

# white paper

AN INDUSTRY  
PRIMER ON  
SMART CARDS

---

PRESENTED BY THE  
TECHNOLOGY COMMITTEE OF  
THE ELECTRONIC TRANSACTIONS  
ASSOCIATION AND DEVELOPED  
IN COOPERATION WITH  
FIRST ANNAPOLIS CONSULTING  
OCTOBER 2001



# **ABOUT THE ELECTRONIC TRANSACTIONS ASSOCIATION**

The Electronic Transactions Association (ETA) is an international trade association representing companies offering electronic transaction processing products and services to merchants within the acquiring industry. Members include financial institutions, independent sales organizations, and manufacturers/distributors of software, equipment, and point-of-sale devices. ETA was established in 1990 to influence policy within the industry by providing leadership through education, advocacy, and the exchange of information.

## **ACKNOWLEDGEMENTS**

Deborah Arnold, Vice President, Integration Technologies, Visa International

Jim Brannon, Worldwide Card Program Manager, Unysis Corporation

Lori Breitzke, Regional Marketing Manager, VeriFone, Inc.

John Cawthorne, Product Director, First Data Merchant Services

Michael Cottrell, Vice President, Market Strategies, Vital Processing Services

Liz Farnsworth, Vice President, Smart Card Applications, Visa U.S.A., Inc.

Patrick Gauthier, Senior Vice President, Smart Card Applications, Visa U.S.A., Inc.

Alan Goulet, American Express

Michelle Graff, Delivery Marketing, VeriFone, Inc.

Joan Hennessey, Vice President, E-Business Leader, North America Acceptance, MasterCard International

Karin Frederiksen Long, Marketing Services Manager, Rite Aid Corporation

John Powell, US Wireless Data, Inc.

Art Roca, Vice President, North America Acceptance, MasterCard International

Barbara Straw, Director of Disbursing/ATMs at Sea Program, Naval Supply Systems Command

George Wallner, Chairman, Hypercom Corporation

Chuck Wilson, Consultant & Author

---

**ETA TECHNOLOGY COMMITTEE**

Sean Riley, Committee Chair & Senior Director, Paymentech, Inc.

Brent Bowen, President, Transaction Payment Systems

Steve DeFeo, Vice President, Commerce Bank

Connie Festa, New Business Development Consultant

Rick Lenz, Acquiring Services Manager, Metavante Corporation

John Mayleben, Director of Sales, Michigan Retailers Association

Vidya Ravichandran, Director, E-Business Development, NPC

James Richards, Chief Technology Officer & Senior Vice President, CardSystems, Inc.

Forrest Sealy, Vice President of Technical & Merchant Support, Retriever Payment Systems

Marc Shultz, Vice President, Business Development, U.S. Wireless Data, Inc.

---

# CONTENTS

CONTENTS .....	3
OVERVIEW.....	5
SMART CARD PRIMER.....	6
SMART CARD DEFINED.....	6
SMART CARD MEMORY .....	6
INTELLIGENT VS. MEMORY CHIPS .....	6
SINGLE VS. MULTI-APPLICATION CHIPS .....	7
OPERATING SYSTEMS .....	7
SMART CARD STANDARDS AND INTEROPERABILITY .....	7
EMV COMPLIANCE .....	8
SMART CARD PAYMENT PROCESS .....	8
SMART CARD BENEFITS .....	10
SECURITY BENEFITS AND FEATURES .....	10
MULTIPLE APPLICATIONS .....	10
IMPROVED FRAUD PROTECTION.....	11
U.S. ENVIRONMENT.....	13
INITIAL U.S. PILOTS .....	13
CURRENT SITUATION FOR CARD ASSOCIATIONS .....	14
CURRENT SITUATION FOR CARD ISSUERS .....	15
REASONS WHY ISSUERS ARE MOVING AHEAD WITH SMART CARDS .....	17
CURRENT SITUATION FOR MERCHANTS .....	18
CURRENT SITUATION FOR MERCHANT ACQUIRERS, ISOS, AND VENDORS .....	18
CURRENT SITUATION FOR SMART CARD CLOSED SYSTEMS .....	19
GLOBAL MARKET PLACE .....	21
EUROPE.....	21
LATIN AMERICA .....	22
CANADA.....	22
ASIA PACIFIC REGION .....	22
SMART CARD APPLICATIONS AROUND THE GLOBE.....	22
KEY CHALLENGES FOR THE SMART CARD .....	24
CONCLUSION .....	25
GLOSSARY OF SMART CARD TERMS .....	26



---

# OVERVIEW

The recent issuance of smart cards in the U.S. by American Express, FleetBoston, First USA, Provident, along with Target's announcement that the national retailer will offer a Visa smart card has consumers and the payment industry wondering if smart cards will soon become the payment method of the future. These cards, with their imbedded microchip processor promise to add great convenience and security to consumers and will be able to perform several functions besides being a credit or debit card. Other uses and benefits include security access, data and money storage, and loyalty programs. Smart card proponents believe that the card will one day replace all cards in our wallets today and maybe even eliminate the need for a card at all. For example, the chip could be stored in cell phones, computers, personal data assistants (PDAs), or some other platform device.

Despite the card's introduction and its many potential benefits, several key issues must be addressed before smart cards become a common fixture in the U.S. Some of these issues include developing the infrastructure for the various smart card applications, getting merchants to upgrade their POS systems and accept chip cards, getting the cards into a sufficient number of consumers' wallets, and developing the critical mass required to generate profitability for issuers, acquirers, and vendors. Moving to smart cards requires a considerable investment and many issuers, merchants, acquirers, and ISOs are spending significant time trying to determine whether this fits with their business plan and strategic goals. Presently, only a few merchants have committed themselves to upgrading their POS systems to be

smart card capable, with Target and Wakefern Food Corporation being two of the largest.

The microchips that are being imbedded on today's smart cards offer little functionality, except in cases where the card is utilized for purchase authentication over the Internet. A key hurdle for the smart card is its ability to offer significantly more benefit than the current mag-stripe technology does today.

Today's smart cards offer credit, debit, and stored value as primary features – all features that the mag-stripe card offers efficiently and inexpensively, albeit not on the same card. The key for smart card ubiquity in the U.S. will be its ability to deliver other value-added features beyond the conventional magnetic-stripe card.

This paper explores the realities of the smart card, its potential benefits and challenges in the U.S. This paper also provides:

- A brief primer on the smart card and its functionality;
- Key events, trends, and movements taking place in the smart card arena;
- An explanation of why moving to smart cards in the U.S. is not easy, despite the card's popularity outside of the U.S.; and
- Recommendations on what actions the acquiring and ISO community should consider in order to prepare for smart cards.

This paper primarily focuses on smart cards used in an open system environment in a payment context, and for purposes of this paper, only provides a snapshot of smart card usage in closed, specialty applications such as the government, universities, and corporations.

---

# Smart Card Primer

## Smart Card Defined

A **smart card**<sup>1</sup> is a plastic card with an imbedded integrated circuit computer chip (i.e., a piece of thin, semiconductor material, such as silicon) that has been chemically processed and etched with a specific set of electrical characteristics such as circuits, storage, and logic elements. When coupled with a smart card reader, this combination has the processing power to perform complex operations previously requiring a personal computer or other larger device.

In the form of a credit card, a smart card contains a built-in chip. The chip memory stores payment information similar to the magnetic stripe, but may also include additional information such as issuer-defined controls (e.g., on-line authorization frequency requirements, floor limit, credit limit, etc.). For the foreseeable future, most chip cards issued in the United States will also include an embossed sixteen-digit account number and a mag-stripe. The non-chip features allow the card to be used at storefronts that are not equipped to interact with smart chips. Smart cards can also be “contactless”, meaning the chip transfers data via a built-in antenna without physically touching the smart card reader.

On the chip are software applications designed for security and to process the transaction. Additional applications or information may be added by the issuing bank, or potentially the cardholder, such as a loyalty program, a stored value application, an e-ticket application, or a secure access verification program. When the smart card is used to transact payment, it often requires a PIN to authenticate the user (governed by the card associations). Unlike at an ATM, the PIN entered by the user is authenticated by the security system resident on the chip. Today’s on-line debit and ATM networks authenticate the PIN entered by the cardholder using a back-end network since the PIN is not stored on debit/ATM cards.

---

<sup>1</sup> Smart cards are used extensively outside of the payment industry for a variety of purposes such as identification and access control, healthcare records storage, and other data retention. However, this paper focuses on smart cards as they relate to the payment industry.

## Smart Card Memory

Smart chip memory ranges in capacity and capabilities, similar to a personal computer hard drive. The capacity of the smart chip dictates the number of non-payment related applications that can be stored on the chip. In circulation today in the U.S. are bankcards with smart chips ranging from 8K to 32K. This refers to the number of kilobytes of Electrical Erasable Programmable Read Only Memory (“EEPROM”) available on the chip (i.e., non-volatile memory that can be stored or deleted after the manufacture of the chip via electric charge as often as needed.) Payment transaction information, as well as some applications and cardholder information are stored in the EEPROM. Conversely, the Read Only Memory (“ROM”) (i.e., non-volatile memory that is written to once, usually during chip production) is used to store a majority of the applications and cardholder information that cannot be changed. ROM is also utilized to store the operating system and algorithms employed by the microprocessor during transactions.

