFirm int nID);	
Data Type	**Field Name**	**Description**
Firmware*	xFirm	Pointer to Firmware structure
int	nID	Interface ID of the communication target.
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Function returns 0 if successful. Otherwise, it returns 2008.	

Table A-9. TCRPAPI: SetPCDProp.

Syntax	int SetPCDProp (PCDProp xPCDprop);	
Data Type	**Field Name**	**Description**
PCDProp	xPCDProp	PCDProp structure
Return Value	0	Successful execution
	2008	Failed execution
Precondition	None	
Return Code(s)	Function returns 0 if successful. Otherwise, it returns 2008.	

Table A-10. TCRPAPI: TransmitToCard.

Syntax	int TransmitToCard (Command_Frame xCommandFrame, Response_Frame* xResponseFrame, BYTE nPICCType, PCD xPCD);	
Data Type	**Field Name**	**Description**
Command_Frame	xCommandFrame	Command_Frame structure for outgoing command frame to the card.
Response_Frame*	xResponseFrame	Pointer to the Response_Frame structure for the incoming response frame from the card.
BYTE	nPICCType	Type of card
PCD	xPCD	PCD structure
Return Value	0	Successful execution
	2008	Failed execution
	2002	Timeout
	2088	No precise diagnosis
Precondition	OpendReader and Poll functions should be executed successfully prior to TransmitToCard function.	
Return Code(s)	Outgoing command status is set to nPCDstatus of the Response_Frame structure. Incoming response frame from the card is set to the byte array baReceiveFrame and the length of the response frame is set to nActualLength in the Response_Frame structure.	

Table A-10 describes the API-provided TransmitToCard function used to instruct the reader to send a block of data to the card and retrieves a response frame if there is a response from the card before a specified timeout, which is configured in the Response_Frame structure.

A.2 API Structures

This section defines the data structures used as parameters by the functions.

Table A-11 defines the Command_Frame structure that contains the outgoing command frame to the card and its length.

Table A-12 defines the DriverCap structure, which contains the supported API version number and information about any support for optional API instructions.

Table A-13 defines the Firmware structure that contains the size, revision level, intended checksum, and actual binary image to be transferred to the target reader.

Table A-14 defines the PCD structure, which contains interface information about the contactless smartcard reader.

Table A-15 defines the PCDProp structure that contains the particular properties and attributes of the associated reader with respect to smartcard communication. It includes the number of SAM slots, the modulation types supported, and options to define the antenna strength, protocols, and target reader identification number.

Table A-16 defines the PICC Structure that contains the options to define behavior of the polling.

Table A-17 defines the POLLPICCTYPE structure that contains an options defined type of card to be polled from the reader.

Table A-18 defines the Response_Frame structure that contains incoming response data from the card and the options to define timeout delay to retrieve the response frame.

Table A-11. Command_Frame structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
short	nLength	Length of the command frame
BYTE*	baSendFrame	Outgoing command data frame **Remark**: Outgoing command data (baSendFrame) must be terminated by 0x00. If the raw command length is 2, a null terminator shall be appended and the length of the command frame in this structure will be 3. For example: the raw command is {0x5F, 0x02}. The data in baSendFrame of this structure would be set to {0x5F, 0x02, 0x00}, and the value of nLength would be set to 3.

Table A-12. DriverCap structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
BYTE	nVersion	Supported TCRP API version
char*	cOptional	Supported optional API instructions

Table A-13. Firmware structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
WORD	nRevisionLevel	Revision level number of the firmware
unsigned long int	nSize	Number of bytes of the firmware content
unsigned char*	cImage	Firmware content
WORD	nCheckSum	CRC of the firmware content

Table A-14. PCD structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
BYTE	nDevice	Target reader to be initialized.
BYTE	nID	Interface ID for identification of communication target. This provides for multi reader operation under a single host
BYTE	nCommType	Communication Type, Serial = 0x01, USB = 0x02
BYTE	nComPort	COM port number
char*	cUsbName	USB device name
BYTE	nPCDstatus	PCD operational status 0: good 1: out of service

Table A-15. PCDProp structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
BYTE	nDevice	Target reader identification number
int	nAntennaStrength	Options to set the reader's antenna strength
char*	cProtocol	Options to set the reader's protocol mode
BYTE	nSAM	Number of SAM slots in the reader
char*	cModType	Reader Modulation Type

Table A-16. PICC structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
POLLPICCTYPE	xPICCTYPE	Type of card to poll
BYTE	nPICCsToSearch	Number of card to search
BYTE	nTimeout	Timeout delay for polling
short	nSessionID	Session ID for communication to the card
BYTE	nPICCUid[256]	Card Serial Number
int	nPICCUidLen	Length of serial number
BYTE	nPICCTYPE	Type of card found, 0x01 = Mifare Ultralight 0x02 = Mifare DESFire **Remark**: Future version will have more card types.
bool	bISOPart4	ISO 7816 part-4 compliant

Table A-17. POLLPICCTYPE structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
bool	ISOA	TYPE A card
bool	ISOB	TYPE B card
bool	MifareClassic	Phillips Mifare Classic 1K card
bool	MifareUltralight	Phillips Mifare Ultralight card
bool	Jewel	Jewel card
bool	MV4000	MV 4K card

Table A-18. Response_Frame structure.

Parameters	List of members	
Data Type	**Field Name**	**Description**
short	nExpectedLength	Expected length of the response frame
short	nActualLength	Actual length of the response frame
BYTE	baReceiveFrame[256]	Incoming response data frame
int	nPCDStatus	Outgoing command status
short	nNumIterations	Number of iteration to check the response frame from the card
short	nIterationTimeout	Timeout delay of each iteration

A.3 Example

(OpenReader, CloseReader, Poll, TransmitToCard):

```
int retValue;

BYTE piccType = 0x02;
PCD reader;

reader.nCommType = 0x01;
reader.nComPort = 0x03;

retValue = OpenReader(&reader);

if(retValue == 0)
{
        PICC card;

        card.xPICCType.ISOA = true;
        card.xPICCType.ISOB = true;
        card.xPICCType.MifareClassic = false;
        card.xPICCType.MifareUltralight = false;
        card.xPICCType.Jewel = false;
        card.xPICCType.MV4000 = false;
        card.nPICCsToSearch = 0;
        card.bISOPart4 = false;

        retValue = Poll(&card, reader);

        if(retValue == 0 && card.nPICCTYPE != 0x00)
        {
                BYTE acutalCommand[3] = {0x5F, 0x02, 0x00};

                Command_Frame commandStruct;
                Response_Frame responseStruct;

                commandStruct.baSendFrame = actual Command;
                commandStruct.nLength = 3;

                responseStruct.nNumIterations = 2;
                responseStruct.nIterationTimeout = 100;
                response.nExpectedLength = 1;

                retValue = TransmitToCard(command Struct, &response Struct, piccType,
                reader);
                }
        }

CloseReader(reader);
```

Abbreviations and acronyms used without definitions in TRB publications:

AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
ACRP	Airport Cooperative Research Program
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
NASA	National Aeronautics and Space Administration
NCFRP	National Cooperative Freight Research Program
NCHRP	National Cooperative Highway Research Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
SAE	Society of Automotive Engineers
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century (1998)
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation