



Module 5: Smart Card Usage Models – Payments and Financial Transactions

**Smart Card Alliance
Certified Smart Card Industry Professional
Accreditation Program**



About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.



Important note: *The CSCIP training modules are only available to LEAP members who have applied and paid for CSCIP certification. The modules are for CSCIP applicants ONLY for use in preparing for the CSCIP exam. These documents may be downloaded and printed by the CSCIP applicant. Further reproduction or distribution of these modules in any form is forbidden.*

Copyright © 2010 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1	INTRODUCTION	5
2	SMART CARD MARKET DRIVERS AND BENEFITS FOR PAYMENTS AND FINANCIAL TRANSACTIONS	6
2.1	REDUCING FRAUD AND ENHANCING SECURITY	6
2.2	ENHANCING CONSUMER CONVENIENCE AND CONFIDENCE	7
2.3	ENHANCING THE BUSINESS CASE WITH MULTIPLE APPLICATIONS.....	7
2.4	IMPROVING EFFICIENCY AND INCREASING SALES VOLUME AT THE MERCHANT POS.....	7
2.5	SUPPORTING INNOVATION AND DIFFERENTIATION	8
2.6	SUPPORTING STRONG AUTHENTICATION FOR ONLINE / INTERNET TRANSACTIONS	8
3	BANK CARDS.....	9
3.1	BANK CARD TECHNOLOGY AND PROCESSING.....	9
4	CREDIT/DEBIT PAYMENT WITH SMART CARDS.....	12
4.1	EMV	12
4.1.1	EMV Security	12
4.1.2	EMV Transaction Flow.....	16
4.1.3	EMV Infrastructure Requirements	17
4.2	CONTACTLESS CREDIT/DEBIT PAYMENT	20
4.2.1	EMV Contactless.....	20
4.2.2	Contactless Credit/Debit Payment in the U.S.	21
4.2.3	Contactless Benefits	22
4.2.4	Developments in Contactless Payments.....	24
5	E-PURSE AND STORED VALUE CARDS	25
5.1	OPEN SYSTEM WITH E-CASH VALUE ON THE CARD AND CENTRAL ACCOUNT MANAGEMENT.....	26
5.2	OPEN SYSTEM WITH NO CENTRAL ACCOUNT MANAGEMENT	27
5.3	CLOSED SYSTEM WITH SEMI-OFFLINE ACCOUNT MANAGEMENT	28
5.4	CLOSED SYSTEM WITH ONLINE CENTRAL ACCOUNT MANAGEMENT (PREPAID ONLINE)	29
6	TRANSPORTATION AND PARKING PAYMENT	30
6.1	TRANSIT.....	30
6.1.1	Transit Smart Card Implementations.....	30
6.1.2	Traditional Transit Payment.....	33
6.1.3	Developments in Transit Payment	34
6.1.4	Smart Card Benefits to Transit	37
6.2	PARKING	39
6.2.1	Parking Market Segments.....	40
6.2.2	Use of Smart Card Technology in Parking	43
6.2.3	Smart Card Benefits for Parking.....	45
7	ONLINE BANKING AND RETAIL ECOMMERCE	49
8	SAMPLE SMART CARD PAYMENT MODELS	51
8.1	U.S. CONTACTLESS CREDIT/DEBIT PAYMENT.....	51
8.2	TRANSIT.....	52
8.2.1	Washington Metropolitan Area Transit Authority and Surrounding Area.....	52
8.2.2	Utah Transit Authority.....	53
8.2.3	London Oyster/Barclaycard.....	54
8.2.4	Hong Kong Octopus Card.....	56
8.3	PARKING	57

8.3.1	<i>Washington Metropolitan Area Transit Authority</i>	57
8.3.2	<i>Parking Operations in Israel</i>	60
9	RELEVANT STANDARDS AND SPECIFICATIONS	63
9.1	STANDARDS RELEVANT TO SMART CARD PHYSICAL CHARACTERISTICS	63
9.2	STANDARDS RELEVANT TO TECHNOLOGIES WHICH COULD BE FOUND ON A SMART CARD	63
9.3	STANDARDS AND SPECIFICATIONS RELEVANT TO TECHNOLOGIES RELATED TO THE CARD INTERFACE	64
9.4	STANDARDS AND SPECIFICATIONS RELEVANT TO THE CARD COMMANDS AND APPLICATION DATA STRUCTURES	64
9.5	STANDARDS AND SPECIFICATIONS RELEVANT TO ISSUERS OR SPECIFIC INDUSTRY SECTORS	64
10	REFERENCES	65
11	ACKNOWLEDGEMENTS	68



1 **Introduction**

This module describes how smart cards are used in payment and payment-related applications. After reviewing this module, CSCIP applicants should be able to answer the following questions and be familiar with examples of reference smart card implementations.

- What are the drivers and benefits for smart card technology in payment applications?
- How are smart cards used for bank card payments?
- What is EMV and how do EMV-based financial transactions work?
- What are contactless payment transactions and how do they differ from magnetic stripe-based transaction?
- How are smart cards used for e-purse or stored value payment?
- How are smart cards used for transit and parking payment applications?
- What are the relevant standards for smart cards used for payment applications?



2 Smart Card Market Drivers and Benefits for Payments and Financial Transactions

Both contact and contactless smart cards are used for many payment and payment-related applications worldwide. Smart card-based payment applications may be categorized across two dimensions:

- The configuration of the payment platform used to deliver payment functionality as either an:
 - Open loop payment system
 - Closed loop payment system
- The location of where the value that is available to the cardholder is stored, either:
 - Held as value in the memory of the card
 - Held in an account in a back office

The matrix in Figure 1 provides an overview of the relationships between these two dimensions and provides examples for each category. The examples identified in the matrix are discussed in further detail throughout this module. Each smart card-based payment application or product can be mapped into one of the four categories defined in Figure 1.

Figure 1. Payment Application Dimensions

Payment Applications	Closed Loop Payment System	Open Loop Payment System
Card-Based Stored Value	<ul style="list-style-type: none"> Traditional transit fare payment cards (e.g., London Oyster, Hong Kong Octopus, Washington, DC SmarTrip) SmartMeter parking card 	<ul style="list-style-type: none"> Visa Cash Mondex
Back Office Account-Based	<ul style="list-style-type: none"> Merchant stored value cards (e.g., Starbucks card) Gift cards Electronic toll collection (e.g., EZ-Pass, FasTrak) 	<ul style="list-style-type: none"> Bank-issued EMV credit and debit cards Contactless bank cards (e.g., MasterCard PayPass; Visa payWave; ExpressPay by American Express)

This section describes the drivers for smart card technology being used for payment applications and the benefits that the technology offers for payment and payment-related transactions. Additional information on benefits for specific markets and applications are included in the sections that follow.

2.1 Reducing Fraud and Enhancing Security

A primary driver for smart card technology in payment applications is its ability to enhance the security of the payment card and the payment transaction to address fraud.

Historically, magnetic stripe technology was used for payment applications. Magnetic stripe technology is limited with respect to modern security techniques as payment transactions rely on static account numbers or data stored on the card. Because this static data is easily copied, information can be stolen and duplicate magnetic stripe cards created. Within the payment systems, fraud checks are therefore performed in the back-end systems to manage the risk of counterfeit or stolen cards being used.

Smart cards address the growing problem of fraud and offer a secure solution for both open and closed payment systems.

Smart card technology provides strong payment card security. Well designed smart cards are very difficult to duplicate or forge and data stored in the chip cannot be modified without proper authorization (a password, biometric authentication or cryptographic access key). Smart cards help to deter counterfeiting and thwart tampering. Smart cards include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks.

Sensitive payment account information and/or value can be securely stored on the smart card. For example, the cardholder personal identification number (PIN) can be stored on the card and verified by the card without having to go online to the card issuer's host system.

The smart card and the payment terminal can interact to make decisions about whether a transaction can take place.

The smart card can generate dynamic data with each transaction, providing both better information for authorization decisions and rendering transaction data impervious to fraudulent use.

2.2 Enhancing Consumer Convenience and Confidence

Consumer convenience is enhanced when using smart payment devices. Contact cards provide the convenience and security of an offline PIN capability in networks where online PIN is not supported.

Contactless payment enhances consumer convenience at the POS. Another advantage for consumers is that they control the contactless payment device. The device is always in the consumer's possession, reducing the possibility of leaving it somewhere accidentally and minimizing the potential for fraud.

Smart stored value payment cards provide consumers with a secure alternative payment mechanism.

Smart contactless transit payment cards allow consumers to quickly and reliably pay fares.

2.3 Enhancing the Business Case with Multiple Applications

Smart card technology enables an issuer to include and offer multiple applications on one card. By taking advantage of the smart card chip's capabilities, issuers can enhance the business case for implementing smart payment cards and increase the ability of that system to handle future needs. Examples of applications that could be offered on a smart payment card include:

- Open credit/debit payment
- Choice of credit, debit or prepaid on one card
- Proprietary payment (e.g., transit payment application or campus payment application)
- Loyalty
- Electronic purse
- Electronic benefits
- Identity applications for physical and/or logical access

2.4 Improving Efficiency and Increasing Sales Volume at the Merchant POS

Contactless payments improve efficiency at the merchant POS. Contactless payments are faster and more convenient for consumers than cash or magnetic stripe card payments. Increased speed and convenience generate greater sales volumes and increase customer spending. Customers spend up to 20%–30% more when using contactless payment devices than when they use cash.¹

¹ Source: Chase

Customers not only spend more: the use of contactless payments also reduces the requirement for and cost of handling cash while also improving operational efficiencies and reducing terminal maintenance costs.

2.5 Supporting Innovation and Differentiation

Both contact and contactless smart card technology can offer issuers and merchants opportunities for innovation and differentiation.

Issuers can differentiate their contactless payment products with innovative new form factors, tailored to specific consumer preferences (for example, key fobs, mobile devices, micro tags, or stickers), and provide products and services that take advantage of the functionality available with the new form factors. Both contact and contactless payment devices can support multiple applications.

Merchants and issuers can collaborate on payment products that blend specific features, packaging (cards, tokens, mobile phones), and applications and target different customer segments that have very particular requirements for the shopping experience.

2.6 Supporting Strong Authentication for Online / Internet Transactions

Both Internet e-commerce purchases and online banking are looking for stronger authentication solutions – beyond usernames and passwords – to validate that the customers accessing systems are who they say they are. Smart cards can be used to enable multi-factor authentication for online transactions, incorporating something that you have (the smart card), something that you know (typically a PIN that activates the card's cryptographic functions), and a one-time password to access the online site. Additional information is included in Section 7.



3 **Bank Cards**

Bank cards are defined as any card issued by a bank that can access a consumer's financial resources. Bank cards include the following:

- Credit cards, which provide access to a consumer's credit line.
- Debit cards, which directly access a consumer's checking or savings account. Debit cards can be used at merchant POS locations either with or without a consumer-unique personal identification number (PIN).
- ATM cards, which provide consumer with access to their checking and savings accounts through automated teller machines (ATMs) using a PIN to authenticate that they are the owner of the account. ATM cards can be used at merchant POS locations, but require a PIN for cardholder authentication.
- Prepaid cards, which provide access to a prepaid value, rather than a line of credit. The card is used until the value is gone and the card is discarded or reloaded.

Bank cards, bank card message formats, and bank card processing requirements are defined by ISO/IEC standards and by specifications developed by the payments industry and payment brands. Key standards and specifications for bank cards include:

- ISO/IEC 7810, defining the physical card characteristics.
- ISO/IEC 7811, defining the specifications for embossing cards and encoding data onto a card's magnetic stripe.
- ISO/IEC 7812, specifying the numbering system for the identification of issuers of cards.
- ISO/IEC 7813, specifying the data structure and data content of magnetic tracks 1 and 2, which are used to initiate financial transactions.
- ISO/IEC 7816, specifying physical dimensions, electrical interface, communications protocols, card logical structure (files and data elements), various commands used by the application programming interface for basic use, application management, biometric verification, cryptographic services and application naming for smart cards.
- ISO/IEC 8583, specifying interchange messages for financial transaction card originated messages.
- ISO/IEC 14443, specifying the interfaces for a contactless smart card.
- EMV 4.2, specifying the standard smart card and transaction terminal operations to support globally interoperable financial smart cards.
- Specifications from American Express, Discover, JCB, MasterCard, and Visa, that define the payment application and the security requirements for branded bank cards.

3.1 **Bank Card Technology and Processing**

Bank cards currently use two technologies to store account information and to allow merchant POS terminals to read the information electronically – magnetic stripe technology and smart card technology.

Up until the late 1990s, magnetic stripe technology was used worldwide for bank cards. Figure 2 shows the information stored on tracks 1 and 2 of the magnetic stripe for bank cards.²

² *Smart Cards and Payments: Technology, Standards and Transactions*, Gilles Lisimaque presentation, Smart Card Alliance webinar, November 18, 2008

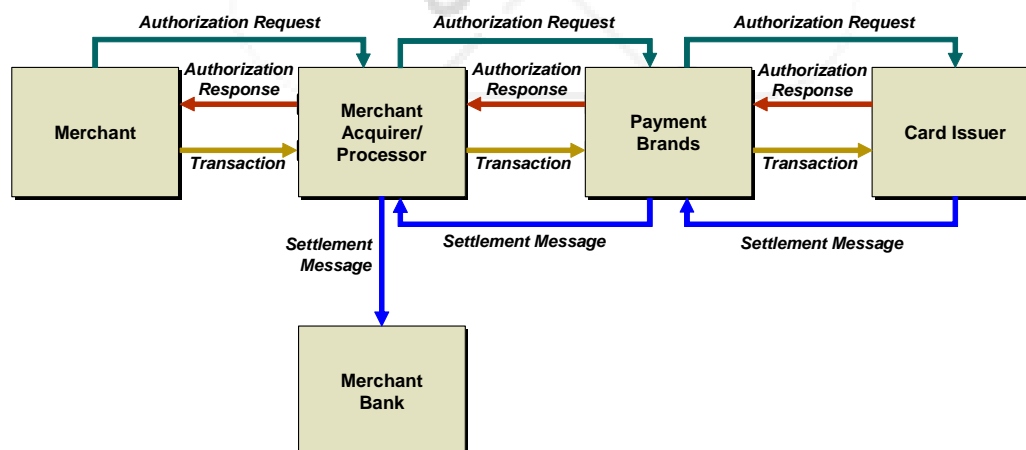
Track 1		210 bits /in.		79 characters		Alpha Numeric	
%B	Primary Acct. # up to 16 Char.	^	Name 2 to 26 Char.	^	Exp. date YY MM	Service Code	Discretionary
Track 2		75 bits /in.		40 characters		Numeric	
:	Primary Acct. # up to 16 Char.	=	Exp. date YY MM	Service Code	Discretionary		
Track 3		210 bits /in.		107 characters		Numeric	
Not used in most applications							

Figure 2. Magnetic Stripe Information on Bank Cards

The flow of a traditional magnetic stripe credit card payment transaction (shown in Figure 3) includes the following steps:

1. The merchant's point-of-sale (POS) system sends an authorization request for the transaction (including the cardholder account number, transaction amount, card verification code (CVC) / card verification value (CVV) for physical merchants) to the merchant acquirer/processor, who then sends it through the payment brands' financial networks to the card issuer. The merchant POS system can request additional information from the card or the cardholder (for example, zip code (for address verification (AVS)), signature, PIN) to authenticate the cardholder and/or to establish that the card was present for the transaction.
2. The issuer performs the necessary security checks (e.g., checking the security information included with the transaction, determining the validity of the payment card, analyzing cardholder behavior to assess if the transaction could be fraudulent), authorizes or denies the transaction, and returns an authorization response to the merchant acquirer/processor, who passes it to the merchant.
3. Authorized transactions are captured (cleared) from the merchant every day, and a settlement message is sent over the financial networks to transfer funds to the merchant account (transaction amount less merchant discount rate)³.

Figure 3. Credit Card Payment Transaction Flow⁴



³ See additional discussion in Section 3.3.

⁴ Source: Booz Allen Hamilton. This figure shows the transaction flow in an 'open loop' payment network (such as MasterCard and Visa); it does not show transaction flow for a 'closed loop' payment network where the acquirer, network and issuer functions are performed by a single entity, such as American Express.

It is important to note that magnetic stripe card transactions rely on static account numbers. Because this data is static the information can be easily stolen and re-used to create a duplicate magnetic stripe card. This practice is known as skimming. Within the financial system, fraud checks are performed in the back-end systems to manage the risk of counterfeit or stolen cards being used.

Increasing counterfeit card fraud led the financial industry to move to smart card technology for bank cards and to develop the global EMV standard for bank cards based on chip card technology. The EMV specification, first available in 1996, defines the global interoperable standard for smart bank cards.

The EMV security model is based on cryptographic authentication, with dynamic data used in the transaction to ensure that the card is authentic.⁵

- The card is programmed to make decisions within the parameters set by the issuing banks. For example, setting a maximum offline transaction amount or maximum cumulative number of offline transactions.
- The terminal and card use cardholder verification data (a PIN) and offline authentication data for risk management.
- The card performs risk management, generates the required dynamic cryptograms, and responds with the transaction data and decision to process online, approve or decline offline, or terminate the transaction.
- The terminal sends the authorization request and cryptograms to the processor for online authorization.

As of the end of 2009, more than 991 million EMV payment cards were in use worldwide, with over 14.5 million EMV terminals active in the marketplace⁶. Payment brand mandates have driven or are driving Europe, Asia, Africa, Latin America and Canada to EMV. Additional information about EMV can be found in Section 4.1.

The United States is the only country with no current plans or mandates for EMV. Within the U.S., however, contactless credit and debit cards are now being issued that include some EMV security features. Additional information about U.S. contactless payments can be found in Section 4.2.

⁵ *Smart Card Standards 101*, William Gostkowski presentation, Smart Card Alliance CTST Workshop, May 4, 2009

⁶ *EMVCo: Creating Global Standards for Proximity Payments*, Brian Byrne (EMVCo) presentation, Smart Card Alliance Annual Conference, May 18, 2010

4 Credit/Debit Payment with Smart Cards

Smart card technology introduced three significant factors to a payment card beyond what was provided by magnetic stripe card technology. The first is greater storage capacity for information. In comparison to the magnetic stripe, which holds 210 bits in track 1 and 75 bits in track 2, the ICC on smart cards in the early 90's provided 2k bytes of storage space. Today the integrated circuit chip (ICC) storage capacity on smart cards used in the payment industry range from 2k bytes to 64k bytes and there are ICCs with even greater storage capacity available. The second factor is the ability to reliably write information back to the ICC on the payment card at the time of the transaction. The third factor is the security provided by the microprocessor embedded in the ICC along with the ability to load applications, not just data onto the ICC. The combination of these factors opened up a wide range of possible approaches toward implementing smart cards payment applications.

Initially there were no standards like the magnetic stripe data standards and so many smart cards were introduced with different operating systems and proprietary payment applications. Essentially everyone was introducing new ways to leverage the computing power, the data storage capacity and the security capabilities of smart cards. The problem with this approach is that every terminal also required a proprietary application in order to interact with the payment application on the smart card. Europay, MasterCard and Visa (EMV) recognized this problem and joined together to build a set of standards that provide a path to leverage the smart card capabilities in the payment industry. Since that time, JCB, Discover and American Express have all joined in to support the EMV standards. As result of the EMV standards, the EMV chip application is now implemented in many different chip operating systems yet terminals are able to communicate to them using the exact same commands.

4.1 EMV

The EMV standard initially started out as a terminal specification and has evolved to contain four books:

- 1) Book 1: The ICC to Terminal Interface specification.
- 2) Book 2: Security and Key Management
- 3) Book 3: Application Specifications
- 4) Book 4: Other Interfaces

When the EMV standards were written, they added support for a significant new capability, a means to authenticate cards offline and thereby significantly reduce the risk of offline transactions. This was a significant development because many countries around the world did not have online transaction processing capabilities and therefore could not perform online authorizations. For this reason, people frequently suggest that EMV is meant for offline transactions environments. However, EMV was designed to provide new security benefits to both online and offline transaction environments.

As with any standard, the EMV standards have evolved over time and continue to evolve. The first release was EMV '96 version 2.0 in 1996 and the second release was version EMV '96 3.1.1 in 1998. In December of 2000, EVM 4.0 was released which is also known as EMV 2000. The current version of EMV is at release 4.2.

4.1.1 EMV Security

At the heart of EMV is the underlying security framework that provides fraud protection for both offline and online transactions. The security is a combination of symmetric and asymmetric key technology.

4.1.1.1 Security and EMV Payment Transactions⁷

EMV improves the security of payment transactions with added functionality in three areas:

- Card authentication – protecting against counterfeit cards and card skimming
- Cardholder verification – authenticating the cardholder and protecting against lost and stolen cards
- Transaction authorization – using issuer-defined rules for authorizing a specific transaction to take place

4.1.1.1.1 Card Authentication Method (CAM)

Card authentication is a security mechanism that protects the payment system against counterfeit cards. These security mechanisms are defined in the Europay MasterCard Visa (EMV) specifications and the associated payment brand chip specifications.

Card authentication can be online, offline or both. Online card authentication typically takes place using symmetric key technology. The card generates a cryptogram using a shared secret key and this cryptogram is validated by the issuer during the online authorization request.

Offline card authentication takes place between the EMV card and EMV terminal. Three methods of offline card authentication method are defined by EMVCo, each one increasing the counterfeit protection that is offered. Offline card authentication approaches are:

- Static data authentication (SDA)
- Dynamic data authentication (DDA),
- Combined dynamic data authentication/application cryptogram generation (CDA)

4.1.1.1.1.1 Static Data Authentication (SDA)

Static data authentication (SDA) means that a cryptogram is calculated using a static public key certificate and static data elements. As of 2009, most cards issued worldwide support SDA. Since the data used for authentication is static, the same data is used over and over again at the start of each transaction. If this data could be skimmed, it could be used to recreate a transaction. In general, SDA helps address card cloning but does not address card skimming.

SDA relies on a public key infrastructure (PKI) where the individual card brands act as the certificate authorities (CA) and provide a public key certificate to any issuer participating in the scheme. During personalization, the issuer signs a set of card-specific data using the issuer private key and loads this signed data, together with the issuer public key certificate, onto the chip card.

In order for a card to be authenticated, terminals are required to load the card brand's public root key. The terminal validates the issuer public key certificate using the card brand root key. After the successful validation of the certificate, the terminal then extracts the issuer public key from the validated certificate. Using the extracted issuer public key, the terminal validates the static card data which has been signed by the issuer. This process is known as static data authentication.

SDA is the simplest method of chip card authentication and therefore provides the lowest level of protection against counterfeit fraud. Although the level of chip counterfeit fraud taking place is currently low, it has the potential to increase as chip markets become more mature and other opportunities for fraud are eliminated. DDA greatly improves the security of chip transactions authorized offline.

⁷ "Card Payments Roadmap in the U.S.: How Will EMV and Contactless Impact the Future Payments Infrastructure?," Smart Card Alliance draft white paper, October 2010

4.1.1.1.1.2 Dynamic Data Authentication (DDA)

DDA means that a unique cryptogram is calculated for each transaction that is performed. In many ways DDA and dCVV or dCVC that are used in online magnetic stripe data (MSD) contactless card transactions achieve the same result. That is, a cryptogram is generated that is unique to a specific card and transaction. DDA protects against card skimming and counterfeiting.

DDA is similar to SDA but goes one step further. In addition to the issuer key pair, an asymmetric (RSA) key pair is generated for each card that is issued. The issuer then creates an associated card public key certificate by signing the card public key, all of which is loaded onto the card during personalization.

In order for a card to be authenticated, terminals follow basically the same process as for SDA, except a random number is also sent to the card to be signed by the card private key. The terminal then validates the signature using the card public key. This technique provides resistance to chip card cloning.

4.1.1.1.1.3 Combined Dynamic Data Authentication/Application Cryptogram Generation (CDA)

CDA combines the DDA function with an additional application cryptogram (AC) at the very end of the transaction. This final AC is used to assure that the data in the transaction maintains integrity even after the transaction is completed. In other words, it prevents a type of fraud where data is manipulated after the host authentication.

4.1.1.1.2 Cardholder Verification Method (CVM)

The cardholder verification method is the method by which the cardholder is authenticated. The chip protects against counterfeiting and authenticates the card, while the personal identification number (PIN) is a common CVM that authenticates the cardholder and protects against lost and stolen cards. EMV supports four types of cardholder verification methods:

- Offline PIN
- Online PIN
- Signature
- No CVM

Depending on payment brand rules and the issuer preference, chip cards are personalized with one or more of the above CVMs so that they can be accepted in as wide a variety of locations as possible. Different terminal types will support different CVMs. Attended POS devices may support online and/or offline PIN, while card activated terminals (CAT) Level 2 devices may support "no CVM."

Offline PIN is the only method of cardholder verification supported by EMV that is not available with magnetic stripe cards. The offline PIN is stored securely on the chip card. During a transaction when the cardholder enters the PIN, the POS terminal sends the PIN to the chip card for verification. The chip card sends the PIN matching result to the POS terminal which can then either approve the transaction offline or send the transaction and PIN verification result online for authorization. The offline PIN is never sent to the host – only the result is passed.

An online PIN, however, is not stored on the chip. Once the cardholder enters the PIN at the POS terminal, the PIN is encrypted by the PIN pad and sent online to the issuer host for validation. Where a card is supporting both online and offline PIN CVMs, the issuer must take proper steps to ensure that the two PINs are synchronized with each other. This is important since when cardholders are being asked to enter a PIN, they do not know if they are entering their offline or online PIN.

For signature CVM, a written signature is required at the POS, as is currently required with magnetic stripe cards. Signature validation occurs when the signature on the receipt is compared to and matches the signature on the back of the card.

For "no CVM," neither a PIN nor a signature is required for the transaction. No CVM would typically be used for low-value transactions or at unattended POS locations.

In general, PIN as a method of cardholder verification is superior to signature and can reduce fraud losses that result from lost, stolen and never-received cards.

It should be noted that online PIN is the only CVM that is valid at ATMs.

4.1.1.1.3 Online and Offline Authorization

EMV transactions may be authorized online or offline. In an online authorization, transactions would proceed as they do today with online transactions using magnetic stripe cards. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction.

In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine if the transaction can be authorized offline. Offline transactions are used with terminals that do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications costs are high.

Cards can be configured to allow both online and offline authorizations, depending on the circumstances. It is also important to note that offline PIN is not exclusively for offline authorized transactions. Offline PIN can take place as the CVM and the transaction can still go online for authorization in the majority of circumstances.

4.1.1.2 EMV Use of Symmetric and Asymmetric Cryptography

EMV uses both symmetric and asymmetric cryptography to protect cards and transactions.

First, EMV leverages the security found in integrated circuit cards (ICCs) and requires symmetric authentication keys to be submitted to gain access to the ICC memory. This helps protect cards in transit to issuers and in warehouse inventory. Protecting card stock is an important deterrent against the creation of authentic-looking counterfeit cards.

Second is the EMV application logical security. For this, EMV specifies special purpose symmetric access keys for personalization, for post-issuance updates and for card and transaction authentication purposes. These keys help:

- 1) Prevent unauthorized personalization of cards,
- 2) Secure transmission of card updates once they are in the cardholders' hands by encrypting all data that is to be sent to a card,
- 3) Authenticate a card and authorization request in an online transaction by validating an Authorization ReQuest Cryptogram (ARQC), and
- 4) Authenticate the issuer by the card validating the Authorization ResPonse Cryptogram (ARPC).

For the symmetric key security to work, the issuer host system and the card must share each of the secret keys that are to be used. The keys are loaded onto the card during the personalization process and also placed in the hardware security module (HSM) used by the issuer's host authorization system. Data can then be encrypted or signed to create a cryptogram and decrypted, or a cryptogram validated, on the other side. For low-cost, always online transaction environments, online validation of the ARQC alone provides sufficient transaction security.

Finally asymmetric keys and certificates, also known as public key infrastructure (PKI), are incorporated to facilitate card authentication in offline transaction environments. At a high level, the following describes how the EMV PKI certificates work. Before an issuer can begin issuing EMV cards, they must obtain an issuer's public key certificate from the payment brand's certificate authority (CA). This issuer's public key certificate then is loaded onto each card that is issued and, at the time of the transaction, the terminal authenticates the card's certificate. The authentication is done by validating the issuer's public key certificate using the corresponding CA public key that is loaded onto the terminals by the payment

brands. The public key that is loaded to the terminals is the “partner” key of the private key that the payment brand used to sign the issuer’s public key certificate. This process enables card authentication without online connectivity.

Issuers are provided three certificate implementation options for card authentication – SDA, DDA and CDA – as described above. Each offers a different level of security based on how the certificate is generated.

It is important to recognize that the offline security features described above, SDA, DDA and CDA, are not needed or required for online EMV transactions. However, these features can enhance the card validation process and typically one of them is applied. In some parts of the world, the adoption of DDA is encouraged.

4.1.2 EMV Transaction Flow

EMV changed the basic risk management workflow while leveraging all of the existing steps in the magnetic stripe card process presented in Section 3.1 of this document. With magnetic stripe cards, all risk management is performed during the transaction authorization process by a central system. The terminal simply serves the purpose of capturing the Track 1 or 2 data and passing it through to the central server.

With EMV, components of the risk assessment are pushed out to the terminal and the card. This is what facilitates greater risk management for offline transactions. In essence, the issuer loads a set of risk management parameters into the EMV application on the chip and the terminal responds by performing each of the functions indicated by those risk parameters. The risk parameters range from the cardholder verification method (i.e., requirement for a signature or PIN), to the form of cryptogram that is used for the card and terminal to perform an authentication routine.

Other risk parameters address what the terminal should do under different authorization failure conditions or how a card can be used.

Figure 4 shows a partial list of other EMV data that is stored in the EMV application on the chip. The data is frequently referred to as an EMV tag. The second column is the tag that the applications use to identify the data sets. After each tag is the value that is associated with the tag.

Description	Tag	Value
Application Currency Code	9F42	840 [US Dollar]
Application Currency Code VIS	9F51	
Application Currency Exponent	9F44	
Application Default Action	9F52	00 00
Application Discretionary Data	9F05	
Application Effective Date	5F25	95 07 01
Application Expiration Date	5F24	10 12 31
Application Identifier - Card	A0	00 00 00 00 03 10 ...
Application Interchange Profile	82	7C 00
Application Label	50	VISA CREDIT
Application Preferred Name	9F12	CREDITO DE VISA
Application Primary Account Number	5A	4761-----0010
Application Primary Account Number Sequence Nu...	5F34	1
Application Priority Indicator	87	01
Application Transaction Counter	9F36	1
Application Usage Control	9F07	FF 00
Application Version Number (ICC)	9F08	140
Card Production Life Cycle History File Identifiers	9F7F	40 70 85 09 40 51 ...
Card Risk Management Data Object List 1	8C	9F 02 06 9F 03 06 ...
Card Risk Management Data Object List 2	8D	8A 02 9F 02 06 9F ...
Cardholder Name	5F20	Visa_VSDC_DDA
Cardholder Name Extended	9F0B	
Cardholder Verification Method List	8E	00 00 00 00 00 00 ...
Consecutive Transaction Counter (International C...		
Consecutive Transaction Counter (International)		
Consecutive Transaction Limit (International Coun...	9F72	
Consecutive Transaction Limit (International)	9F53	
Cryptogram Version Number		10
Cumulative Total Transaction Amount		
Cumulative Total Transaction Amount (Dual Curre...		
Cumulative Total Transaction Amount Limit	9F54	
Cumulative Total Transaction Amount Limit (Dual ...	9F75	
Cumulative Total Transaction Amount Upper Limit	9F5C	
Currency Conversion Factor	9F73	
Dedicated File Name	84	A0 00 00 00 03 10 10
Derivation Key Index		01

Figure 4. Examples of other EMV Data Stored in the EMV Chip

Many of the EMV tags in the Figure 4 have numerous sub-configuration options. For example, Figure 5 shows the list of options within the EMV tag 9F07 – Application Usage Control.

Application Usage Control
Valid for domestic cash transactions
Valid for international cash transactions
Valid for domestic goods
Valid for international goods
Valid for domestic services
Valid for international services
Valid at ATMs
Valid at terminals other than ATMs
Domestic cashback allowed
International cashback allowed

Figure 5. Example of EMV Options

When the EMV card is inserted into the terminal, the terminal finds the EMV application and reads the EMV tags to get directions for handling the transaction. Both the terminal and the card perform an assessment to determine if the card should be declined, if the transaction should go online or if it can be accepted as an offline transaction. If it is determined that the transaction requires an online authorization, a cryptogram referred to as an ARQC (Authorization Request Cryptogram) is sent to the host system for final card and authorization validation. In response, the host calculates an ARPC and sends it back to the terminal to validate the issuer.

4.1.3 EMV Infrastructure Requirements

To leverage the full security of the EMV application placed on a smart card changes to all of the major infrastructure components – the card, terminal, acquiring system and host authorization system – are required. Sections 4.1.1 and 4.1.2 presented many of the changes to the card and the new authentication capabilities. In this section we will address the corresponding changes required for each of the other infrastructure components.

4.1.3.1 Terminal Changes

The point of acceptance, or the terminal, is the first component that requires changes. In particular there is a need to have a smart card reader added to the terminal and to have the hardware components certified by EMVCo. This is referred to as an EMVCo Level 1 Certification. In addition, the new decision process that is conducted between the card and the terminal to perform both the card and terminal authentication process and the risk management assessment must be programmed into the terminal. The EMV functions that are required on the terminal are frequently referred to as the EMV kernel. At a high level, Figure 6 shows the steps that are followed by the terminal software in an EMV transaction.

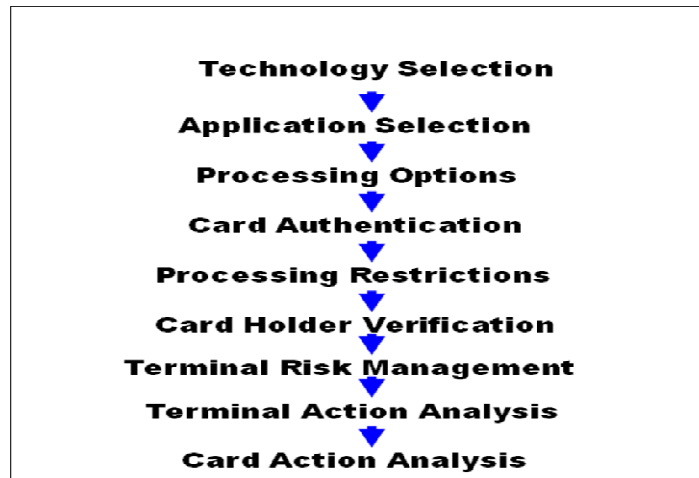


Figure 6. Steps Followed by Terminal Software in an EMV Transaction

In addition to the internal transaction logic, EMV and each of the payment brands may have terminal prompt and receipt printing requirements. Finally the terminal must package the EMV cryptogram that is sent to the host for authentication and the EMV data elements shown in Figure 7 in the transaction data.

Data Element
Application Interchange Profile * 12
Application Transaction Counter *
ARQC *
CID
CVM Results
IFD Serial Number
Issuer Application Data *
Terminal Capabilities
Terminal Type
TVR *
Unpredictable Number*

Figure 7. EMV Transaction Data Elements

These changes in the terminal application are frequently referred to as Level 2 application changes by EMVCo and EMVCo has defined a specific set of tests that terminals must pass to obtain EMV certification. These tests are referred to as EMV Level 2 Certification tests.

In summary, two new certifications are required before a terminal can be certified to be EMV-compliant. The Level 1 certification certifies the hardware-level smart card reader compliance and Level 2 certification certifies the EMV kernel (software) functionality of the terminal. EMV compliance tests must be performed at an EMVCo approved test lab. In addition to the EMVCo certifications, terminals must also pass tests in order to be certified by specific payment brands before they can be installed at

merchant locations. In this case, a payment brand is defined as a Visa, MasterCard, American Express or other independent payment scheme.

4.1.3.2 Acquiring System Changes

In the payment system infrastructure transaction flow, the acquirer performs the function of interfacing to merchant terminals and switching the transactions to the appropriate authorization system. This is an oversimplification of all the functions performed by the acquirer but is the function most pertinent to the EMV changes. The acquirers are also responsible for implementing terminals and terminal changes to large numbers of merchants.

For the new EMV message data to get passed through to the issuer authorization systems, they must pass through the acquirer systems. As a result, the acquirers typically need to get the terminal certifications from the payment brands and perform internal tests before they rollout the new terminals. For Visa the tests are referred to as ADVT tests and for MasterCard they are referred to as TIP testing.

Part of the changes to acquirers' systems is mapping the terminal transaction data to the format that the issuer needs so that they can receive the data through the Visa and MasterCard networks and perform the authorization and EMV cryptogram validation. In summary, the acquirer does not use the EMV data but performs data transformation and network switching functions to connect the card transaction to the appropriate issuer authorization system. The data that is used in the EMV authorization is typically placed in Field 55 of the ISO/IEC 8583 authorization message.

4.1.3.3 Issuing System Changes

Issuers have a number of areas to change because preparing for EMV card issuance must be approached from a product perspective. This means that there are implications on the promotion material, the customer service systems, the cardholder system, the authorization system and the card issuance process. From a minimalist perspective, the card issuing system and the authorization system require changes.

The issuing system can be augmented by EMV key management, data preparation and personalization system that can take a standard emboss file used for issuing magnetic stripe cards and add the information required to issue EMV cards. The implementation of such a system can be anywhere from two to six months.

On the authorization system, issuers need to add the support of a Hardware Security Module (HSM) to perform the EMV cryptogram (ARQC) validation and send back to the terminal an Authorization ResPonse Cryptogram (ARPC) and to store the other EMV data elements that are passed in Field 55 of the authorization message.

To leverage the ability to change the data on the chip after it is issued, issuers also need to add the ability to generate EMV scripts and place them in the authorization file. EMV scripts are simply chip commands for updating data in the chip EMV application. These commands are then passed back to the terminal and submitted to the card.

4.1.3.4 EMV Migration and Infrastructure

In summary, EMV migration is a system migration. The new application and capability on the chip must work in conjunction with the terminals, the acquiring systems and the issuer host authorization system in order to leverage the full advantage of EMV.

In many cases, if not most, the changes of all components do not get completed at the same time. Early on in the EMV migration in other countries, many issuers implemented a partial grade EMV implementation. This basically means that they implemented the cards and terminals, but the host systems had not completed the EMV updates. As a result, they leveraged the new offline authentication functions and began addressing the card cloning issues.

However, a partial grade EMV implementation loses possibly the most powerful component of EMV authentication which is the cryptogram validation between the card and the issuer host system. If an SDA card were copied, it could be used in offline transactions without being caught or stopped. However, as soon as an online transaction is performed, the cryptogram authentication would fail and cause the transaction to be rejected. For this reason the payment brands discourage this type of partial EMV implementation.

4.2 Contactless Credit/Debit Payment

Contactless payment has had the fastest deployment and acceptance of any emerging payments technology in recent memory and speaks of a unique market momentum for the industry. Contactless payment is being delivered around the world by the payment brands and their issuing and merchant customers by leveraging the existing payment card infrastructure as its basis for implementation. Since mid-2005, leading financial issuers around the world have placed tens of millions of contactless credit and debit cards and devices into the hands of consumers worldwide. Merchant acceptance has also increased dramatically over the past 3 years: over 246,000 merchant locations⁸ worldwide now accept contactless payments.

Contactless payments are simply payment transactions that require no physical contact between the consumer payment device and the physical point-of-sale (POS) terminal. In a contactless payment transaction, the consumer holds the contactless card or device in close proximity (less than 2-4 inches) to the merchant POS terminal and the payment account information is communicated wirelessly (via radio frequency (RF)).

This section reviews "branded" contactless payments with credit and debit cards, using payment products from American Express®, Discover® Network, MasterCard, and Visa.

Contactless payments are currently supported by multiple card issuers and financial service providers. American Express, Discover Network, MasterCard, and Visa all have contactless payment products (ExpressPay from American Express®, Discover® Network ZipSM, MasterCard® PayPassTM and Visa payWaveTM, respectively). These products rely on ISO/IEC 14443-based technology, ensuring payment solution compatibility regardless of brand or payment device when used with contactless readers that have been approved by the payment brands.

The initial introduction of contactless financial payment devices focused on markets that had lower value transactions (less than \$25), where consumers used cash for payment, and where transaction speed and customer convenience were critical. Contactless payments made quick progress in many merchant segments including quick service restaurants, convenience stores, pharmacies, theaters, and sports venues. Contactless payments have expanded beyond these initial merchant segments, however, moving into other traditional retail segments (e.g., office supplies, specialty retailers, grocery stores), and opening up credit card acceptance in new merchant categories (e.g., taxis, vending machines, transit fare payment).

It is important to note that the approach to contactless credit and debit payment differs in the U.S. and in countries implementing EMV.

4.2.1 EMV Contactless

EMV contactless closely follows the EMV standards for authentication and authorization. An EMV contactless solution may support both offline authentication and offline authorization using techniques such as SDA or DDA. In addition the EMV solution makes use of strong online authentication based on EMV standard cryptograms. Support for the EMV cryptogram requires a network change to carry the additional data required for online authentication.

⁸ MasterCard, http://www.paypass.com/performance_insights.html.

The primary market driver for the adoption of contactless EMV has been the ability to extend bank card payment into the micropayments transaction space. To do so requires a faster and more convenient transaction flow compared to the standard contact EMV card. The initial implementations of contactless EMV included most, if not all, of the functionality of contact EMV. However, this required the card to stay within the terminal contactless field to complete the standard EMV transaction process. This proved to be too time consuming.

As a result, multiple variations of contactless EMV have evolved over the past five years. Each iteration has striven for a balance among security and risk management options, transaction speed and convenience. As a result, the transaction flow for each of the payment brands varies. The flow varies according to the extent of EMV risk management functions and type of authentication cryptogram that is implemented in the contactless application. For example, one version of contactless EMV implements a standard EMV CDA application cryptogram while another version implements a unique version of a DDA application cryptogram referred to as fDDA. In each case, the transaction flow varies.

The multiple independent contactless EMV kernels required POS terminals to be approved by each payment brand. EMVCo recognized the need for standardization and developed the common contactless terminal roadmap. In Phase 1, EMVCo is creating a combined set of terminal specifications from the existing four payment brands' specifications and will manage the testing and approval of the contactless kernels according to these specifications. In Phase 2, EMVCo will create a common contactless online-only kernel and, in Phase 3, EMVCo will address the offline market.⁹

Contactless EMV transactions are designed to function in both offline and online transaction environments and they all leverage the EMV cryptogram security function to validate the authenticity of the card and the transaction. This prevents card cloning and replay fraud. Given that one of the primary goals for contactless EMV is to capture micropayment transactions, DDA and CDA authentication is required. Contactless EMV applications also provide the ability to leverage the EMV velocity counters to limit the number or dollar value of consecutive offline transactions.

4.2.2 Contactless Credit/Debit Payment in the U.S.¹⁰

The U.S. led the way with contactless credit and debit payments, with issuance starting in 2005.

In the U.S., the payment brands implemented contactless payment transactions to leverage the existing magnetic stripe payments infrastructure and minimize the impact on the merchant and the acquirer network messaging. This approach, called contactless MSD (magnetic stripe data), facilitated straightforward contactless payment implementations by issuers, merchants and payment processors and faster consumer adoption and merchant acceptance.

With contactless MSD, the message layout for Track 1 and Track magnetic stripe data remained intact, with one notable difference. The chip on the card allowed for the calculation of a dynamic card verification value based on a card-unique key and a simple application transaction counter. The dynamic card verification value significantly enhanced the security of the transaction and was passed in the message in the same field that was used for the original card verification value. The automatic transaction counter (ATC) was passed in the area reserved on the track layout for issuer discretionary data. Contactless MSD does not support offline authentication or offline authorization.

The use of dynamic data in the transaction added security to the payment process by preventing replay attacks (no transaction can be done twice) and card cloning or skimming (the card key never leaves the protection of the smart card memory).

The current generation of contactless cards being issued in the U.S. are based on the EMV standards and utilize the constructs of a contact EMV card to pass an EMV-compatible cryptogram to the issuer with the authorization request.

⁹ "EMVCo Common Contactless Terminal Roadmap," EMVCo General Bulletin No. 43, First Edition, November 2009

¹⁰ Sources: Smart Card Alliance white papers.

Section 8.1 includes additional detail about the U.S. contactless payments transaction flow.

4.2.3 Contactless Benefits

4.2.3.1 Consumer Benefits

Industry surveys have shown that consumers value the benefits of contactless payments.¹¹ Consumers appreciate the speed of contactless payment and enjoy the convenience and “coolness” factor offered by the various new contactless payment form factors, such as key fobs and mobile phones. Contactless payments are easy to use—consumers simply place the device in close proximity to the reader. They need not worry about having enough cash or fumbling for cash in a purse or wallet. In addition, new acceptance locations allow consumers to use their contactless devices for purchases that previously required cash—in taxis, at vending machines, and on subways and buses.

Another advantage for consumers is that they control the contactless payment device. The device is always in the consumer’s possession, reducing the possibility of leaving it somewhere accidentally and minimizing the potential for fraud. In addition, the transaction uses dynamic data, providing additional protection against fraudulent misuse of contactless data.

4.2.3.2 Merchant Benefits

Merchants who accept contactless payments realize advantages in several areas. First, contactless payments are faster and more convenient for consumers than cash or magnetic stripe card payments. Studies have shown that contactless payments reduce customer time at the POS by 30%–40%.¹² A recent Visa study compared the speed of cash, magnetic stripe “swipe” and contactless transactions at merchants accepting Visa payWave in Columbus, OH. With uniform usage (no signature/PIN) across 465 transactions, the study found that contactless transactions were 4.5 seconds faster than cash and 3 seconds faster than swipe.¹³

Increased speed and convenience generate greater sales volumes and increase customer spending. Customers spend about 20%–30% more when using contactless payment devices than when they use cash.¹⁴

Customers not only spend more: the use of contactless payments also reduces the requirement for and cost of handling cash while also improving operational efficiencies and reducing terminal maintenance costs.

Contactless payments present merchants with a tailor-made opportunity for clear differentiation and competitive advantage. Being able to offer “the latest thing” puts merchants in an excellent position to offer closed-loop products (such as gift cards) that strengthen customer loyalties and increase brand awareness. The variety of form factors in which contactless payment devices can be available also supports differentiation. Merchants and issuers can collaborate on payment products that blend specific features and packaging (cards, tokens, mobile phones) and target different customer segments that have very particular requirements for the shopping experience.

Merchants who accept contactless payments are also prepared for what is expected to be the next payment revolution – NFC-enabled proximity mobile payments. The contactless POS readers being put in place to accept payment from current branded contactless credit and debit cards are able to accept payment from the same brands without additional modifications when consumers use NFC-enabled mobile phones.

¹¹ Smart Card Alliance, <http://www.smartcardalliance.org/articles/2008/09/17/contactless-payment-try-it-youll-like-it>

¹² Source: Chase

¹³ *Contactless & Mobile Payments*, Sandy Thaw, Visa presentation, 2009 Payments Councils Summit, February 24, 2009

¹⁴ Source: Chase

4.2.3.3 Issuer Benefits

Contactless credit and debit cards provide issuers with the opportunity to increase cardholder usage in cash-heavy and small-ticket payment environments by making the payment experience faster and easier. Issuers see an increase in transactions in everyday spend categories with merchants who don't typically accept credit and debit cards.

In addition, the consumer's contactless payment card moves to "top of wallet." Consumers spend more (28%-42% more)¹⁵ and use the card more frequently, driving incremental transactions and revenue to issuers. Issuers also report better customer retention, as cardholders increase their rewards by increasing daily use of the card for small value purchases.

Another benefit is that issuers can differentiate their products with innovative new form factors, tailored to specific consumer preferences (for example, key fobs, mobile devices, micro tags, or stickers), and provide products and services that take advantage of the functionality available with the new form factors. Issuers also see the potential for multi-application cards that include credit/debit payment and applications such as transit fare payment, campus or corporate ID, and loyalty/rewards programs.

Contactless payments technology provides issuers and merchants with a platform for enhanced security and authentication. The current generation cards use technology based on the global EMV payments standards to generate a dynamic cryptogram with every transaction, providing both better information for authorization decisions and tools to reduce fraud resulting from counterfeit cards.

Published metrics from payment brands on issuer benefits are summarized in Table 1.

Table 1. Published Metrics on Issuer Benefits

Issuer Benefit	MasterCard ¹⁶	Visa ¹⁷
Cardholder Spending	<ul style="list-style-type: none"> Cardholders spend more with their <i>PayPass</i> card¹⁸ – Increased overall usage of 36% per <i>PayPass</i> account. Taking the effect of reactivation into account in the issuer case studies analyzed, increases grew between 28%-42%. 	Statistics not available
Cardholder Use	<ul style="list-style-type: none"> Cardholders use their <i>PayPass</i> card more often – Increased transaction frequency per account by 32%. Taking the effect of reactivation into account in the issuer case studies analyzed, increases grew between 33%-52%. Cardholders use <i>PayPass</i> for smaller purchases – Average ticket for <i>PayPass</i> transactions is just over \$37. Approximately 56% and 79% are for purchases of \$25 and \$50 or less respectively, a sign that <i>PayPass</i> is increasingly displacing cash. Cardholders use <i>PayPass</i> at merchants that mostly accept cash – <i>Consumers</i> 	<ul style="list-style-type: none"> Usage is strong and frequent: 58% of Visa cardholders use their card most of the time when it is accepted. 52% with Visa <i>payWave</i> have made a transaction in the past week. Much of the contactless usage replaces cash and check payments, especially in merchant categories where card payments were less common: 43% at fast food outlets Many use their card more often than they did before it was contactless enabled. 42% of Visa

¹⁵ http://www.paypass.com/performance_insights.html

¹⁶ MasterCard *PayPass* Performance Insights, June 2010 (http://www.paypass.com/performance_insights.html)

¹⁷ *Contactless & Mobile Payments*, Sandy Thaw, Visa presentation, 2009 Payments Councils Summit, February 24, 2000 (from C&R Research Awareness & Usage survey, September 2007)

¹⁸ MasterCard *PayPass* Performance Insights, June 2010.

Issuer Benefit	MasterCard ¹⁶	Visa ¹⁷
	<p><i>card volume grows because purchases are no longer limited to cash on hand.</i></p> <ul style="list-style-type: none"> More than 70% (77%) of <i>PayPass</i> cardholders say that their <i>PayPass</i> enabled card is the primary card they use.¹⁹ 	<p>cardholders use their cards either 'much' or 'somewhat' more often than before. 45% of Visa cardholders use their cards either 'much' or 'somewhat' more often for transactions under \$25.</p>
Cardholder Activation	<ul style="list-style-type: none"> <i>PayPass</i> is a proven tool to convert inactive accounts. In one issuer case study, for example, 15% of active "tappers" were previously inactive. 	Statistics not available

4.2.3.4 Industry-wide Benefits

The payments industry as a whole benefits from the reduction of fraud that results from the implementation of contactless payments. Features such as dynamic data generation and verification reduce the possibility of skimming and merchant server attacks. Every additional contactless transaction reduces the possibility of fraud.

4.2.4 Developments in Contactless Payments

Contactless payments have opened up new opportunities for issuers and merchants that take the consumer payment device into new markets and applications.

- Contactless technology can be issued in many form factors. Key fobs, mini-cards and stickers are now being issued, providing increased convenience to consumers.
- Contactless implementation uses EMV contactless specifications for creating dynamic cryptograms with every transaction. The combination of smart chip technology, which is tamper-resistant and virtually impossible to counterfeit, and the dynamic cryptogram, which makes every transaction unique, addresses the growing fraud problem of counterfeit cards.
- The smart chip used in contactless credit and debit cards has the ability to support multiple applications (for example, payment and loyalty, or credit payment and transit payment).
- The contactless payments merchant acceptance infrastructure that is being put in place is able to accept transactions both from branded contactless payment and from branded payment applications on Near Field Communication (NFC)-enabled mobile phones. Additional information about NFC can be found in Module 6, Section 6.

¹⁹ *PayPass Update: MasterCard PayPass Consumer Benchmark Survey, 2008*, Burt Wilhelm presentation, 2009 Payments Councils Summit, February 25, 2009

5 E-purse and Stored Value Cards

Electronic purses (e-purses) are available in very different types and forms. All have the common objective of creating electronic cash (e-cash) to free the customer and the merchant from needing to manipulate physical cash for small value purchases. The payment transaction is electronic but instead of having the money come from a debit or credit account, the funds come from an amount of cash the customer has already reserved for such payments. Systems vary based on where the money (or value) is stored and how universal it is (in terms of buying power). Systems also have very different security risks to address (e.g., fraudulent creation of cash, loss of cash, anonymity of users).

Electronic purse systems can be classified based on where the cash reserve is held and managed, either:

- On a central server, or
- On a card

Systems can also be classified based on the type of merchant that accepts the electronic purse for purchases.

- A closed system will have only one merchant accepting the e-cash (or value) stored in the e-purse
- An open system is when all merchants accept the same e-cash payment mode, allowing a consumer to use a single stored value card or e-purse in a variety of locations for a broad range of purchases.²⁰

Closed system stored value cards are also known as prepaid cards. Example implementations of closed system stored value cards include: mass transit fare payment cards, college or corporate campus cards, telephone company prepaid cards.²¹

This section will discuss four different types of electronic purse implementations:

- Open system with central account management of operations
- Open system with no central account management of operations
- Closed system with semi-offline e-purse usage (e.g., prepaid account with balance in a smart card)
- Closed system with online centrally managed accounts (i.e., prepaid online)

Table 2 shows examples of open and closed e-purse systems.

Table 2. Examples of Open and Closed E-Purse Systems

Open E-purse Systems	Closed E-Purse Systems
<ul style="list-style-type: none">• Chipknip, Belgium and Netherlands• Danmont, Denmark• Edy, Japan• GeldKarte, Germany• Mondex• Moneo, France• NETS Cash Card, Singapore• Proton• Quick, Austria• Visa Cash	<ul style="list-style-type: none">• French prepaid telephone cards• Hong Kong Octopus Card• London Oyster Card• Parking e-purses• San Francisco Bay Area Clipper card• Store-branded prepaid cards• Washington, DC SmarTrip card

²⁰ *The Electronic Purse*, by John Wenninger and David Laster, Federal Reserve Bank of New York, April 1995

²¹ Ibid.

5.1 Open System with E-cash Value on the Card and Central Account Management

An open e-purse system that is able to work in a semi-offline environment and that uses a central account management system includes the following participants, or actors:

- Customers (or end users), who have smart cards which contain electronic funds (the e-purse).
- Merchants, or service providers, who are equipped with POS terminals able to accept the e-purse smart cards for small value purchase transactions. The terminals accept purchases and deduct the purchase value from the e-purse in the smart card without being online.
- The e-purse central account management system, which manages the transactions and the fund pool (the cash which was prepaid by the customers but not yet spent). This fund pool receives hard money (either cash or funds from a credit or debit card) from the customer and transfers an electronic representation of this money into the e-purse in the smart card. This fund also provides payments to the merchants.
- Banks. For legal reasons (i.e., laws related to printing, handling and managing money), many countries, including the United States, require banks to be involved in such an open e-purse system, on the customer side, merchant side, or both.

In this architecture, all transactions are accounted for (though some systems may aggregate the transactions) and the e-purse account is settled periodically (e.g., once per day, or once per week) by the central system. The smart card acts as if it is a purse containing cash, which can be used anywhere, at any merchant accepting cash (assuming ubiquitous acceptance locations for the e-purse approach). The terminals may send the transactions to the central system in real-time, but they primarily use batch mode (connecting to the central system or using portable memory devices to unload the value).

If a card is lost or stolen, the system can quickly block the card use (based on the settlement cycle) and the customer may not lose all of the e-cash stored in the card. According to the system's financial rules, the customer would have the value that was on the card when it was blocked restored to the card. (The settlement process enables the system to know how much money was available on a card after all accepted transactions were settled.)

By design, the system does not provide any anonymity for customer purchases and appears to work like a debit card (or a gift card) from the user's stand point (without having to present a PIN for transactions under a certain amount).

The main difference from a debit card system is that the funds are first maintained in the card and then verified in the back-end system. The e-purse system also has the ability to work with offline terminals since the card keeps track of the amount of money available in the account. Such a system is primarily suitable for countries (or situations) where online telecommunications are costly or unreliable for low value transactions. E-purse cards may include counters that would force the card to go online at some point for security purposes or to synchronize the balance.

The cost of running this type of system can be very expensive if all transactions must be accounted for, since this requires a lot of processing in the back end. The system also requires that the keys are maintained at various levels: in cards to sign the transactions; in the merchant's terminal to authenticate the card. This key management, when done properly, can be an important part of the system's cost of operation.

The largest implementation of such a model was done in Denmark (known as the Danmont e-purse) and was phased out in December 2005.

The Comité de Européen Normalisation (CEN) produced a European standard, EN 1546, for inter-sector electronic purse systems. The Danmont e-purse and Austria Quick e-purse were both based on this standard.

The international standard, Common Electronic Purse Specification (CEPS)²², was developed by Visa in the early 2000s; essential features of CEPS were based on the EN 1546 standard.²³ The CEPS specification has had little adoption around the world as a universal e-purse. Nevertheless, the specification can be used in closed systems (see Sections 5.3 and 5.4) and can be very useful in defining the functional requirements for security application modules (SAMs) protecting the application keys in the terminal.

Another commercial e-purse system specification is Proton, published by Proton World. The Belgian and Netherlands Chipknip e-purse and Swiss and Swedish "Cash" e-purses use the Proton specification.²⁴

Figure 8 illustrates an open e-purse architecture.

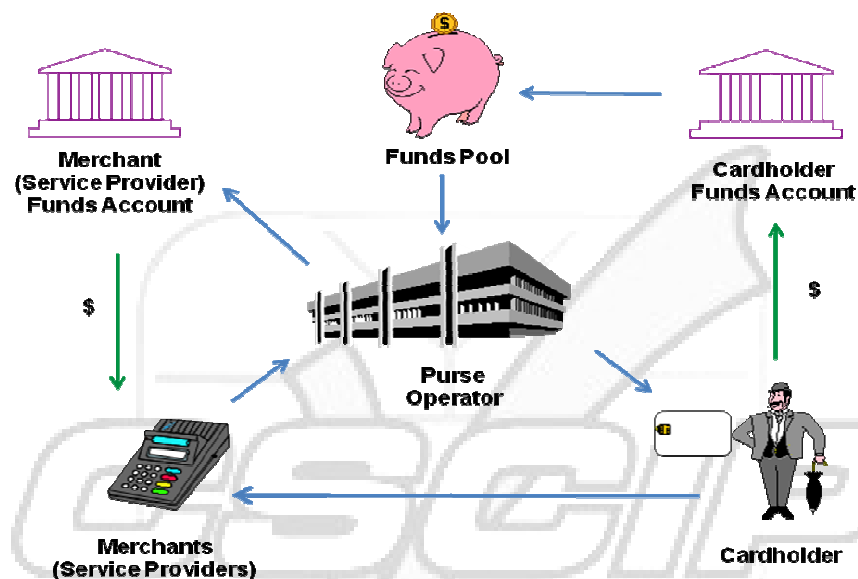


Figure 8. Open Electronic Purse System Architecture.

5.2 Open System with No Central Account Management

An implementation of an open system with no central account management was developed by Mondex (a consortium of companies), using the smart card MULTOS operating system. Based on public key technology, this system architecture allowed each card to authenticate any other card of the system, enabling transfer of electronic money from one card to another without a terminal being involved in any secure operation.

In this architecture, the actors are:

- Customers (or end users), who have smart cards which contain electronic funds (the e-purse).
- Merchants, or service providers, who are equipped with a merchant card using the same e-purse as the customers and able to accept the e-purse smart cards for small value purchase transactions. The merchant (or any customer willing to accept cash in payment) needs to also have a terminal that can facilitate communication between two cards in order to exchange cash.

²² The CEPS specifications can be found at <http://www.irisa.fr/vertecs/Equipe/Rusu/FME02/functionalrequirements6-3.pdf>

²³ *Smart Card Handbook*, Wolfgang Rankl and Wolfgang Effing, Fourth Edition, John Wiley and Sons, Ltd., 2010, p. 760

²⁴ Rankl, p. 775

In theory, no transaction is used for the settlement, but some implementations allow transactions to be created by terminals for audit and journaling purpose.

- The central e-purse system, which only manages the funds pool (i.e., real cash that is converted into e-cash and e-cash that is converted to real currency) and some transaction auditing and reconciliation functions.
- Banks. For legal reasons (i.e., laws related to printing, handling and managing money), many countries, including the United States, require banks to be involved on the customer side, merchant side, or both. In some countries, this approach is not even allowed since it could be used to launder money or create false money if the system security is breached.

In this model, the merchants are paid directly by the customer's card and are able to use the cash they receive immediately to make payments or to deposit the funds into a bank account. This system has no simple reconciliation of accounts. The system does not know the exact amount of money in a given card since all transactions are not reported. Since the cash in a card is not known, users typically cannot recover the funds when a card is lost or broken. Some countries have expressed concerns about this architecture being used by money laundering organizations. Another major concern is that criminals could determine how to hack cards and add funds into the system; the lack of a simple reconciliation function would make this type of fraud hard to trace.

5.3 Closed System with Semi-Offline Account Management

The most widely used application of smart card e-purses around the world is implemented as a closed system with semi-offline account management. This architecture is the same as the open system with e-cash on the card and central account management, but use is limited to a given area, service, or group of merchants and does not involve as many players. (Thus, the term "closed" is used since as the e-cash cannot be used for all services for all merchants.) Initially used by telephone companies for prepaid cards (mainly in France and Germany), many transport systems all around the world are now using this model. The e-cash in the card allows the user to pay for transportation (or parking) related services, or for various services in a given city or on a given campus.

In this type of system, one "merchant" provides various services (e.g., parking, subway ride, bus ride) and the prepaid funds cannot be used to purchase services from any provider that is not part of the "closed" system. The generic architecture for this approach is less complex since the need for a financial partner is much more limited. The "money" stored on the cards is not really e-cash, but pre-paid funds for specific services and no more. Another name for the funds could be "local money" (as with a store gift card), which presents more limited fraud risk on many levels. The system does not require reconciliation among merchants and the funds pool is directly administered by the service provider (or its bank if a financial institution involved).

From the user's standpoint, the system's behavior is similar to a closed system with centrally managed accounts (described in the next section), as long as transaction processing is fast and reliable. Because the funds in the system are not equivalent to cash, fraud risk is more limited and the system does not provide a high level of return on investment for a hacker. (However, this does not prevent negative reporting if a hacker finds a weak point to attack the system.) Many systems are built on this model where the card contains an amount of prepaid cash. This approach also allows the system to be able to work in offline, when the network goes down or when infrastructure costs justify offline operation. Examples of closed systems with semi-offline account management include: Washington, DC SmarTrip card, London Oyster Card, San Francisco Bay Area Clipper card, Hong Kong Octopus Card, French prepaid telephone cards. Figure 9 illustrates a closed e-purse system architecture.

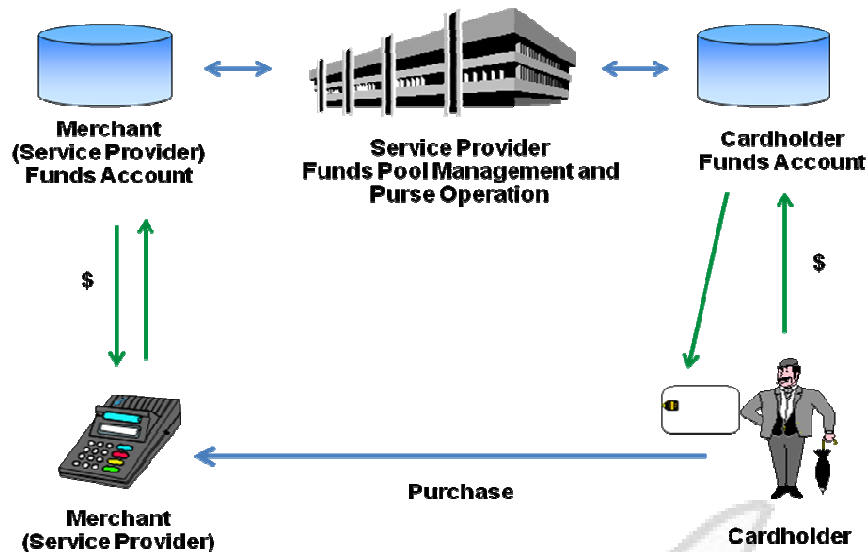


Figure 9. Closed Electronic Purse System Architecture

5.4 Closed System with Online Central Account Management (Prepaid Online)

A closed system with online central account management generally does not use smart cards since all of the security is provided by the central system. An example of this type of system is a store gift card. The gift card has a unique number, and when activated, the card provides access to an online account (maintained by the store) which manages the funds that have been prepaid into the account. Another example of this type of system is EZ-Pass, which is used for toll payment throughout the U.S. East Coast.

With this type of system, the customer prepays a certain amount of money; this allows the cardholder (who may not be the customer who paid for the account) to buy a given service, up to the amount secured in the account pointed to by the card. When the account is empty, new funds can be deposited in the account or the account holder may have agreed to have automatically refill the account from another type of financial account (e.g., credit card, bank account).

This system does not require a lot of card-level security, since all the verifications are made in real-time in the central system. Most systems use non-intelligent cards, such as magnetic stripe cards. The customer assumes most of the risk in this system. If the card is lost or stolen, or if anyone is able to create a counterfeit card pointing to the account, the funds can be used until the customer indicates to the central system that the card number should be blocked.

Debit cards are a variation of this type of scheme, since they are also payment instruments that access a pre-funded account. Debit cards, however, often require customers to enter a PIN to prove that they are the legitimate account holder.

Prepaid, closed, centrally-managed e-purses are quite common and are often used by transit authorities for parking or transit fares, or by libraries for copies or Internet access. The cards are often quite simple and have little or no security or some proprietary protection.

The fraud risks for this type of system are rather low, since the system is able to verify every transaction at the time it happens. The system will immediately accept or deny the purchase (as with debit or credit payment systems), and will not allow purchases beyond the amount of funds that are deposited in the account.

6 Transportation and Parking Payment

6.1 Transit

Mass transit agencies worldwide have been using stored value prepaid cards for electronic ticketing since the 1970s. Through the late 1990s, this market steadily began transitioning from magnetic stripe technology to contactless smart cards. Today, virtually all transit fare payment systems in the delivery and procurement stages use contactless smart cards as the primary ticket medium. Major deployments are operational in cities around the world, including London, Hong Kong, Seoul, Tokyo, Washington, D.C., and Shanghai.

6.1.1 Transit Smart Card Implementations

Table 3 shows examples of contactless smart card use by international transit programs and Table 4 includes examples of U.S. transit agencies using contactless smart cards.

Table 3. Examples of Smart Card Use by International Transit Programs.²⁵

Program Name/Location	Type of Program	Status
EZ-Link (Singapore) ²⁶	Electronic payment system used for multi-modal transportation payment and retail payment	Over 10 million cards in circulation, with 4 million transactions per day. The EZ-Link card now complies with the Singapore standard, Contactless E-Purse Application (CEPAS). ²⁷
Leon, Mexico ²⁸	AFC for bus fare payment	Over 400,000 cards
Lokaltrafik (Stockholm, Sweden) ²⁹	Multi-modal transportation payment	Contract awarded for 1.4 million cards
Octopus Card (Hong Kong, Macau, Shenzhen)	Electronic payment system used for multi-modal transportation payment, retail payment and access control	Over 19 million Octopus in circulation, with over 10 million transactions per day and 2,000 service providers accepting Octopus, including non-transit retailers ³⁰
Oyster Card (Transport for London)	Electronic payment system used for multi-modal transportation payment	Over 15 million Oyster cards in circulation, , with more than 8.5 million daily transactions. A modernization program to include ITSO ³¹ and open payments ³² support is in progress.
PRESTO card (Toronto, Canada)	Multi-modal regional transportation payment	System operational with additional transit stations being added
RATP (Paris) NAVIGO ^{TM33}	Multi-modal transportation payment	1.5 million passes in circulation
Suica (Japan) ³⁴	Electronic payment system	Over 25 million cards and 1 million

²⁵ Sources: Smart Card Alliance white papers

²⁶ Ibid.

²⁷ <http://en.wikipedia.org/wiki/EZ-Link>

²⁸ Ibid.

²⁹ Ibid.

³⁰ Source: Hong Kong Octopus web site, <http://www.octopuscards.com/enindex.jsp>

³¹ Source: Cubic

³² <http://www.theregister.co.uk/2010/10/04/oyster/>

³³ <http://www.gemalto.com/transport/index.html>

Program Name/Location	Type of Program	Status
	used for multi-modal transportation payment and retail payment	mobile phones in circulation.
Taipei EasyCard and TaiwanMoney Card ³⁵	Electronic payment systems used for multi-modal transportation payment and retail payment	13 million cards in circulation; cards co-branded with other payment applications (bank-issued EasyCash, Visa payWave, MasterCard PayPass)
T-Money (Seoul, Korea) ³⁶	Electronic payment system used for multi-modal transportation payment and retail payment	8.5 million cards in circulation, with 25 million transactions per day ³⁷
Translink goCard (Brisbane, SE Queensland, Australia) ³⁸	Multi-modal, zone-based transportation fare payment system with multi-operator revenue apportionment, settlement and clearing.	Over 1 million cards issued. "There were 23.6 million goCard trips between January and March 2010 which is more than double the trips for the same quarter last year." ³⁹
Transantiago (Santiago, Chile) ⁴⁰	Multi-modal transportation payment	Over 5 million daily travelers

Table 4. Examples of Smart Card Use by Transit Programs in the U.S.⁴¹

Agency & Program Name	Type of Program	Status
Atlanta MARTA (Breeze) (http://www.breezecard.com/)	Multi-agency inter-modal smart card fare collection system	System operational.
Boston MBTA (Charlie Card) (http://www.mbtta.com/fares_and_passes/charlie/)	Automatic fare collection system	System operational with over 1.4 million Charlie Cards issued.
Chicago CTA (Chicago Card and Chicago Card Plus) (http://www.chicago-card.com/)	Fully inter-modal and inter-agency smart card fare collection system	System operational; two-step RFP issued August 2009 for smart card-based open payments system
Houston METRO (Metro Q card) (https://www.ridemetro.org)	Automatic fare collection system	System operational.
Las Vegas Monorail (http://www.lvmonorail.com)	New fare system (new service)	Transit service opened in July 2004.
Los Angeles LACMTA (TAP) (http://www.mta.net)	Multi-agency regional fare system	System operational. The TAP ReadyCARD combines Visa prepaid debit functionality with the TAP

³⁴ APTA Asia Fare Collection Study Mission, Ging Ging Fernandez, Booz Allen Hamilton, presentation, 2009 Payments Councils Summit, February 24, 2009

³⁵ Ibid.

³⁶ APTA Asia Fare Collection Study Mission, Ging Ging Fernandez, Booz Allen Hamilton, presentation, 2009 Payments Councils Summit, February 24, 2009

³⁷ Source: "APTA Trade Mission-Asia Smart Card Tour," David deKozan, Cubic

³⁸ Source: Cubic

³⁹ <http://www.translink.com.au/mediarelease.php?id=153>

⁴⁰ Ibid.

⁴¹ Sources: Smart Card Alliance white papers, public transit agency web sites.

Agency & Program Name	Type of Program	Status
		proprietary transit application on a single card. ⁴²
Maryland Transit Administration (MTA) (http://www.mtmaryland.com)	Statewide smart ticketing with all subway, light rail and commuter rail systems using the same smart card, plus linking the state's commuters to the regional bus and commuter rail system that feeds into Washington, DC	System fully installed. MTA branded (Charm) cards issued on pilot basis to same specification as WMATA SmarTrip. Plans to launch Charm as regionally interoperable media with bi-directional cross acceptance across SmarTrip program. ⁴³
Miami-Ft. Lauderdale-Palm Beach MDTA/SFRTA (EASY Card) (http://www.miamidade.gov/transit)	Multi-agency CFMS-compliant regional fare system ⁴⁴	System operational, with buses, Metrorail and Metromover using the card
Minneapolis-St. Paul/Metro Transit (Go-To Card) (http://www.metrotransit.org/buy/Pass/goToCard.asp)	Regional ticketing system for light rail and bus rapid transit	System operational.
Newark/PANYNJ, PATH & NJT (SmartLink) (http://www.pathsmartlinkcard.com/)	Integrated fare system for PATH subway - CFMS-compatible	SmartLink system operational. Contactless open bank card payment trial active.
Philadelphia PATCO (Freedom) (http://www.ridepatco.org/schedules/freedom.asp)	Multi-modal contactless smart card-based AFC system that links rail and parking services	System operational.
Utah Transit Authority, Salt Lake City, UT (http://www.rideuta.com/)	Regionally-based open payments contactless smart card program	System operational on all modes, including regional and express buses, light rail and commuter rail
San Diego MTDB (Compass card) (http://compass.511sd.com/)	Regional integrated smart card-based AFC system for the county's busses, trolleys, Coaster Commuter Rail, and future expansion of light rail system	System operational.
San Francisco MTC (Clipper) (https://www.clippercard.com)	Regional multi-modal integrated smart card-based AFC system that will extend to over 25 operators	System operational with five operators, with additional operators planned in 2009/2010. Over 150,000 active cards in circulation in August 2010.
Seattle-Puget Sound/KC Metro (Orca card) (http://www.orcard.com/ERG-Seattle/p1_001.do)	Regional multi-modal integrated smart card-based AFC system that will extend to 6 operators	System operational.
Philadelphia SEPTA (http://www.septa.com/)	Multi-modal automatic fare collection system	RFP in process. System will include SEPTA branded cards, contactless

⁴² Visa Opens Doors for Mass Transit Riders in New York and Los Angeles, Visa press release, Sept. 21, 2010, <http://www.marketwatch.com/story/visa-opens-doors-for-mass-transit-riders-in-new-york-and-los-angeles-2010-09-21>

⁴³ Source: Cubic

⁴⁴ Case Study: Miami EASY Card System, <http://cts.cubic.com/Customers/UnitedStates/CaseStudyMiami/tabid/428/language/en-US/Default.aspx>

Agency & Program Name	Type of Program	Status
		credit and debit cards, authorized/registered media, senior/disabled contactless media.
Ventura County, California (GoVentura) (http://www.goventura.org/?q=get-there-by-bus/goventura-smartcard)	Regional dual-interface farecard	System operational
Washington-Maryland-Virginia WMATA (SmarTrip) (http://www.wmata.com/fares/smarttrip/)	SmarTrip® is a regionally-based, multi-modal, fully integrated AFC system	Over 2.5 million cards in active use on MetroRail and Metro buses, in Metro-operated parking lots, and with nine regional transit operators; RFP issued in June 2009 for two-step process to develop and install smart card-based open payments system

6.1.2 Traditional Transit Payment⁴⁵

Traditional transit fare payment systems rely on transit agency issuance of some form of fare media or ticket. The fare media in an automatic fare collection (AFC) system is typically based on a stored value payment model. The stored value can be represented in different ways: as electronic cash, as a fixed number of rides, or as a period pass. Transit customers prepay a certain amount, which is then stored in an electronic purse (e-purse), either on the fare medium (e.g., a contactless smart card) or in a central account on a host system that communicates with the fare medium.

Cash, credit, debit and prepaid payment products are widely accepted in the transit industry for purchasing fare media and for loading stored value on the transit payment cards. Transit patrons now use financial payment cards (either magnetic stripe, EMV chip or contactless cards) to buy transit fare cards from vending machines, customer service agents, and transit web sites. Patrons are issued the transit-specific fare medium, which is then used for a fare payment transaction at the entrance to a subway, bus, or other mode of transportation.

Transit stored value instruments are typically valid for fare payment only at the agency issuing the fare media or across localized regional operators holding acceptance agreements with the issuing agency. These multi-agency solutions are facilitated by agreeing on a single standard payment media and service provider, or by promoting a single technical standard to which systems can be built.

On-board or in-station equipment reads, interprets, and processes this data to apply fare policies and generate transaction records. Terminals are designed so that the fare payment process can occur offline. Records are stored for forwarding or collection later, supporting consolidation, detailed audit reporting, and security. Networks are designed to leverage intermediate consolidation nodes that facilitate this process and protect against data loss.

In a fare payment transaction, the fare value is deducted at the point of entry from the stored value or validity is checked for a fare product (pass, multi-trip ticket, transit benefit). Transit e-purse transactions resemble typical cash transactions with two important differences:

- Communication between the local reader and the card at the point of entry completes the transaction. This interaction is generally both a validity check (through the application of rules that apply to the use of the fare media) and, in the case of stored value, an update of the remaining value on the fare media. In some cases, the transaction occurs offline (e.g., on a bus) and a central system is updated later. In other cases, a virtually real-time data exchange is possible. In most cases, however, the transit system validates payment at the time of use of its fare media rather than accumulating charges and billing later.

⁴⁵ Sources: Smart Card Alliance white papers

- During the transaction at the point of entry, data elements critical to the transaction (e.g., location identifiers, descriptions of past use) are transmitted to enable payment of the proper fare using applicable rules. To meet the operational requirements of most transit agencies, the transaction must be completed typically in less than 300 ms.

In a multi-operator system, clearing functions are either handled in a central system by one of the participating operators or by a third party. Figure 10 illustrates a smart card-based transit payment system architecture incorporating multiple operators, multiple modes and a central clearinghouse. Transaction data is collected and reconciled at the central system, and the correct fare revenue is deposited in the appropriate operator's account. If external merchants participate in the program, the clearinghouse can also clear funds for the merchants as well.

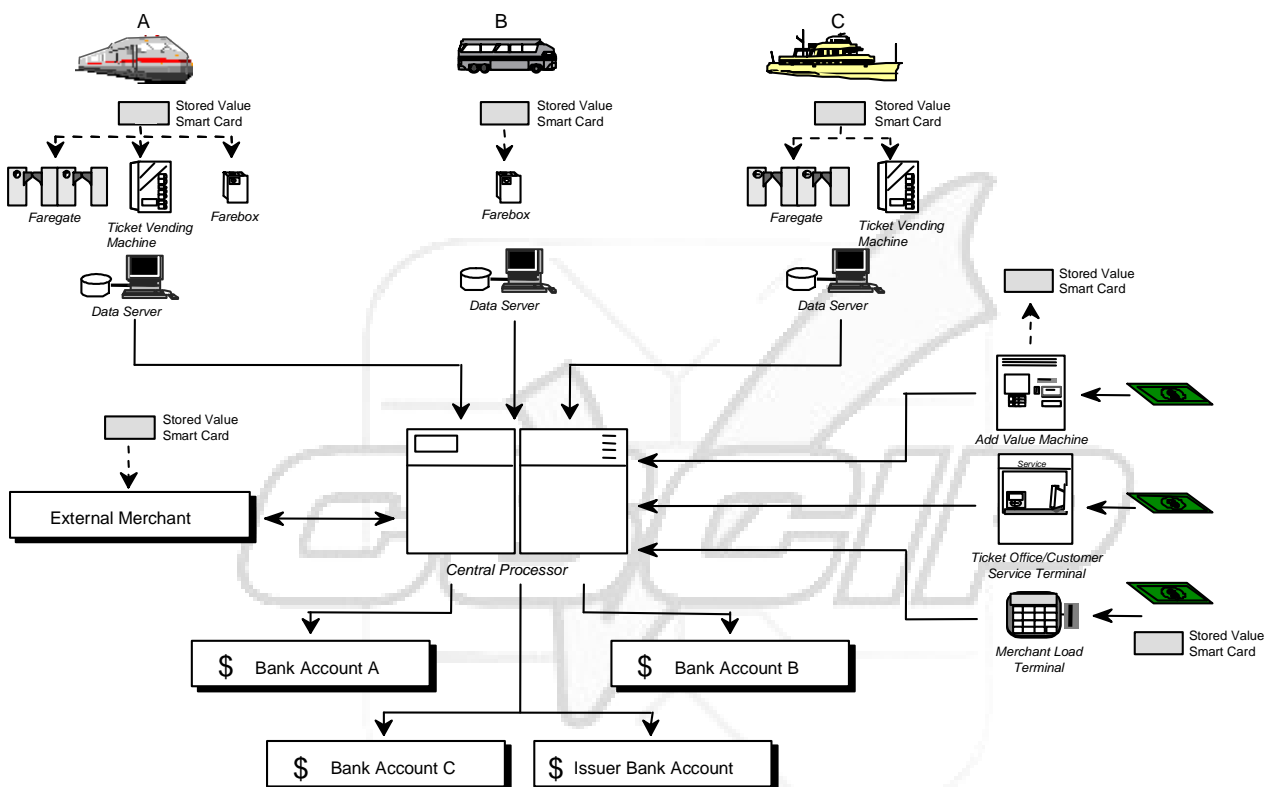


Figure 10. Multi-Operator Transit Stored Value Smart Card Payment

6.1.3 Developments in Transit Payment⁴⁶

6.1.3.1 Transit Standards, Specifications and Guidelines

While initial transit AFC systems were closed, proprietary systems, the industry has made significant progress in moving to standards-based systems.

- New transit initiatives are using the ISO/IEC 14443 international standard for the contactless smart fare card-to-reader interface and are beginning to apply transit-industry defined standards for the contactless smart fare card-to-reader interface.

⁴⁶ Sources: Smart Card Alliance white papers

- Transit industry associations and private organizations have defined and published transit-specific application-level and intersystem messaging standards, specifications and guidelines to make distributed regional system architectures easier to design, procure, implement and operate. These include:
 - The American Public Transportation Association (APTA) Contactless Fare Media System (CFMS)⁴⁷ standard in the U.S.,
 - The ITSO standard⁴⁸ in the United Kingdom;
 - The Electronic Fare Management (EFM) standard⁴⁹ defined by the Verband Deutscher Verkehrsunternehmen (Association of German Transport Undertakings – VDV) in Germany. The VDV Core Application system development began in 2003 and has started to be implemented in various projects to varying levels of complexity. The Germany-wide back-office solution for VDV Core Application is under development. It is estimated 5 million cards will be in the market by 2011 and by 2015 it is forecast that 10 million cards will be in the market in 30 regions.⁵⁰
 - The Scandinavian standard, RKF, which was developed to facilitate one travel card in Denmark, Norway and Sweden.⁵¹ The standard is being implemented in various regions of Denmark and Sweden. The standard has yet to be developed to permit interoperability between regions.
 - The Calypso specification⁵² is a privately owned European specification that is available for license to industrial partners. Calypso describes the transaction between a contactless card and reader and offers a standardized approach that is supplier-independent.
- In Europe, several previously disparate standards, such as ITSO, VDV, and Calypso (France), are being harmonized under IOPTA. This move to standardization is also reflected by national smart card programs currently in the design stages in countries such as the Netherlands, Denmark, and Germany.

6.1.3.2 Transit and Open Payment Systems

While the transit industry was investing in smart card-based AFC systems, parallel developments were taking place in the financial industry: the introduction of contactless credit, debit and prepaid payment products; new programs and rules for low value transactions; and processing approaches that can handle micropayments cost effectively. Both of these industries also settled on the common ISO/IEC 14443 standard defining the card/reader interface. These developments created opportunities for transit agencies to work with the financial industry to accept contactless financial payment devices and offer new payment mechanisms for the transit rider population.

Three U.S. transit agencies have launched programs to accept contactless credit and debit cards at the point of entry to the transit system (i.e., at the subway gate and on the bus).

- Utah Transit Authority officially launched its new electronic fare collection system (EFC) in January 2009⁵³, after completing a pilot started in 2006 and issuing an RFP in May 2007. The UTA system accepts the UTA Ed Pass and Eco Pass, as well as open contactless credit and debit cards. A profile of the UTA implementation can be found in Section 8.2.2.

⁴⁷ Additional information is available on the APTA web site at <http://www.aptastandards.com/>.

⁴⁸ Additional information is available on the ITSO web site at <http://www.itso.org.uk/>.

⁴⁹ Additional information is available on the VDV web site at <http://www.vdv.de/en/index.html>.

⁵⁰ Source: Cubic

⁵¹ *Smartcard Interoperability Issues for the Transit Industry*, Transit Cooperative Research Program, TCRP Report 115, 2006, http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_rpt_115.pdf

⁵² <http://www.calypsonet-asso.org/index.php>

⁵³ *Electronic Fare the Future for UTA*, UTA press release, January 2, 2009

- MTA New York City Transit partnered with MasterCard and Citibank in a successful pilot accepting MasterCard PayPass credit and debit payment at subway fare gates in 2006. The trial produced good results for NYC Transit. The overall feedback from riders was very positive, with the approach easily understood and used. NYC Transit found that the system was highly reliable, accurate and effective and had proven direct cost savings. There were no unanticipated technical issues and the 300 msec or less read was achieved. In addition, the Phase I average fare increased 17 percent and ridership increased 8 to 13% in both revenues and ridership.

Phase II of the trial started in June of 2010 and expanded to include participation from two additional transit authorities in the region, Port Authority New York New Jersey and New Jersey Transit. The Phase II trial includes nearly 500 points of purchase with roughly 350 buses, all 26 stations on the MTA's Lexington line and one faregate at each PATH train station. The Phase II regional pilot supports both the base fare (\$2.00 and Pay-As-U-Go), as well as all passes, transfers and reduced fares. Phase II also expands payment choices, accepting both MasterCard PayPass and Visa payWave.⁵⁴

- Los Angeles (LACMTA) recently launched a 12-month pilot with Visa to offer a co-branded, dual-application contactless prepaid card that can be used both for transit payment and as a general purpose retail payment card.⁵⁵

These programs have had a significant impact on the U.S. transit industry, with many transit agencies now evaluating how they can accept open contactless credit/debit payment in addition to or instead of proprietary payment systems. Four such agencies are now conducting procurements which reflect support for open payment acceptance within the system. Additional information about these transit programs can be found in Section 8.2.

6.1.3.3 Transit Extensions to Retail Payment

Transit agencies in a number of countries have also extended the use of the transit-issued e-purse for payment at the traditional retail point-of-sale, including the Hong Kong Octopus Card, Korea Smart Card Company Ltd (KSCC) T-money card, Japan Suica card, and Singapore Symphony for e-Payment (SeP).

- **Hong Kong Octopus Card.** The Octopus card was launched in 1997 as an electronic purse for public transportation in Hong Kong. The card's acceptance and popularity have since extended its use to retailers for general retail payment. This contactless smart card system currently includes over 2,000 service providers, including public transportation services, apparel stores, bakeries, car parks, cinemas, convenience stores, fast food chains, household stores, leisure facilities, personal care stores, photo finishing stores, photocopiers, supermarkets, and vending machines. Octopus cards are also used on school campuses and at residential and office facilities for building access control.⁵⁶
- **KSCC T-money card.**⁵⁷ The T-Money card is used for rail, bus and taxi service, parking and retail payment (convenience stores, museums, interior malls, payment of city fines, tax payments, and civil services). Over 10 million unique users generate approximately 25 million daily transactions. 60% of users carry a bank-issued credit card that includes a "light" version of the T-Money application. KSCC has begun to introduce mobile payment in collaboration with three mobile network operators, with just over 300,000 T-Money-enabled phones now. The phones are specially fitted with an antenna and a SIM loaded with the application. These units are not compliant with Near Field Communication (NFC) standards but functionally perform the same way.

⁵⁴ Source: Smart Card Alliance Transportation Council Meeting, New York, NY, Sept. 22-23, 2010

⁵⁵ *Visa TAP Co-Branded Card*, Jane Matsumoto, LACMTA, presentation, 2009 Payments Councils Summit, February 24, 2009

⁵⁶ <http://www.octopuscards.com/consumer/payment/use/en/index.jsp>

⁵⁷ "APTA Trade Mission-Asia Smart Card Tour," David deKozan, Cubic

- **Japan Suica card.**⁵⁸ JR East launched the Suica card in 2001 as part of an effort to decrease congestion by improving service and speeding ticket purchase and processing through the faregates. Over 25 million cards and 1 million Suica-enabled mobile phones are in circulation and are used at over 140,000 terminals. The Suica card is used for rail fare payment and, starting in 2004, for retail payment at shopping malls, convenience stores and airport merchants. Of the approximately 20 million transactions on Suica cards per day, 1.15 million are non-transit e-Money transactions.
- **Singapore SeP.**⁵⁹ SeP is the backend processing, security and clearing system developed by the Singapore Land Transport Authority (LTA) for transit and non-transit payments supporting the Singapore standard for Contactless ePurse Application (CEPAS).⁶⁰ SeP will allow any card to be used for payment purposes, as long as it complies with CEPAS. CEPAS enables Singaporean issuers to offer a single multi-purpose stored value card for all micro-payments, including transit, taxi, road tolls, parking, and retail. CEPAS-compliant EZ-Link cards have been available for sale since December 2008.

6.1.3.4 Regional Initiatives in the U.S.

U.S. transit payment systems had historically been closed systems that restricted acceptance to cards from a single operator. Over the last several years, however, multiple regional agencies have forged cooperative alliances and established regional administrative bodies to manage activities such as card distribution, customer service operations, transaction processing, and IT. Examples include:

- The **WMATA SmarTrip® system**, which operates in the Washington, D.C.–Baltimore corridor, now includes 12 independent transit operators currently accepting the SmarTrip card, each with its own suite of products, discounting, and social equity programs.
- The **San Francisco Bay Area Metropolitan Transportation Commission** has launched the Clipper card for payment across multiple agencies in the region, including Golden Gate Ferry, AC Transit, San Francisco Muni, Caltrain, BART, VTA and SamTrans. Clipper implements a regional electronic purse and agency-specific fare products. Over 150,000 active Clipper cards have been placed in circulation since product launch in June of 2010.⁶¹

Supporting these regional efforts, the transit industry has also been defining guidelines and standards that are designed to enable interoperability among agencies and systems. The American Public Transportation Association (APTA) published the Contactless Fare Media System (CFMS) standard, which defines the data elements and their on-card organization as well as the messages sent between operator-specific systems and the regional processing center; this effort is one piece of the full standards development process to ensure interoperability of systems

6.1.4 Smart Card Benefits to Transit

Smart cards offer numerous benefits for transit fare payment transactions.

6.1.4.1 Increased Customer Convenience

A contactless smart card is easy to use. The traveler simply taps the card on the gate reader, with no specific card orientation required. Convenience helps generate ridership growth, enhances the cost-recovery ratio, and improves the transit agency's bottom line. Contactless smart cards support flexible

⁵⁸ "APTA Trade Mission-Asia Smart Card Tour," David deKozan, Cubic

⁵⁹ Sources: Cubic; <http://en.wikipedia.org/wiki/CEPAS>; EZ-Link Pte Ltd (2008-12-26). "Commencement of sale of the NEW CEPAS-Compliant EZ-Link card," http://www.ezlink.com.sg/NEWS_ez_press26Dec08.htm;

⁶⁰ "Evolution of E-payments in Public Transport--Singapore's Experience," Silvester Prakasam, LTA, Journeys, Nov. 2009

⁶¹ *TransLink Program Update*, David Weir, Metropolitan Transportation Commission, presentation, 2009 Payments Councils Summit, February 25, 2009

fare arrangements for riders – for example, automatic discounts and multiple types of fares. When a contactless smart card can be used to pay for any mode of transportation (e.g., subway, bus, train), transfer between operators, perform fare addition and deduction on the fly, and take the guesswork out of paying fares, public transportation is more convenient to consumers and more competitive with the automobile for commuting and discretionary trips.

6.1.4.2 Efficient and Convenient Cash Replacement

A smart card-based stored value payment system provides an easy-to-use alternative to cash. Consumers can conveniently load and replenish value for transit payment through a variety of in station, on-line, and partner merchant locations. The smart card also provides an opportunity for transit agencies to partner with the financial industry or with retailers to allow payment for non-transit purchases (e.g., at quick service restaurants or other locations that value fast and convenient consumer payment).

6.1.4.3 Lower Operating Costs

While the deployment of a contactless smart card-based system is capital intensive, such a system can lower operating costs. Contactless smart card readers are more reliable and require less maintenance than electromechanical readers. Contactless transit payment cards are more secure, have a longer life, and require fewer replacements than magnetic stripe cards during their life cycle. Contactless smart cards can also increase security and reduce fraud, reduce handling costs for fare media and/or cash, and provide cash flow advantages by shifting riders to prepaid fares.

6.1.4.4 More Efficient Revenue Management Activities

Depending on how the transit operator processes currency, reconciling reports from electronic transactions can be more efficient and secure than processing cash.

6.1.4.5 Improved Customer Relationship Management

While protecting personally identifiable information, smart card-based fare collection systems provide transit operators with information about their customers' activities. Operators can use high-level data to better understand customer trip behavior and serve customers more effectively. This value is maximized as transit payment systems are deployed across multiple operators in a region. For example, traveler origin and destination information can be used to better coordinate schedules between operators within a region.

6.1.4.6 Increased Product Differentiation

Smart cards can help transit operators differentiate their service offerings and offer innovative features to customers. Smart card-based AFC systems can encourage innovative strategic thinking, such as linking transit operators with non-transit partners, resulting in deployment of multi-application payment cards. Several transit systems are laying the groundwork to make it possible to shift from a traditional role as a card-issuing agency to the role of a card-accepting system (e.g., becoming a retailer of transit services and accepting a non-transit-issued payment card).

6.1.4.7 Efficient Implementation of Transit Benefits Programs

Beginning on March 1, 2009, U.S. employers were able to offer their employees up to \$230 per month in pretax transit benefits.⁶² This figure represents an increase from the \$120 previously allowed under the federal tax code and was made possible by the Transportation Equity Act for the 21st Century. Program participants can use the benefits to commute to work on buses, commuter and light-rail trains, subways, and vanpools.

⁶² http://www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=2474

The benefit provides an optimal opportunity to link private and public sector resources to improve the quality of transportation choices. Providing these choices is seen as a major tool for mitigating regional traffic congestion and urban sprawl.

Transit benefit programs can contribute a large fraction of transit operator revenue. Administration of transit benefits programs with magnetic stripe fare media or paper vouchers is difficult and less secure. Smart card technology is being considered by organizations implementing transit benefits programs since smart cards can simplify program administration and deliver benefits electronically.

6.1.4.8 Collaboration Opportunities

Smart card-based AFC systems provide transit operators with opportunities to collaborate, both within the transit industry and with external partners. For example:

- Within a region, multiple transit operators can collaborate to use a single fare payment card for multiple modes of transit, increasing rider convenience and streamlining operations.
- Transit operators use the same smart fare card for transit-run parking facilities and/or collaborate with parking operators to use the same payment mechanism.
- With the financial industry move to contactless credit/debit payment, new opportunities are available for transit operators to work with bankcard issuers and payment brands to accept contactless credit/debit cards for fare payment.
- In addition to acceptance, transit authorities are also afforded the opportunity to enter into collaborative issuance relationships for credit, debit, and pre-paid cards,
- As NFC-enabled mobile phones enter the market, opportunities will be created to engage with carriers and members of the mobile payments eco-system to create innovative product fulfillment, payment acceptance, and mobile marketing programs. Additional information on NFC applications for transit and ticketing is included in CSCIP Module 6.
- The transit industry can also collaborate with local employers or government organizations to combine transit payment with employee ID badges used for access.

6.2 Parking⁶³

This public parking market is characterized by three primary segments, defined by different operational practices:

- Entry-/exit-controlled garages and surface lots
- Open surface lots and garages
- On-street parking

Systems and payment practices vary significantly across these segments, and historically each segment has tended to use different solution providers.

In terms of technology and systems, parking revenue automation has developed in parallel with mass transit automation. Currently deployed solutions incorporate the use of a wide range of technologies (e.g., read/write magnetic tickets, bar code tickets, RFID and proximity devices, automatic vehicle identification (AVI) systems, smart cards), currency validation components, and both attended and unattended credit card processing.

One characteristic that distinguishes the parking market from the transit market, however, is the amount of fragmentation in the industry. This fragmentation has led to the presence of significant amounts of aging payment infrastructure, management companies with poorly aggregated data and audit controls, and facilities that are particularly prone to credit card fraud and other forms of loss.

⁶³ Source: *Smart Cards and Parking*, Smart Card Alliance white paper, January 2006

In the on-street market, the industry is looking for the most effective parking solution possible. Many in that market are motivated to introduce changes to their existing infrastructure by a strong desire to enable or increase cashless payments (including credit card) as well as to improve data collection and respond to patron desires to receive receipts. Considering the online communication requirement necessary for credit card transactions and the fact that currently there is no viable single-space solution to enable them, some municipalities are turning to more sophisticated multi-space pay stations incorporated into regional wireless networks. While these features are often achieved with the new pay stations, new challenges arise including costs and enforcement (e.g., for motorcycles and convertibles). Regardless of whether single-space meters or multi-space pay stations are the best for on-street applications, the desire to increase the use of cashless payment and improve data collection in on-street parking equipment are at least two of the factors motivating changes in the parking industry.

When these factors are coupled with the new credit card processing requirements imposed by the payment brands (lack of conformance to which creates significant financial risk), the climate created is similar to that of the late-1990s transit industry. A wave of investment in payment technology and infrastructure has already begun and will continue for the next several years. The opportunity currently exists for transit and parking entities to leverage common standards, systems, technology, and support infrastructure to make overall operations more cost-effective and add value for the consumer.

6.2.1 Parking Market Segments

Parking is provided by a broad spectrum of public and private entities and, in most cases, fees are collected to pay for this valuable service. The mechanisms for fee collection vary, not only by service provider but also by whether parking is on-street.

6.2.1.1 On-Street Parking

On-street parking is primarily the domain of municipal parking programs, although some campus, hospital, transit, and airport parking programs include paid curbside parking. On-street meter programs are typically implemented and managed by municipal parking agencies. The outsourcing of municipal meter operations is a recent development, and companies are selected via competitive procurements to provide these services. The services include meter installation, maintenance, and fee collection.

Because on-street spaces are typically the most convenient, both in terms of accessibility to the motorist and accessibility to nearby places of business, these spaces must be carefully regulated to ensure that they are not monopolized by long-term parkers. On-street spaces must turn over frequently, and frequent turnover is typically encouraged by imposing time limits on their use. However, time limits alone are not adequate. There must also be a mechanism for enforcing these time limits, and the ubiquitous single-space parking meter is a well-established tool for enforcing these regulations. Paid or unpaid status determines whether a parker is in compliance with the time limit.

While the initial intent of using parking meters was regulatory, parking meters generate another obvious benefit—revenue. Municipalities now use parking meters both to control the use of curb space and to generate much-needed revenue.

6.2.1.2 Single-Space Meters

Today's single-space parking meter does not look significantly different from the meters that were deployed decades ago. Figure 11 shows examples of typical single-space meters.

However, the materials used to manufacture the meter shell and the timing mechanism have changed considerably. The shells have gone from steel to cast iron or zinc alloy, to improve durability and reduce vandalism. The mechanisms have evolved from springs and gears to electronic components, a development that opened the door for the use of contact smart cards.

Single-space meters are low cost and easy to maintain. They are almost always conveniently located near the user's parked car and they are easy for the parking public to understand and use. Typically, single-space meters accept coins, tokens, and often contact smart cards.

Single-space electronic meters are powered by low voltage batteries and are currently incapable of the online communications necessary for remote monitoring and online payment card processing. They also are required to fit into meter housings that have, for the most part, been standardized across the industry. These power and space constraints limit the ability of most such meters to house the RF transceiver required for contactless smart cards. Data is typically collected using handheld data terminals that periodically probe the devices.

In addition to the traditional single space meters found worldwide, meters with magnetic vehicle sense coils buried in the parking space are making headway in a number of municipalities in France. The town of Issy-les-Moulineaux and approximately 60 other towns have installed this new technology. The meter senses the time of arrival and the time remaining after payment. If the vehicle leaves the spot before the time expires, the meter resets to zero time for the next vehicle. However, if the time runs out and the vehicle is still parked, a digital message is sent from the meter to alert the parking authority of an overtime parker. Revenue increases have been observed.

Figure 11. Single-Space Meter Examples⁶⁴



6.2.1.3 Multi-space Meters

While single-space meters have long been a fixture on the parking landscape, new technology is now starting to be deployed. The operational constraints imposed by single-space meters (described above) have led most of the market outside North America to embrace multi-space meters, which are more sophisticated curbside payment devices. Multi-space meters accept payment for parking at multiple available spaces (either on- or off-street). Multi-space meters support a variety of online functions and a wider array of payment options. Due to their cost, they are typically configured to manage multiple spaces in a single block and provide wireless online communications necessary for real-time credit card processing and remote monitoring. Industry norms are in the range of 8 to 10 on-street spaces per meter. Networked systems also provide value-added features such as paying by cell phone. Figure 12 shows examples of typical multi-space meters.

⁶⁴ Source: MacKay Meters

Figure 12. Multi-Space Meter Examples⁶⁵



Most on-street multi-space meters operate in pay-and-display mode, in which a receipt is printed by a machine that documents the time purchased. This receipt is then placed on the dashboard for visual inspection by enforcement personnel. An alternative to pay-and-display is pay-by-space. In this scenario, spaces are numbered, and the machine logs the time purchased by space number. A printed or electronically retrieved manifest is then used for enforcement. Wireless handheld computers compliment enforcement capabilities, providing access to the paid-space database and facilitating violation issuance.

Multi-space meters are powered by either AC power or larger batteries (often trickle-charged using a solar cell), incorporate the use of wireless communications technology, and facilitate the use of credit and debit cards as well as coins and tokens for payment. Their expanded power capacity makes possible the incorporation of the RF transceivers required by contactless smart card technologies. The machines sit on real-time networks that can communicate alerts and need for collection and/or service, as well as enabling more sophisticated asset management and revenue reporting.

An additional recent development links municipal on-street programs using regional wireless networks. An example of this type of initiative is found in the City of Houston, Texas, which is attempting to procure a citywide WiFi network in concert with its movement to upgrade pay-and-display systems.

Multi-space meters are also proving to be a cost-effective alternative for collecting parking fees in off-street surface parking lots. In addition to the obvious benefit of needing fewer devices, there are indirect cost savings. Single-space meters cannot accept credit/debit cards and have limited coin storage capacity, so manual coin collection is required. Both collection and maintenance costs can be reduced if multi-space meter operations are managed effectively.

6.2.1.4 Off-street Parking

The parking demands of commuters or motorists who have business that requires more than a 1- to 2-hour visit are served by off-street parking, including surface lots and under- and above-ground parking structures. The location of these facilities is typically dictated by population density. These garages are stand-alone facilities or part of another structure and are operated by a larger group of real estate and facilities owners as well as by municipalities, port districts, stadium authorities, universities, and hospitals.

Because off-street parking facilities are expensive to construct, there must be a sound value proposition for building them. The value proposition is typically based on the level of demand created by parking generators, including office, residential and hotel/casino use for private sector garages and general, mass event, and office use for public sector garages. Regardless of the business case for construction, once such parking facilities are in operation, management is often outsourced to private parking operators.

⁶⁵ Sources: MacKay Meters, Parkeon, Reino, Cubic Parking Systems

Off-street parking facilities are expensive to construct, but they also generate a significant amount of revenue. The cities with the greatest urban density typically have the highest rates.

Regardless of either the amount of revenue collected at a facility or the entity responsible for collecting it, revenue “shrinkage” due to employee pilferage and customer fraud is an issue. To address this issue, the industry is deploying increasingly sophisticated revenue/access control systems. These systems use a variety of electronic media (e.g., bar code, proximity reader, debit system, magnetic stripe, automatic vehicle identification technology), and some systems use more than one type of medium.

The primary objectives of these revenue control systems are (1) to reduce or minimize employee contact with cash, (2) to close loopholes that enable customers to pay less than the required fee or avoid payment altogether, and (3) to improve auditability. A significant additional benefit of such systems is that the data they collect can be used to generate reports on the financial and operational performance of a particular garage or, in some cases, multiple facilities.

Revenue control for collecting off-street parking fees is primarily accomplished using one of two operational models. The first model is used where the length of stay is the basis for pricing. It uses equipment that controls access at both entry and exit points. These systems calculate hourly fees by recording entry and exit times. In the past, systems of this type typically employed a cashier to collect system-calculated fees at the point of exit. However, such systems are now incorporating credit-card-in—credit-card-out capabilities to eliminate cashier involvement and expedite egress. One variation of this type of system incorporates pay-on-foot or central pay stations. Tickets generated at the point of entry are inserted into a pay station located in the garage or at the nearby generator, and cash or credit card payment is made at this point. The ticket is updated to reflect payment and reissued for insertion into the exit lane controller. Central pay stations have been used extensively in Europe and are now gaining popularity in North America. The second operational model utilizes the pay-and-display or pay-by-space metering approach .

The choice of operational model is largely influenced by lot size and how susceptible the facility is to peak traffic flows. Unstaffed entry–exit systems accelerate payment processing and move people out of a facility quickly, enhancing user convenience.

In both cases, online connectivity is key to the effective processing of credit and debit transactions and to the remote monitoring and reporting functions. Entry–exit systems, in particular, depend on communications. The ability to serve the patron remotely is crucial to preventing a vehicle from being trapped. Systems often incorporate the use of live intercoms to communicate with centralized service personnel. The electronic media used include bar code tickets, magnetic tickets, RFID cards, and credit cards. Encoded tickets carry entry information, enabling local rate table lookup at exit. RFID and credit cards are sometimes processed at entry, updating a back-end database that is then searched at exit to calculate the fee. The use of smart cards can take the place of the encoded ticket.

In order to distribute patron flow and avoid queuing at the exit lane, pay-on-foot stations are often the point at which the rate is calculated and payment accepted. The media issued at entry is coded for exit when payment is accepted, and the exit equipment permits egress upon proper validation. Cashier terminals often compliment pay-on-foot stations to avoid the delays that can result when patrons fail to visit the machine.

6.2.2 Use of Smart Card Technology in Parking

Use of contact smart card technology is well established in the parking market, with vendors providing solutions for all segments: single-space meters, multi-space meters, and off-street parking.

The large parking vendors have installed closed-loop contact smart card solutions in many cities, including: New York, NY; Portland, Oregon; Hong Kong, China; Paris, France; Ottawa, Canada; San Francisco, California. The parking operator issues (and reissues) the smart cards, manages retail outlets (where they exist), manages cardholder queries, reloads the cards (where this is possible), and manages the entire card system.

Many of the cities implementing smart cards are doing so by leveraging their existing meter infrastructure, replacing single-space meters with smart card-enabled single-space meters. Others are upgrading their single-space meters to accept smart cards and adding additional multi-space meters where appropriate. In those cities, the multi-space meters and single-space meters share the same smart card program, and multi-space meters anywhere in the city can be used to load value onto the smart cards.

Some of these solutions only work with one parking payment vendor's technology, although there are instances of collaboration between non-competing vendors in some cities. The current implementations are restricted to one type of parking operator (either public or private), with no cross-operator implementations (for example, between public and private operators). Other solutions being implemented allow multiple cities to take part in a single collaborative parking payment system using smart cards. In these systems, a third party manages and operates the smart card payment system on behalf of the participating cities.

Meters accepting smart cards typically also accept coins, and, in the case of multi-space meters, bills and magnetic stripe credit/debit cards. The smart card solutions for on-street parking have primarily been based on both the ISO/IEC 7816 standard and proprietary smart card technologies, depending on the age of the solution.⁶⁶ With the growth in the use of multi-space technology, the door has been opened for the use of ISO/IEC 14443 contactless smart cards as well.

In addition to specific smart card-based parking programs implemented by municipalities, transit authorities around the world have implemented a model that allows the same contactless smart card fare medium that is used to pay for transit fares to also pay for parking. Examples of this model include Washington DC (Washington Metropolitan Area Transit Authority (WMATA) SmartTrip card), Metropolitan Atlanta Rapid Transit Authority Breeze card, Hong Kong Octopus card and Singapore EZ-Link card.

The security used in the different smart card solutions is implementation-specific and ranges from the use of passwords to unlock the cards to DES-based cryptography. Most meters that contain security information store it in the memory of the meter, although some contain security access modules (SAMs). The SAM stores cryptographic algorithms and the keys used to encrypt and decrypt messages securely. The smart cards can typically be used only to buy time at the meters, although there are solutions with enough security to allow the cards to be used to purchase items from local merchants.

Historically, the adoption rates for contact smart card systems have been low. Many cities record usage rates in single-figure percentages. Low usage rates have been attributed to the lack of an effective card distribution and reload infrastructure, the lack of an effective card marketing plan (for which cities typically lack budget and expertise), and the fact that the cards can only be used to pay for agency-specific parking and, typically, must be purchased from a city-authorized agent. Most implementations have used simple memory cards that cannot be reloaded, forcing the patron to purchase another card when the stored value in the first card has been used up. Some newer systems allow cards to be reloaded at a variety of terminals and over the Internet. Cardholders can also subscribe to auto-load programs, in which a link to a credit or debit card account enables the stored value to be replenished automatically, without forcing the patron to purchase a new card or find a reload location.

If implemented properly, however, a smart card system can allow a city to increase revenues dramatically. The city can increase rates on existing meters without incurring the high initial replacement costs associated with implementing a completely new system.

⁶⁶ There are some exceptions. In 1997, the Hong Kong Transportation Department initially upgraded all of its on-street mechanical coin-operated parking meters with 19,500 battery-powered electronic parking meters that only accepted payment from a disposable contact stored value smart card solely used for parking. Then in 2004, following a number of pilots and trials, the on-street single- and multi-space meter equipment was again upgraded so that it only accepted payment by the City's very popular Octopus card, which is based on technology that is similar to the ISO/IEC 14443 standard.

6.2.3 Smart Card Benefits for Parking

Smart card technology is the clear leader for on-street and short-term electronic parking payments. By implementing smart card technologies, parking operators can take advantage of the increasing consumer preference for electronic payments and achieve significant benefits.

6.2.3.1 Better Customer Service

Smart card technology has the potential to allow customers to use one card both for parking and for other payments, such as transit, tolls, or small purchases. While customers appreciate the convenience of being able to use a single card for a variety of uses, parking operators can also spread the cost of operating the smart card system over a larger number of transactions and share the costs with other application providers.

For example, schemes such as the Hong Kong Octopus card and Washington SmarTrip card (see Sections 8.2.4 and 8.2.1, respectively) allow customers to use one payment card to pay for parking at multiple sites over a large geographic area.

Smart cards, due to their strong security features, do not necessarily require the same level of user verification (i.e., a signature) as credit cards. This advantage can result in reduced transaction times, lowering customer wait times.

Smart card applications can protect users if their cards are lost or stolen. For example, a smart card can be disabled by the terminal at first use after the card is reported lost or stolen. This capability allows parking operators to ensure that customers suffer no financial loss while minimizing the cost of providing such service.

Customers using contactless smart cards never need to let the card leave their hands. Presenting the smart card to the reader enables the terminal to scan the card for user data and encode relevant data into the chip for future use. If the card is a contactless payment card, the terminal processes the transaction without the danger that the card may be captured and not returned due to equipment malfunction. This capability can be particularly beneficial at gated parking locations, such as airports.

For parking applications that calculate fees according to length of stay, entry data can be encoded into the card's chip memory and then accessed for rate table lookup. This capability eliminates the need to issue magnetic or barcode tickets, increasing customer satisfaction. Stored value or contactless credit card systems allow customers to avoid even visiting a pay-on-foot machine; the exit terminal calculates the fee and debits the transaction from the card in less than 1 second.

Smart cards allow parking operators to charge motorists only for the amount of parking time actually used. Motorists find this to be a much fairer system and the parking operator benefits by achieving a higher turnover at each parking space, since these types of systems reduce the ability for motorists to "feed the meter." For example, in Saskatoon, Saskatchewan, Canada, motorists use a smart card to purchase the maximum time allowed at a particular meter. When they return, they reinsert the card, which is then credited for any unused time, and the meter is set back to zero.

Another customer service example is the University of Wisconsin Flex Parking Program, which has implemented personal parking meters that hang on a car's rear-view mirror and work in conjunction with prepaid smart cards. The personal parking meter tracks the time and subtracts the required amount directly from the smart card. Unlike traditional parking permits, personal parking meters can pay for only the precise amount of parking time used. The meters also allow faculty the option of parking in staff and public spaces. The personal parking meters therefore allow users to park in more locations than the traditional permit, and offer the flexibility of infrequent parking for those users who opt to use alternative modes of transportation.

Smart cards make it easy for motorists to maintain value on their cards, thus encouraging use of parking services that accept smart card-enabled payments. For example, SmarTrip and Octopus cards that allow payment for parking can automatically be topped-up when the amount in the card falls below a predefined

level. Smart cards can also be recharged manually at kiosks, retail locations, and gas stations, using traditional payment methods like cash and credit/debit cards.

6.2.3.2 Increased Revenues

Smart cards increase motorists' willingness to pay at the meter. In most cases, motorists have only one choice for payment which, for a single-space meter, is generally coins. If motorists do not have the correct coins, they are more likely to simply risk a ticket. Studies have shown that offering flexibility in payment options can increase motorist compliance by as much as 20%, thereby increasing revenues for the parking operator.

Another source of increased revenue is increased rates for on-street parking. Local governments have been reluctant to raise rates to market levels, fearing that motorists would resent not only the higher rates but also the need to carry more coins. However, the City of San Francisco recently approved significant on-street parking rate increases (from \$2 to \$3 per hour in the city center). These increases were approved because the city is implementing a MacKay Meters smart card payment system for parking meters, thus offering motorists an alternative method of payment.

Since smart cards can eliminate the need for coins, consumers are also likely to increase their use of on-street parking, rather than searching for off-street parking in less convenient areas. Businesses located in city centers often claim that they have a disadvantage when competing against businesses located in suburban areas, where parking is free. While there is no direct evidence to suggest that card payment options for on-street parking provide downtown businesses with any competitive advantage over suburban shopping locations, the City of Portland has found that more people choose on-street locations when they can pay by card. In addition, it appears that in Portland the average card transaction is approximately \$2, while the average coin transaction is approximately \$0.70. The implication is that people park for longer periods and shop for longer periods when they use cards to purchase parking.

Smart card-based electronic purses may also provide parking operators with a benefit by allowing them to accrue interest on funds that the customer has prepaid. The more cash there is in the bank (as opposed to the machine), the more interest the operator earns on the money. In addition, transaction amounts tend to be higher when customers pay with credit, debit, or stored value card payments as opposed to cash.

6.2.3.3 Increased Operational Efficiency

Using smart cards can increase the efficiency of parking operations in several areas: security; labor requirements, and equipment.

Smart card systems incorporate advanced security features that reduce the risks associated with not having every transaction authenticated by a back-end management system. Parking operators need not incur the cost of installing and maintaining a full-time communication link for each parking device.

Electronic parking payments also provide economies of scale that are not available for labor-intensive processes like servicing coin-operated parking meters. The incremental cost for each additional smart card transaction declines sharply, in comparison to the transaction costs incurred using coin-operated parking meters. In addition, reduced transaction times mean that fewer staff (or gates) are required at off-street parking facilities. If the smart card used for parking is also used for other applications, parking operators can spread the cost of operating the smart card system over a larger number of transactions and share the costs with other application providers.

Other benefits can be realized in lower equipment and material costs. Cash-handling systems are complicated electromechanical assemblies that suffer from extensive wear and tear and intermittent failure. They are expensive to design, build, and maintain. Using smart cards can decrease failure potential and repair costs and also decrease the cost of consumables, such as the ticket stock associated with entry/exit systems.

However, parking operators must take into consideration that as long as cash continues to be accepted for payment, the unit cost of handling cash will increase as the percentage of total revenues collected from cards increases.

6.2.3.4 Stronger Internal Controls and Security

Cash-heavy businesses in general are vulnerable to errors made while handling cash. By reducing cash-handling requirements, smart card parking meters strengthen internal controls, reducing opportunities for inaccuracies.

Smart card technology incorporates stronger security features than any token or payment card technology. Applications can leverage the many security features supported by smart cards to ensure the integrity, confidentiality, and privacy of stored or transmitted information and to counter potential security threats. Smart card systems are much harder to compromise than magnetic stripe systems, decreasing the losses experienced by parking operators due to fraud. This is one reason that credit card issuers in Europe and elsewhere are now issuing smart card-based credit cards.

Smart cards also have extensive built-in tamper resistance. A variety of hardware and software capabilities can detect and react to tampering attempts immediately. The ability to support authenticated and authorized information access combined with strong data security make smart chip-based devices excellent guardians of personal information and individual privacy. Consequently, implementing a smart card system allows parking operators to assure motorists that effective security measures are used to protect their personal information.

Cash left in parking meters between collection cycles can be an enticing opportunity for vandals and thieves. Smart card-enabled parking meters reduce the amount of cash present in meters, thus reducing the potential and incentive for vandalism. However, it should be noted that without adequate security and controls, the reduction in physical vandalism can be offset by an increased potential for other types of fraudulent activities, such as the use of counterfeit cards, issues with reconciliation of tendered revenues with the cash receipts from the sale of cards, and theft of cards.

6.2.3.5 Expanded Strategic Marketing Opportunities

Smart cards can capture critical operational data. Captured operational data can then be analyzed to enable strategic marketing schemes such as increased price points, loyalty reward programs, payroll deductions, corporate billing, customer relationship management, and usage forecasting applications. The promise of mining such data has long been discussed; however, the majority of smart card programs have yet to reach sufficient maturity and the necessary standards have been lacking for this promise to be fulfilled. That said, a new era in the market place is coming where payment card issuers and transit collectives are embracing common technology, while interoperability standards are nearing completion. In addition, large-scale infrastructure deployments are being completed with major card roll-outs approaching. The new systems are offering a variety of “opt-in” web-based facilities that will create the mechanisms for commercial agreements surrounding shared data and applications. Discussions are taking place between transit agencies, financial institutions, online ticketing firms, parking operators, and venue managers, just to name a few.

For those municipalities deploying multi-space on-street metering programs, smart cards make a significant new revenue opportunity available. The municipality can offer load services using the meter infrastructure. For example, transit agencies are constantly looking for ways to provide convenient reload capability for bus riders. Current strategies include placing specially equipped terminals in selected retail locations. By providing a contactless transceiver on a parking meter, the meter could accept currency and credit and debit cards in payment and facilitate the sale of stored value or pass products on behalf of the transit agency. By doing so, a municipality may be eligible for the commission typically paid to a retail merchant. As smart card programs increasingly support multiple applications, the opportunity to use the meters to sell a diverse range of digital products is possible.

Smart cards allow parking lot vendors to offer consumer loyalty benefits and subsidized parking programs in partnership with local merchants. In addition, discounts can be offered to selected consumer classes like students, senior citizens, or clergy. Zoning and preferential parking rates can be offered to residents.

In places like Hong Kong and Korea, co-branded cards are being issued, smart objects (e.g., watches) are being sold and non-transit applications are being supported on cards issued primarily for transit payment. Examples include retail payment, recreational facilities access, parking payment, and security access control. The forecasted promise appears to be arriving.

6.2.3.6 Simplified Tax Benefits Administration

Beginning March 1, 2009, U.S. employers can provide employees with a tax-free or pre-tax transit benefit allowance of up to \$230 per month⁶⁷ and a parking benefit of up to \$230 per month⁶⁸. A smart card payment system can reduce or eliminate the need for employers to purchase and distribute paper transit/parking benefit checks to employees. In addition, a parking operator can easily accept and process smart card transactions. The paperless smart card-enabled payment system allows employers to simply update a cardholder database and perform an electronic funds transfer. The system can then electronically distribute the benefit to the smart card at the next point of use (train station, bus, or parking lot).

Similarly, employers can provide their employees with prepaid smart cards to use for local business travel. Both employees and employers can then receive a single monthly statement for all parking payments, eliminating the need to store or acquire individual receipts. This valuable service may encourage motorists to use the operator's facilities over others.

6.2.3.7 Compliance with Laws/Statutes

Many municipalities collect taxes on the parking revenues generated by private operators. But the cash-only systems common in private lots do not generate an effective audit trail, putting the operator at risk of being accused of tax evasion. State-of-the-art revenue control parking equipment ensures that reporting is accurate and correct rates are charged. By implementing a smart card system, a parking operator can eliminate the need to purchase and maintain parking machines, using only a handheld computer to collect parking fees from motorists securely.

⁶⁷ http://www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=2474

⁶⁸ http://www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=2474

7 Online Banking and Retail eCommerce

Over the past ten years, consumers have increasingly turned to the Internet for convenient access to bank accounts and retail purchases.

With the increase in identity theft (where an individual's personal information is stolen and used fraudulently) and in Internet threats like phishing (where a fraudulent web site link is sent to consumers in an attempt to get their personal information), the industry is starting to move to stronger authentication techniques for validating the identity of online consumers accessing bank accounts or purchasing products with credit and debit cards. While government and commercial organizations have moved to smart card-based tokens for employee identity authentication, most consumer authentication implementations are using techniques managed by the back-end systems (i.e., detecting fraudulent or suspicious activity through the online banking or eCommerce system), rather than using a hardware token that to validate the consumer's identity.

There are a few notable exceptions.

- "More than one million Barclays customers are using a Gemalto cryptographic smart card reader – PINsentry (TM) by Barclays, that offers stronger authentication for online banking. Barclays started deploying its strong authentication program in July 2007 and not one PINsentry online customer has suffered fraud since then. User feedback has proven extremely positive and Barclays observed that customer acceptance was higher than anticipated by 30%.

With PINsentry, not only do Barclays customers easily generate one-time passwords to authenticate themselves at log in, but they also use it to sign transactions, which provides a much higher level of security than just authentication using static credentials. All that customers need to do is insert their standard chip-enabled bank card into the PINsentry reader from Gemalto and type in their card's PIN code. They carry the devices with them and can perform these secure online transactions from any personal computer.

As part of the program, Barclays is now offering additional services to its online customers. The maximum amount for personal online transactions has risen from an initial £1,000 to £10,000 and plans are in place to offer international payment for the purpose of funds transfer worldwide in the near future."⁶⁹

- MasterCard Chip Authentication Program (CAP) and Visa Dynamic Passcode Authentication (DPA) allow EMV smart cards to be used to authenticate the user for online transactions (where no card is present). For an online transaction, the user would insert the EMV credit or debit card into a handheld reader. Once the user enters the PIN, the reader will display a one-time password which can be used to validate the user's identity. The user enters the password in the appropriate field on the merchant's checkout page (or online banking site) and is passed back to the issuer for authentication using the MasterCard® SecureCode™⁷⁰, Verified by Visa⁷¹ or online banking infrastructure.
- Bank of America offers SafePass® to its online banking customers to protect against online banking fraud and identity theft. SafePass provides a six-digit one-time passcode sent as a text message to the consumer's mobile phone or generated from a smart card. Consumers then use the passcode to complete online banking transactions. When SafePass is enabled, consumers are prompted to enter the SafePass code when adding new transfer and bill pay accounts and

⁶⁹ *Over One Million Barclays Customers Bank Online with Gemalto's Solution in the UK*, Gemalto press release, July 9, 2008

⁷⁰ *OneSMART Authentication*, MasterCard,
https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/cap/index.jsp

⁷¹ *Dynamic Passcode Authentication: Overview Guide*, Visa publication,
<http://www.visaeurope.com/documents/aboutvisa/dynamicpasscodeauthentication.pdf?d=070207>

payees, when making large transfers, when verifying identity and (optionally) when signing in to online banking.⁷²



⁷² http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass

8 Sample Smart Card Payment Models

8.1 U.S. Contactless Credit/Debit Payment

Contactless payment is being delivered around the world by the payment brands and their issuing and merchant customers by leveraging the existing payment card infrastructure as its basis for implementation. In the U.S., the payment brands implemented contactless payment transactions to leverage the existing magnetic stripe payments infrastructure. This approach facilitated straightforward contactless payment implementations by issuers, merchants and payment processors and faster consumer adoption and merchant acceptance.

It is important to note, however, that U.S. contactless payments do use EMV-compatible payment features that allow the existing magnetic stripe transaction-based networks to use the enhanced security of smart cards. A unique, dynamic cryptogram is generated on the contactless card or device for every transaction. This approach adds security to the payment process by preventing replay attacks (no transaction can be done twice) and card cloning or skimming (the card key never leaves the protection of the smart card memory).

The flow of a traditional magnetic stripe credit card payment transaction includes the following steps:

- The merchant's point-of-sale (POS) system sends an authorization request for the transaction (including the cardholder account number and transaction amount) to the merchant acquirer/processor, who then sends it through the financial networks to the card issuer.
- The issuer performs the necessary security checks (e.g., checking the security information included with the transaction, determining the validity of the payment card, analyzing cardholder behavior to assess if the transaction could be fraudulent), authorizes or denies the transaction, and returns an authorization response to the merchant acquirer/processor, who passes it to the merchant.
- Authorized transactions are captured from the merchant every day, and a settlement message is sent over the financial networks to transfer funds to the merchant account (transaction amount less merchant discount rate).

The same flow and process applies to contactless financial payment transactions in the United States, with the following exceptions:

- Cardholder payment information is transferred to the POS system wirelessly, using radio frequency (RF) technology. The ISO/IEC 14443 is used as the communications protocol between the card and the reader.
- At the card level, each contactless card can have its own unique built-in secret "key" that is used to generate a unique card verification value or a cryptogram that exclusively identifies each transaction. No two cards share the same key, and the key is never transmitted. Contactless cards employ standardized encryption technology, 128-bit (e.g., Triple DES).
- At the system level, payment networks have the ability to differentiate contactless and magnetic stripe transactions and automatically detect and reject any attempt to use the same transaction information more than once.
- Many contactless payment cards and devices do not transmit the name of the cardholder, limiting the amount of information that is communicated during the transaction. The cardholder name is part of the existing magnetic stripe data common on most traditional credit cards.
- Some contactless payment cards and devices do not include the cardholder's account number, but use an alternate number that is associated with a payment account by the issuer's backend processing system. This alternate number would not be able to be used in other payment transactions (e.g., with a magnetic stripe card or on the Internet).

- After a traditional credit card transaction is approved, the merchant provides a sales receipt for the cardholder to sign. In many cases, merchants accepting contactless payment cards also participate in programs for low-value transactions; the consumer completes the transaction without signing a receipt.

The transaction flow for a contactless payment transaction in the U.S. differs based on the payment application (e.g., PayPass, payWave, ExpressPay), but follows the basic steps below.⁷³

- The POS terminal starts the transaction when a contactless card is brought within range (1-2 inches). Based on the card, the terminal selects the payment application.
- Contactless implementations differ somewhat, but all generate some form of dynamic data.
 - An application transaction counter (ATC) is incremented on the card.
 - The terminal generates an "unpredictable number," asks the card to generate dCVV or CVC3 and the ATC, and creates a cryptogram using a secret key.
 - The card calculates the proper cryptogram or signature that is unique for the transaction. The card appends account information and sends all information to the terminal.
- The terminal then packs the transaction data and signature into a discretionary field of the standard financial message, and transmits the data over the existing magnetic stripe network. This allowed the U.S. payments industry to implement contactless payments with minimal modification to the magnetic stripe payments infrastructure. The dynamic signature, which was generated by the card, increases the security of the transaction versus magnetic stripe transactions; the transaction cannot be replayed and the card cannot be copied or cloned.

8.2 *Transit*⁷⁴

This section profiles four different transit programs, each of which implements a smart card-based payment model, including:

- Washington Metropolitan Area Transit Authority and Surrounding Area, who implemented a region-wide closed system contactless fare payment card
- Utah Transit Authority, who accepts both a closed system contactless fare payment card and open credit and debit payment cards
- London Oyster/Barclaycard, who implemented a closed system contactless fare payment card, plus accepts a combined bank-issued card that includes the transit application and bank card payment.
- Hong Kong Octopus Card, who implemented a closed system contactless fare payment card for transit which can now be used at general retail locations

8.2.1 Washington Metropolitan Area Transit Authority and Surrounding Area

The major public transit operator in the Washington, DC, marketplace is the Washington Metropolitan Area Transit Authority (WMATA), which is an interstate compact agency. WMATA operates the local subway system (Metrorail, with 86 stations, 106 miles) and a regional bus system (Metrobus, with 1,450 buses) with ridership of approximately 1.3 million trips per day.



⁷³ *Smart Card Standards 101*, William Gostkowski presentation, CTST 2009 Smart Card Technology and Payments Applications Workshop, May 4, 2009

⁷⁴ Sources: Smart Card Alliance white papers

WMATA was the first transit authority to push aggressively for the use of smart cards in its systems. WMATA has been using the SmarTrip® card (based on the Cubic Gocard) for Metrorail and parking since May 1999. The Metrobus system became fully SmarTrip capable in August 2004, and a series of contracts are in place between the system provider and multiple independent transit agencies throughout the State of Maryland, the District of Columbia, and Northern Virginia to expand SmarTrip acceptance throughout the region. Now 12 agencies accept SmarTrip, with over 8,000 processing devices deployed.

Since its launch, WMATA has issued over 2.5 million SmarTrip cards. The SmarTrip card is available as a stored value card (up to \$300) for full-fare and reduced-fare customers. A SmartBenefit service allows the cards to be electronically loaded with transit benefits.

In June 2004, SmarTrip became the only form of payment accepted at Metro-operated parking lots. (See Section 8.3.1 for additional information on WMATA's parking implementation.) To handle card availability and distribution, WMATA placed card dispensers in each of its rail stations with parking facilities. This mandatory use of the card at parking facilities resulted in a surge in the quantity of cards sold. During the first year of automated card vending, WMATA sold over 700,000 SmarTrip cards, of which 80% were sold from the card dispensers.

In 2005, WMATA and Citibank teamed up to offer the Citi® Platinum Select® SmarTrip MasterCard, a combination Metro SmarTrip card and Citibank credit card. As an added benefit to the SmarTrip program, customers receive 5% back as a statement credit for 6 months (up to \$300) when they use the card to pay for Metrorail and Metrobus fares or Metro-operated parking. The pilot ran from November 2005 to July 2009 and was very popular with the customers. Success of this pilot was a key indicator to advance the open payments program at WMATA.



In 2010, the Maryland Mass Transit Authority began issuance of the Charm card developed using common specifications with SmarTrip. Each agency will cross honor the two interoperable smart card products.

The WMATA smart card distribution network includes retail stores and mail-order options. At WMATA parking locations, the organization relies on vending machines that sell cards with value to patrons requiring the mandatory card to park. The addition of these vending machines has sharply increased the penetration rate of the cards.

8.2.2 Utah Transit Authority⁷⁵

UTA serves six primarily urban counties along the Wasatch Front with a population of 1.9 million people covering an area of 1,400 square miles. UTA is the only major transit operator in the region. The agency operates 489 peak-period buses in regular service, 41 buses in special ski service, and 80 paratransit vehicles. The TRAX light-rail line operates 46 vehicles on two lines for a total of 18 miles. Fare collection is through a proof-of-payment (POP) honor system. Commuter rail service started in 2008 with an initial 44-mile-long line. Plans call for a POP zone-based fare system.

UTA provides 32 million trips per year with a \$136-million operating budget. It has a 14% operating ratio, with \$20 million collected as fares. Pass products are responsible for 70%–80% of fare revenue. These products include the Ed Pass program, which allows students to use their student IDs as passes; the Eco Pass program for employers, who issue passes to all their employees; and period passes sold at retail outlets throughout the region. Cash collections through fare boxes total \$3.5 million. The basic adult cash fare is \$1.50 and includes a two-hour transfer. The one-way fare for ski service is \$3.00.

UTA officially launched its new electronic fare collection system (EFC) in January 2009⁷⁶, after completing a pilot started in 2006 and issuing an RFP in May 2007. Thousands of UTA riders now tap their passes

⁷⁵ Sources: <http://www.rideuta.com/electronicfare>; UTA Electronic Fare Collection System: Development Progress Report, Craig Roberts, UTA, presentation, 2009 Payments Councils Summit, February 25, 2009

⁷⁶ Electronic Fare the Future for UTA, UTA press release, January 2, 2009

to electronic readers installed on buses and train platforms from Brigham City to Payson. The new EFC system initially serves only some UTA riders, but eventually will expand to become the primary method of fare collection for the transit agency.

Initially, most users of the new EFC system are Ed and Eco Pass holders—students and employees who carry annual UTA transit passes issued by their school (Ed Pass) or employer (Eco Pass). They, as with other users of EFC, are required to tap on when boarding and tap off when exiting a bus or train platform to validate their fare.

The new EFC system also accepts contactless credit and debit cards. Contactless credit and debit cards are a new form of payment media issued by banks and credit card companies that allow a consumer to make a payment without swiping their card, signing for the transaction, or entering a pin number. These include Visa payWave, MasterCard PayPass and American Express ExpressPay. By tapping a contactless credit or debit card to an electronic reader on a bus or train platform, riders may initially pay a single adult cash fare. Credit card holders are also asked to tap off when exiting in order to complete their trip and get an electronic transfer.

All other fare types (e.g., monthly pass, cash fare) continue to be accepted as they have in the past until they are transitioned to the new EFC system over the next two years.

EFC readers are located at all bus doors and train platform entrances for easy access. Transit police officers who inspect fares on board TRAX and FrontRunner also have handheld inspection devices that allow them to check whether a card has been validated at a reader prior to boarding.

To implement the new EFC system, UTA installed readers at all doors of 520 fixed route buses, installed 170 validators on 35 TRAX and FrontRunner platforms and installed wireless gateways on buses that support WiFi in four depots and 3G continuous mobile service throughout the service area. The system is account-based, with business rules and transaction processing in the back office, and authentication achieved in real-time or near-real-time. A key goal for the program was to accept open bankcard credit and debit payments, which it achieved.⁷⁷

The new EFC system is one component of a state-of-the-art technology and communications infrastructure upgrade that UTA will implement over the next few years.

8.2.3 London Oyster/Barclaycard⁷⁸

Transport for London (TfL), through a concession contract to Transys Ltd., developed and deployed a contactless smart card system for all London Underground and London Bus operations. The contactless card was branded Oyster[®] and launched in August 2002.

The system was the first large-scale deployment of a fare terminal infrastructure compliant with ISO/IEC 14443, Type A and Type B. The basic card technology uses NXP (then Philips) MIFARE[®] Classic smart cards. The system incorporates over 18,000 devices, including fare gates, ticket vending machines, ticket office machines, bus fare registers, bus validators, handheld terminals, and merchant POS equipment.

Since system launch, a variety of user convenience options have been introduced to complement the original stored value utility provided by Oyster. These include: web-based sales with product collection at point of validation (ad-hoc load); automatic top-up of value; daily price capping.

The project is a well-documented success, winning a variety of awards, and has a current circulation in excess of 15 million Oyster cards. Today, more than 75% of all daily bus and subway rides use Oyster for payment.

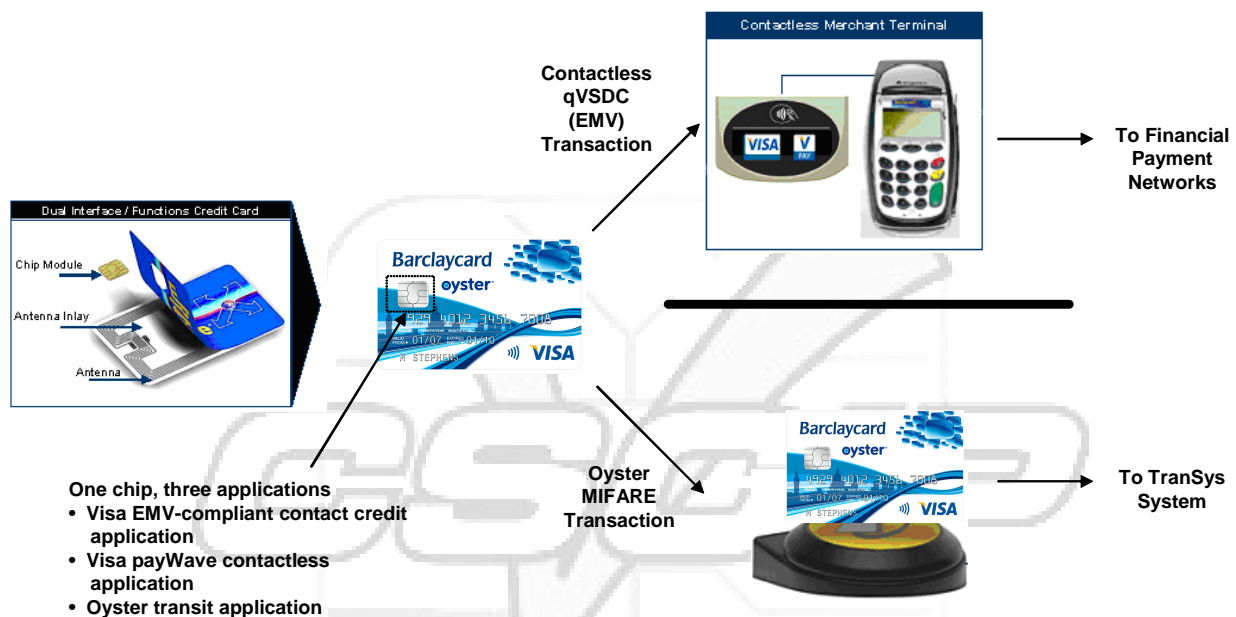
⁷⁷ UTA Electronic Fare Collection System: Development Progress Report, Craig Roberts, UTA, presentation, 2009 Payments Councils Summit, February 25, 2009

⁷⁸ Source: *Co-Branded Multi-Application Contactless Cards for Transit and Financial Payment*, Smart Card Alliance Transportation Council white paper, February 2008

In 2006, TranSys and TfL negotiated an innovative arrangement with Barclays Bank PLC for the issuance of a multi-application co-branded bankcard. Under the terms of the licensing agreement, Barclays has an exclusive license for a fixed period of time to place the Oyster application and brand on new contactless financial payment cards.

The first product resulting from this agreement is the Barclaycard OnePulse card⁷⁹, a three-in-one card that combines Oyster (a closed system electronic purse application using ISO/IEC 14443 Type A) with contactless Visa payWave (based on ISO/IEC 14443) and traditional contact EMV⁸⁰ credit and debit payment (based on ISO/IEC 7816). (See Figure 13.) The Barclaycard OnePulse card carries the transit and financial applications on the same chip. There is no interaction between the two applications. The financial application is a standard, fully certified EMV application.

Figure 13. Barclaycard OnePulse Card Operation



From the transit reader's perspective, Barclaycard OnePulse cards are indistinguishable from standard Oyster cards. Barclaycard OnePulse cards could therefore be used immediately on every mode of transport and with all retail, validation, and handheld equipment on the transit system. The only change was to create a new configuration setting for these cards so that the transactions they generate on the transit system are distinguishable from transactions generated by other Oyster cards. This change allows card use to be reported easily and relevant management information to be generated (e.g., where the cards are being used, how frequently they are being used, and what travel products are being loaded onto them).

Under the terms of the agreement, TranSys provides Barclays with the tools and data necessary to load the transit application onto the chip when the card is personalized. The transit application itself is not personalized but is marked as "registered," and the relevant personal details are passed to TfL for its records, thereby providing Barclaycard OnePulse users with all the benefits of Oyster registration. The personal data is passed to TfL after card personalization, using automated processes.

Customers are instructed to contact Barclaycard for payment inquiries and TfL for transit inquiries. For inquiries specifically related to the card itself (e.g., lost or stolen cards), customers contact Barclaycard.

⁷⁹ Additional information on the Barclaycard OnePulse card can be found at <http://www.barclaycard-onepulse.co.uk>.

⁸⁰ Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

Barclaycard's customer service staff direct Oyster-related queries to TfL and vice versa. The bank call-center representatives have no access to transit activity other than to assist a customer in setting up automatic top-up. The transit application itself can be funded by all means currently available for traditional Oyster cards, including cash, debit, and credit.

Card replacement is handled by Barclaycard. Replacement of outstanding transit balances or products is initiated by Barclaycard and passed to TfL, who uses the ad-hoc load facility to load balances or products onto a replacement card.

TfL has also stated that it hopes to be accepting open payment debit, credit and prepaid bank cards directly at the underground gates and onboard buses and trams and trains by 2011.⁸¹

8.2.4 Hong Kong Octopus Card⁸²

The Hong Kong Octopus card, launched in 1997 as an electronic purse for public transportation. The card's acceptance and popularity have since extended its use to nearby retailers.

Octopus cards were developed as an automatic fare collection (AFC) scheme for Hong Kong's transit system. Over 19 million Octopus cards have been issued, with 95% of Hong Kong residents (aged 16 to 65) using Octopus, and over 10 million transactions are processed daily, valued at HK\$85 million.⁸³ The Octopus system currently includes all of the major transport operators (bus, taxi, subway, train, tram, and ferry services). Because Hong Kong's main transport operators are all partners in the Octopus card, kiosks are widely available, making it easy for customers to check the balance on a card and recharge it with cash or electronic payments. The use of the card has shortened queues at ticket barriers, because the card doesn't have to be taken out of a bag or wallet — customers can just wave it past a scanner at a distance of several centimeters.

The first non-transit applications for the Octopus card allowed the card to be used for payment at photo booths located in the Mass Transit Railway (MTR) stations and pay phones operated by New World Telephone.

The Octopus system currently includes public transportation services, apparel stores, bakeries, car parks, cinemas, convenience stores, fast food chains, household stores, leisure facilities, personal care stores, photo finishing stores, photocopiers, supermarkets, and vending machines. Octopus cards are also used on school campuses and at residential and office facilities also use Octopus for building access control.⁸⁴ Approximately 25% of all payment transactions are non-transit.⁸⁵

1.5 million people are using account-linked payment, where the value is maintained in a back-end system and charges are billed to the individual's credit card.⁸⁶

An Octopus Rewards program is also offered where registered card holders get a 0.5% value bonus on each purchase in the retail environment. Retail payment does not have to be via Octopus as rewards can be earned with cash, credit, or Octopus payment methods. Over 1 million patrons are signed up and there are ten participating merchants including McDonalds, Wellcome, UA Cinemas, and Fotomax. Registered cards must be personalized. About 20% of active cards are registered/personalized.⁸⁷

The contactless Octopus card is based on Sony's FeliCa™ technology, a proprietary 13.56 MHz technology similar to but not compliant with the ISO/IEC 14443 standard. This technology has widespread acceptance in the Asia Pacific region, with over 25 million cards issued worldwide, according to JCB International Credit Card Company. Terminals read the cards instantly, processing transactions in less than one-third of a

⁸¹ "Transport for London," NFC Times, November 12, 2009

⁸² "Hong Kong Octopus Card," Smart Card Alliance profile, 2005, with updates from Cubic and Octopus web site

⁸³ <http://www.octopuscards.com/consumer/general/global/en/aboutus.jsp>

⁸⁴ <http://www.octopuscards.com/consumer/payment/use/en/index.jsp>

⁸⁵ Source: "APTA Trade Mission-Asia Smart Card Tour," David deKozan, Cubic

⁸⁶ Ibid.

⁸⁷ Ibid.

second. On the MTR, a scanner at the ticket barrier loads data on the card that is then used by scanners at the exit gates to deduct the correct fare and show the remaining credit.

In 2002, the Asia Pacific Smart Card Association reported that 95% of the “economically active population” was using the Octopus card. Travelers have found that the card provides increased convenience, allowing them to pass through fare collection points 15 to 20% faster, according to Octopus card statistics. The scheme has succeeded because it offers real convenience to cardholders.

8.3 Parking⁸⁸

This section profiles two different parking programs, one in Washington, DC and one in Israel, each of which implements a different smart card-based payment model.

8.3.1 Washington Metropolitan Area Transit Authority

As described in Section 8.2.1, WMATA has been using a contactless transit fare payment card, SmarTrip, since 1999.

WMATA is also the largest parking operator in the region, with over 55,000 parking spaces at 35 subway stations, including both surface lots and parking garages. Throughout most of WMATA’s operating history, parking operations have been handled through third parties. WMATA has been using SmarTrip for the subway and for parking since May 1999.

The subway and bus contactless smart card fare collection systems are tightly controlled and provide both revenue and a wealth of information about passengers. In contrast, the WMATA parking facilities were viewed as losing large amounts annually; cash was the primary way customers paid for parking. As a result, in early 2004 the WMATA Board of Directors decided to shift the direction of parking operations and institute cashless parking at all WMATA lots, effective June 27, 2004. This gave WMATA staff about 120 days to replace the parking lot attendants and the existing payment infrastructure.

8.3.1.1 SmarTrip Dispenser Introduced

To handle the problem of card availability and distribution, WMATA contracted with Lexis Systems (now Cubic Parking Systems, a new business unit for Cubic Transportation Systems) to purchase 55 card dispensers to be placed in each Metrorail station that had parking facilities. Several stations with large parking facilities received multiple devices to assure sufficient sales capacity. The dispensers are equipped with bill validators and accept \$1, \$5, \$10, and \$20 bills. They do not escrow bills, give change, or issue receipts. The devices accept Visa, MasterCard, Discover, and American Express credit cards with zip code verification. They also accept debit cards and require authentication with the cardholder’s personal identification number (PIN).

⁸⁸ Source: *Smart Cards and Parking*, Smart Card Alliance white paper, January 2006



Figure 14. Smart Card Dispensers

Patrons who park in a WMATA lot are required to use a SmartTrip card to exit the parking facility. Fees are collected until midnight or until the facility closes. The card is preloaded with \$5 of value and sold for \$10 in Metrorail stations with parking lots. Cards can also be purchased from three dispensers at the Metrorail sales office at the Metro Center station.

8.3.1.2 No-Cash Policy

The Metrobus system became fully SmartTrip capable in August 2004. By June 2004, WMATA had issued in excess of 500,000 smart cards. Card issuance was handled primarily by three transit store sites, the Internet, tables in stations, and a bank lockbox.

The SmartTrip card base increased from 700,000 to 1.2 million between 2004 and 2005. Cards sold using the card dispensers accounted for 80% of the increased sales; store sales dropped to 15% of total sales. Station dispensers sold as many cards in a single year as were sold in the previous 5 years.

8.3.1.3 Reserved Parking

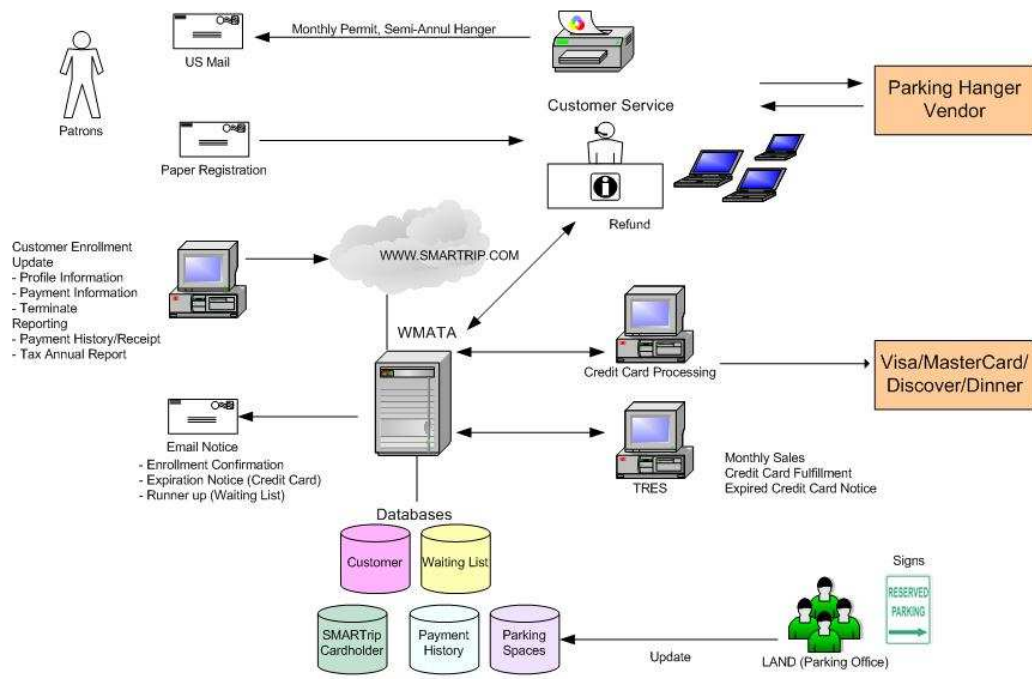
The WMATA parking contractor was also operating a monthly reserved parking program for about 5,000 daily users. Each reserved parking patron received a mirror hanger and a monthly payment sticker to display when the patron parked at an assigned reserve space at the designated facility. Patrons paid \$90 per month and exited without additional payment. This approach represented potentially missed revenue.

Under the new system, customers pay a monthly premium of \$45 for reserved parking but must also pay a daily fee when they exit the lot. The reserved parking patron is guaranteed a spot until 10 AM, at which time any unused reserved spaces are opened to the general public. Parking is free on weekends and Federal holidays.

To accommodate the contractor's reserved parking program, WMATA used their existing web site to host patron enrollment and support internal lot administration. Between the 10th and 15th of the month, a reserve parking permit subscriber's credit card is charged and a sticker is mailed out for the hang tag. There are approximately 5,000 such subscribers, representing about 10% of the spaces available. Approximately 500 people pay by check. WMATA is considering discontinuing check acceptance.

Figure 15 illustrates how the reserve permit system works.

Washington Metropolitan Area Transit Authority
Monthly Reserve Permit Parking Data Flow Diagram



WMATA ITSV Application Branch Software Engineering 2004

Figure 15. WMATA Reserve Permit Data Flow

8.3.1.4 One-Time Visitors

While many lots are at or near capacity daily (90% system wide), spaces remain available. Utilization rates remain fairly consistent through the year, with tourists filling in for local residents who are on vacation. About 50% of the current patrons who buy a SmartTrip card through the dispenser use it only once. Many presumably find the park-and-ride fee of \$10 reasonable for the Washington, DC, area.

Since WMATA continues to pay over \$3 per card for card stock and the card must be handled prior to sale, WMATA is anticipating the introduction of limited-use paper-based contactless cards. One-time visitors often react very negatively to paying \$5 just to obtain a zero value card, although this reluctance can often be overcome when the visitor receives an explanation of how to use the card. WMATA is in the process of evaluating limited use (previously called disposable) smart cards to reduce the cost for one-time visitors.

The system experiences 400–500 non-payer transactions per day ($\leq 1\%$), where the patron does not have a card when arriving at the exit gate. Each non-payer receives a form and payment can be made to a bank lockbox.



8.3.1.5 Conclusions

WMATA was in a unique position to move to cashless parking as a result of its substantial investment in contactless smart card technology. Nevertheless, adoption of cashless parking constituted a significant risk to the SmartTrip card program. WMATA's move to cashless parking has been a success: shrinkage in cash collections is no longer a factor. SmartTrip card distribution through dispensers has resulted in

dramatic growth in card ownership and use. Web site applications allow staff and users to manage parking program spaces more efficiently.

Table 5 summarizes the situation before and after WMATA implemented this system.

Table 5. Comparison of Parking Payment Before and After Smart Card Implementation.

Early 2004 System (Cash and Smart Cards)	Late 2004 System (Smart Cards Only)
<ul style="list-style-type: none"> • Fees collected in cash on exit by the contractor at parking kiosks • Kiosks open weekdays from 2–10 PM • Reserved parking spaces paid monthly in advance; \$90 for a hang tag and monthly sticker; space reserved until 10 AM weekdays • No exit fee collected from reserved parkers • More than 95% of all patrons registered their cards to insure replacement if lost or stolen 	<ul style="list-style-type: none"> • SmarTrip required for payment at all Metro parking facilities • Parking fees collected from 9 AM to closing each business day • Card dispensing machines in all stations with parking and at Metro Center station • Contract employees assist customers and monitor transaction process at SmarTrip readers (but do not handle cash) • Reserved parking fee reduced to \$45/month, but now exit fee must be paid (daily \$3.50 to \$4.00 fee upon exit) • Registration dropped to 55% of card base
<p>Cashier Lane</p>  <p>Express SmarTrip Lane</p>	 <p>Contract employees assist customers and monitor transaction process.</p> 

8.3.2 Parking Operations in Israel

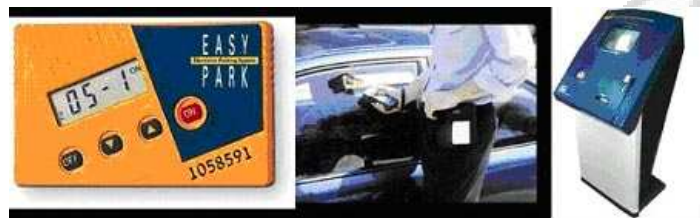
Israel has implemented a nationwide parking application called EasyPark that uses one card to pay for parking anywhere in the country. Previously, on-street parking in Israel was paid for using a municipal punch card that was available for purchase in local kiosks. EasyPark was an ideal solution for this environment. Drivers simply activate a contactless in-vehicle parking device (card) when they park and display it in the card window (see Figure 16). When they return to the car, they turn off the device. Drivers are no longer required to obtain individual parking punch cards for every city, and they pay only for the exact amount of time parked, whether it is an hour or only 10 minutes. The card includes a built-in screen that displays payments and remaining balances.

The EasyPark card is sold in post offices; value reload stations are available in post offices and gas stations. The system is currently fully operational, with 250,000 subscribers using it in 30 different parking zones across the county. (Parking zones can be different areas of a city in which it costs different amounts to park, or time periods, which can be classified as subzones, or even entire cities.) The EasyPark application can manage up to 60,000 parking zones. A total of 30 zones have been assigned to date.

In addition, residents use a residential parking permit to park in their neighborhoods. This permit is renewed annually and is automatically updated once the annual fee is received by the parking authority participating in each city/zone.

Municipal and private parking lots can participate if they choose. EasyPark's parent company, OTI, compensates the 30 parking authorities according to usage. OTI EasyPark manages the system for the parking authorities for a negotiated transaction fee. OTI implemented a business model of generating revenues from product sales as well as transaction fees and customer support. This business model shares the risk and success of the project between municipal parking authorities and vendors, reducing the risk for both entities.

Figure 16. Easy Park System Components



EasyPark card (left), a hand-held terminal (center), and a loading station.

8.3.2.1 System Characteristics

The EasyPark card and the residential parking permit use ISO/IEC 14443-compliant smart card chips. The parking authority needs to acquire only the enforcement reader/printer and loading stations; no other on-street devices are required.

The value loading stations are kiosks or POS-type devices deployed in retail locations, gas stations, or postal facilities. They are clearly identified as loading stations and placed strategically throughout each zone. Each parking authority decides on the number and location of the stations. Reloading is accomplished using credit/debit cards. The stations can be outfitted with bill acceptors at the discretion of the parking authority.

Over-the-counter attended POS devices could also be used as loading stations. In Israel, however, a totally unattended, cashless system is being used, further reducing cost to the parking authorities.

8.3.2.2 Customer Benefits

EasyPark provides customers with the following benefits:

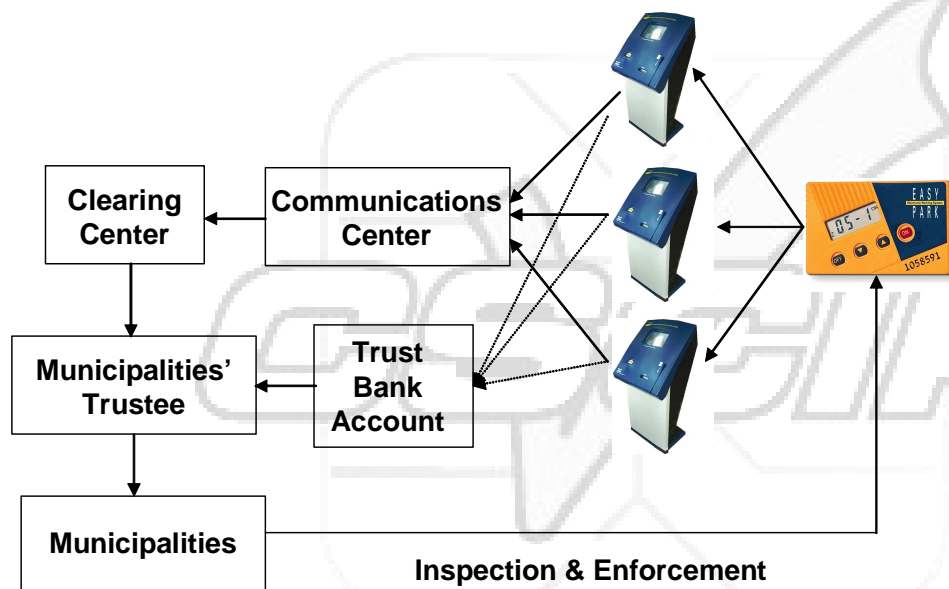
- The customer pays only for exact time used.
- The device is simple to operate.
- There is no need to leave the vehicle to pay for parking or search for coins for a meter.
- The system provides a receipt and proof of payment/parking.
- The system can be reloaded in convenient retail locations and gas stations using cash or credit or debit cards.

8.3.2.3 Municipality Benefits

EasyPark provides the municipality with the following benefits:

- The system provides higher income, which is distributed proportionally among parking authorities for actual usage in each city/zone.
- Minimal initial investment is required.
- EasyPark operates in parallel with other systems.
- The prepayment principle provides float.
- The system is tamper-proof, reducing losses from meter break-ins.
- The system is eco-friendly—there are no pay-and-display tickets or unsightly meters.
- Using EasyPark creates a positive, progressive image for the municipality.
- A parking monitor can check a larger number of vehicles per shift.

Figure 17. Easy Park System Diagram



9 Relevant Standards and Specifications

Numerous standards are relevant to smart card applications and more are created every year. They have various impacts at different levels of a smart card based-system and may deal with physical characteristics, security certifications, transmission protocols, and application loading or design. There are also industry "specifications," which are not "standards," but which play a very important role in smart card applications. Not all application specifications are listed in this section, though some of the important industry-focused applications are included.

Standards are voluntary, but are generally adhered to in the interest of achieving conformity and interoperability. A brief synopsis of the various smart card standards and specifications is included in this section. Additional information can be found in the body of work referenced with each smart card standard or specification.

ISO/IEC is the worldwide standard-setting body for technology, including plastic cards. These standards set minimums, but also include many options and tend to leave some issues unaddressed. As a result, conformance to ISO standards alone does not necessarily ensure interoperability – nor does it ensure that cards and terminals built to the specifications will interoperate. The main standards that pertain to smart cards are ISO/IEC 7810, ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 24727 and ISO/IEC 7501.

The following should be noted:

1. Some standards listed below are available free of charge, but many must be purchased.
2. Some standards may not be listed in this section, but could be relevant to a specific application or a specific technique required by an implementation (e.g., standardized format of a biometric information).

This section contains a list of standards and specifications relating to this module. A more complete listing of standards and specifications, with descriptions of each, can be found in Module 1.

9.1 Standards Relevant to Smart Card Physical Characteristics

- ISO/IEC 7810 – Identification Cards – Physical Characteristics
- ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards⁸⁹

9.2 Standards Relevant to Technologies Which Could Be Found on a Smart Card

Smart cards often include other technologies in the card body. The following standards apply to common technologies:

- Magnetic stripes: ISO/IEC 7811 series, Identification cards – Recording technique
- Linear bar codes: ISO/IEC 15416 Information technology – Automatic identification and data capture techniques – Bar code print quality test specification – Linear symbols
- PDF417 bar code: ISO/IEC 15438 Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification
- Optical memory cards: ISO/IEC 11693 Identification cards – Optical memory cards; ISO/IEC 11694 Identification cards – Optical memory cards - linear recording method

⁸⁹ Source: <http://www.iso.org>

9.3 Standards and Specifications Relevant to Technologies Related to the Card Interface

- ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards with Contacts
- ISO/IEC 14443 – Contactless Integrated Circuit Cards – Proximity Cards

9.4 Standards and Specifications Relevant to the Card Commands and Application Data Structures

- ISO/IEC 7816 Series – Identification Cards – Integrated Circuit(s) Cards with Contacts
- GlobalPlatform⁹⁰
- Java Card⁹¹

9.5 Standards and Specifications Relevant to Issuers or Specific Industry Sectors

- ISO/IEC 7812 Series, Identification Cards – Identification of Issuers
- ISO/IEC 7813, Identification Cards – Financial Transaction Cards
- ISO/IEC 7816 Series, Identification Cards – Integrated Circuit(s) Cards with Contacts
- ISO/IEC 8583 – Financial Transaction Card Originated Messages – Interchange Message Specifications
- ISO/IEC 9992 – Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device
- EMV: Integrated Circuit Card Specifications for Payment Systems⁹²
- Common Electronic Purse Specification (CEPS)
- CEN EN 1546 – Identification card systems. Inter-sector electronic purse
- APTA Contactless Fare Media System Standard
- Integrated Transport Smartcard Organization (ITSO)
- Verband Deutscher Verkehrsunternehmen (VDV)

⁹⁰ GlobalPlatform specifications are available at <http://www.globalplatform.org/specifications.asp>

⁹¹ Java Card specifications are available at <http://java.sun.com/javacard/3.0.1/specs.jsp>

⁹² EMV specifications can be found at <http://www.emvco.com>.

10 References

- American Express ExpressPay, <http://www.americanexpress.com/expresspay>
- American Public Transportation Association web site, <http://www.apta.com/>
- Accepting Contactless Payments: A Merchant Guide*, Smart Card Alliance Contactless and Mobile Payments Council white paper, July 2007, <http://www.smartcardalliance.org>
- APTA Asia Fare Collection Study Mission*, Ging Ging Fernandez, Booz Allen Hamilton, presentation, 2009 Payments Councils Summit, February 24, 2009
- APTA Manual of Standards and Recommended Practices for Universal Transit Fare Cards*, <http://www.aptastandards.com/PublishedDocuments/PublishedStandards/UTFS/tabid/191/Default.aspx>
- Banking Payments Pilot: MTA New York City Transit*, Steve Frazzini, NYC Transit, presentation, 2008 Payments Councils Summit, February 28, 2008
- Barclaycard OnePulse card web site, <http://www.barclaycard-onepulse.co.uk>
- Calypso Networks Association web site, <http://www.calypsonet-asso.org/index.php>
- Card Payments Roadmap in the U.S.: How Will EMV and Contactless Impact the Future Payments Infrastructure?*, Smart Card Alliance draft white paper, October 2010
- Co-Branded Multi-Application Contactless Cards for Transit and Financial Payment*, Smart Card Alliance Transportation Council white paper, February 2008, <http://www.smartcardalliance.org>
- Common Electronic Purse Specification (CEP)*, <http://www.irisa.fr/vertecs/Equipe/Rusu/FME02/functionalrequirements6-3.pdf>
- Contactless & Mobile Payments*, Sandy Thaw, Visa presentation, 2009 Payments Councils Summit, February 24, 2009
- Contactless Payments: Frequently Asked Questions*, Smart Card Alliance Contactless and Mobile Payments Council publication, February 2007, <http://www.smartcardalliance.org>
- Discover, <http://www.discovernetwork.com/discovernetwork/discovernetwork.html>
- Dynamic Passcode Authentication: Overview Guide*, Visa publication, <http://www.visaeurope.com/documents/aboutvisa/dynamicpasscodeauthentication.pdf?d=070207>
- Electronic Fare the Future for UTA*, UTA press release, January 2, 2009
- The Electronic Purse*, by John Wenninger and David Laster, Federal Reserve Bank of New York, April 1995
- EMVCO web site, <http://www.emvco.com>
- EMVCo: Creating Global Standards for Proximity Payments*, Brian Byrne (EMVCo) presentation, Smart Card Alliance Annual Conference, May 18, 2010
- EMVCo Common Contactless Terminal Roadmap*, EMVCo General Bulletin No. 43, First Edition, November 2009, November 2009, <http://www.emvco.com/news.aspx?id=46>
- End-to-End Encryption and Chip Cards in the U.S. Payments Industry*, Smart Card Alliance Contactless and Mobile Payments Council position paper, September 2009, <http://www.smartcardalliance.org>
- Evolution of E-payments in Public Transport—Singapore's Experience*, Silvester Prakasam, LTA, Journeys, Nov. 2009, http://www.lta.gov.sg/corp_info/doc/Singapore_Saikou_080901.pdf
- Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud*, Smart Card Alliance Contactless and Mobile Payments Council white paper, October 2009, <http://www.smartcardalliance.org>

Hong Kong Octopus Card web site, <http://www.octopuscards.com/enindex.jsp>

International Organization for Standardization web site, <http://www.iso.org>

Intelligent Transportation Society of America, <http://www.itsa.org/>

International Parking Institute, <http://www.new.parking.org/>

Issuer and Merchant Best Practices: Promoting Contactless Payments Usage and Acceptance, Smart Card Alliance Contactless and Mobile Payments Council white paper, July 2009, <http://www.smartcardalliance.org>

ITSO web site, <http://www.itso.org.uk/>

JCB, <http://www.jcbusa.com/>

MasterCard PayPass, <http://www.mastercard.com/us/personal/en/aboutourcards/paypass/index.html>, http://www.paypass.com/performance_insights.html

National Parking Association, <http://www.npapark.org/>

OneSMART Authentication, MasterCard, https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/cap/index.jsp

Open Payment Standards Approach to Fare Payment: NYCT Pilot Phase II Update, Steve Frazzini, MTA NYC Transit, presentation, Payments Summit 2009, February 25, 2009

Over One Million Barclays Customers Bank Online with Gemalto's Solution in the UK, Gemalto press release, July 9, 2008

PayPass Update: MasterCard PayPass Consumer Benchmark Survey, 2008, Burt Wilhelm presentation, 2009 Payments Councils Summit, February 25, 2009

Serving Unbanked Consumers in the Transit Industry with Prepaid Cards, Smart Card Alliance Transportation Council white paper, June 2008, <http://www.smartcardalliance.org>

Smart Card Handbook, Wolfgang Rankl and Wolfgang Effing, Fourth Edition, John Wiley and Sons, Ltd., 2010

Smart Card Standards 101, William Gostkowski presentation, CTST 2009 Smart Card Technology and Payments Applications Workshop, May 4, 2009

Smart Cards and Parking, Smart Card Alliance Transportation Council white paper, January 2006, <http://www.smartcardalliance.org>

Smart Cards and Payments: Technology, Standards and Transaction, Gilles Lisimaque presentation, Smart Card Alliance webinar, November 18, 2008

Smartcard Interoperability Issues for the Transit Industry, Transit Cooperative Research Program, TCRP Report 115, 2006, http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_rpt_115.pdf

'Smart' parking meters catching on across U.S., USA Today, February 24, 2009

Transit and Contactless Financial Payments: New Opportunities for Collaboration and Convergence, Smart Card Alliance Transportation Council white paper, October 2006, <http://www.smartcardalliance.org>

Transit and Retail Payment: Opportunities for Collaboration and Convergence, Smart Card Alliance Transportation Council white paper, October 2003, <http://www.smartcardalliance.org>

Transit Payment System Security, Smart Card Alliance white paper, August 2008, <http://www.smartcardalliance.org>

TransLink Program Update, David Weir, Metropolitan Transportation Commission, presentation, 2009 Payments Councils Summit, February 25, 2009

UTA Electronic Fare Collection System: Development Progress Report, Craig Roberts, UTA, presentation, 2009 Payments Councils Summit, February 25, 2009

Verband Deutscher Verkehrsunternehmen (Association of German Transport Undertakings – VDV) web site, <http://www.vdv.de/en/index.html>.

Visa payWave, <http://usa.visa.com/personal/cards/paywave/index.html>, http://usa.visa.com/personal/cards/paywave/issuers_offering.html, <http://usa.visa.com/paywave-merchants/>

Visa TAP Co-Branded Card, Jane Matsumoto, LACMTA, presentation, 2009 Payments Councils Summit, February 24, 2009

Washington Metropolitan Transit Authority (WMATA) SmarTrip, <http://www.wmata.com/fares/smartrip/>



11 Acknowledgements

This document was developed by the Smart Card Alliance for the Certified Smart Card Industry Professional (CSCIP) program. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks **David deKozan, Cubic; Willy Dommen, Booz Allen Hamilton; Greg Garback, WMATA; Simon Hurry, Visa, Inc.; Ken Indorf, CardLogix; Gilles Lisimaque, Identification Technology Partners;** and **John Rego, OTI America** for their review of this CSCIP module.

The Smart Card Alliance thanks: **David deKozan, Cubic**, for contributing content for Section 6.1 *Transit* and Section 8.2 *Sample Transit Smart Card Payment Models*; **Guy Berg, Collis America**, for contributing Section 4.1, *EMV*; **Gilles Lisimaque, Identification Technology Partners**, for contributing Section 5, *E-purse and Stored Value Cards*; and **Willy Dommen, Booz Allen Hamilton** for contributing the introduction to Section 2, *Smart Card Market Drivers and Benefits for Payments and Financial Transactions*.

The Smart Card Alliance wishes to thank the many current and past members of the Smart Card Alliance Councils and Task Forces who contributed to the development of the white papers and reference material that was used to create this module, including:

ACS	Gemalto	Power2Process
American Express	Giesecke & Devrient	Ready Credit Corporation
American Public Transportation Association (APTA)	IBM	Scheidt & Bachmann
Arby's Restaurant Group	IfD Consulting	Smart Commerce, Inc.
Ascom	Infineon Technologies	Taipei Smart Card Corporation
ASK Contactless	INSIDE Contactless	Thales Transportation Systems
Bank of America	JPMorgan Chase	Transport for London
Barclays	Keane	TranSys
Booz Allen Hamilton	MacKay Meters Inc.	Tri-County Metropolitan Transportation District of Oregon (TriMet)
Capital One	MasterCard Worldwide	U.S. Department of Transportation/Volpe Center
Chase	MBTA	USA Technologies
City of Portland, Oregon	METRO/SORTA	Utah Transit Authority (UTA)
Collis America	Metropolitan Transportation Commission (MTC)	VeriFone
Cubic Transportation Systems, Inc.	MTA New York City Transit	Visa, Inc.
Datacard Group	Oberthur Technologies	ViVotech
Discover Financial Services	OTI America	Washington Metropolitan Area Transit Authority (WMATA)
Douglas Holdings	Parcsmart Technologies, Inc.	
EDS	Parsons	
ERG Group	PBS&J	
First Data Corporation	PepperCoin	

Special thanks go to all of the individuals who worked on the development of the white papers and reference material, including:

Karim Aboud	Alfred Dagher	Jennifer Hale	Chris Marconi	John Rego
Zoltan Ambrus	Doug Deckert	Duke Hanson	Josh Martiesen	Craig Roberts
Dave Andrews	Joe Defilippo	John Hill	Boris Masip	James Russell
Jake Avidon	David deKozan	Simon Hurry	Ellis McCoy	Robert Sadeckas
Nancy Baunis	Tom Delaney	Linh Huynh	David McIlwraith	Keith Saunders
Deborah Baxley	Jean-Marc Delbecq	Ashok Joshi	Cathy Medich	Martin Schroeder
Bob Beer	Sunil Dewan	Will Judge	Manny Menard	Garfield Smith
Guy Berg	Gwen Dido	Mansour Karimzadeh	Bob Merkert	Chandra Srivastava
Ted Bergh	Jim Diezemann	Mohammad Khan	Mike Merringer	Brian Stein
Troy Bernard	Mike Dinning	Dana Klaboe	Chuck Meyer	David Stone
Rachana Bhatt	Willy Dommen	Paul Korczak	Jason Mondanaro	Tim Walsh
Beth Bitetto	Brian Douglas	Mike Kutsch	Leisa Moniz	Charles Walton
Brent Bowen	Ian Duthie	Michael Laezza	Brian Monk	Gavin Waugh
Matt Byrne	Kerri Flanagan	Paul Legacki	Ben Morris	Mike Weekes
Michael Cariou	Steve Frazzini	Philippe Levy	Richard Mould	Timothy Weisenberger
Jean-Charles Caulier	Greg Garback	Marcelo Lima	Mike Nash	Burt Wilhelm
Chuck Chagas	Jennifer Garcia	Cyber Lin	Adam Nelson	Pamela Zuercher
Greg Chauvin	Regina Gaston	Dan Loomis	Tomas Oliva	

Sri Chawla
Chris Cipperly

Adam Gluck
Sydney Green

John MacKay
Kim Madore

Ron Pinkus
JC Raynon

About LEAP and the CSCIP Program

The Smart Card Alliance Leadership, Education and Advancement Program (LEAP) was formed to: offer a new individual members-only organization for smart card professional; advance education and professional development for individuals working in the smart card industry; manage and confer, based on a standardized body-of-knowledge examination, the Certified Smart Card Industry Professional (CSCIP) designation.

LEAP members who wish to achieve certification as experts in smart card technology may do so at any time. Certification requires that LEAP members meet specific educational and professional criteria prior to acceptance into the certification program.

A series of educational modules forming the CSCIP certification body of knowledge has been developed by leading smart card industry professionals and is updated regularly. These educational modules prepare applicants for the multi-part CSCIP exam administered by the Smart Card Alliance. The exam requires demonstrated proficiency in a broad body of industry knowledge, as opposed to expertise in specialized smart card disciplines. Applicants must receive a passing grade on all parts of the exam to receive the CSCIP certification.

LEAP membership in good standing is required to sustain the certification, and documentation of a required level of continuing education activities must be submitted every three years for CSCIP re-certification.

Additional information on LEAP and the CSCIP accreditation program can be found at <http://www.smartcardalliance.org>.

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.