## Intelligent vs. Memory Chips

Generally speaking, smart card chips can be categorized as either **intelligent** chips or **memory** chips. Intelligent chips contain a microprocessor that has various read/write capabilities (e.g., EEPROM and ROM space), and the chip actually interacts with the smart card reader using software applications stored on the chip. Conversely, memory chips lack processing capability and don’t manage files dynamically. The smart cards currently issued by bankcard issuers in the U.S. for payment contain intelligent chips. For example, a memory card would be an access control application where the chip authenticates the cardholder and provides the user with access to a previously locked door or a computer network. Information on the chip is read from a card reader, and the chip is designed so that information conta

---

ined cannot be changed. As it relates to the payments industry in the U.S., the role of memory chips will probably be limited to gift and stored value<sup>2</sup> cards.

### Single vs. Multi-Application Chips

There are two types of intelligent smart cards that exist in the marketplace today, **single-application** smart cards and **multi-application** smart cards.

Single-application smart cards are designed for one use, such as the storage of an electronic purse application used to house money and the PIN for a re-chargeable stored value card.

Currently, over 99% of the smart cards in the global marketplace are single-application, most of which exist outside of the payments industry. The **Visa Cash** smart card used in several U.S. pilots is an example of a single-application chip.

Multi-application smart cards provide the ability to perform multiple functions on the same chip. A typical financial services multiple application smart card could include all of the following on the same chip:

- Payment facilitators such as credit, debit, and/or stored value, potentially combined with an e-wallet;
- Loyalty and rewards programs; and
- Information storage such as a driver's license or insurance data, and healthcare information.

In general, multiple application cards require greater memory and faster processing speeds. They tend to be more expensive than single payment cards because they offer more functionality. It is the multi-application card, not the single purpose card that holds so much promise in the U.S. payments industry.

### Operating Systems

An operating system for a smart chip is similar to a personal computer, meaning it controls the execution of the applications. The primary difference with a smart chip is that the operating system is programmed into the ROM portion of the chip at the time of manufacture, and cannot be altered. The leading operating system today is

**Java**, with **MULTOS** and **Windows for Smart Cards** functioning as viable alternatives. Between the operating system and the applications is an Applications Programming Interface ("API"), the message management process through which the operating system and applications interact.

The operating system and breadth of applications on the smart chip are not necessarily important to the merchant and the acquirer, as long as it is an open platform that can interface with the smart card reader and provide payment information to the merchant's POS terminal.

### Smart Card Standards and Interoperability

The global distribution, usage, and interoperability across borders of smart cards will only become reality when standards are globally accepted. **ISO 7816** is the International Standards Organization standard on smart card physical, electrical, and low-level software communication. The standard contains seven parts, published from 1987 through 1998. However, compliance with the standards alone will not ensure interoperability across borders in the fashion experienced by the magnetic-stripe card today.

In 1993, Europay International decided to migrate to smart cards for **credit and debit** transactions in an effort to reduce fraud and make the cards multi-functional. In 1994 Europay, MasterCard and Visa began working together to develop specifications, within the guidelines of ISO standards, for the interface between a smart card and the card reader/terminal for credit and debit payments. Their primary goal was to define a set of requirements to ensure interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the card issuer, or the location of the transaction. Ancillary goals included increased security, promotion of uniform software development, and flexibility. In May 1998 the parties published initial specifications, called **EMV Level 1** for (hardware) and **EMV Level 2** (software). *(It should be noted that EMV specifications apply to credit and debit payment applications only.)* In 1999 the three associations formed EMVCo, LLC to manage, maintain, and enhance the EMV interoperability standards for the smart card industry. The latest version of the specifications, **EMV 2000** version 4.0, was published in December 2000, although testing to that new standard is not expected until January 2002.

---

<sup>2</sup> A payment card that contains electronic money, generally used for low-dollar transactions.

---

While EMVCo worked on developing standards for credit and debit applications, many other groups worked on developing specifications for stored value cards. While a significant portion of Europe was using stored value cards during the 1990's, each scheme was proprietary and incompatible outside of a defined geographic region. Several groups published specifications, although none was adopted as a global standard. In 1998 Visa, American Express and ERG Ltd. invested significantly in the new Proton World International spin-off from Banksys SA, and subsequently adopted **Common Electronic Purse Specifications ("CEPS")** for stored value/electronic purse applications. CEPS is the stored value chip standards equivalent of EMV for credit and debit chips. CEPS has been well accepted due to its open, common specifications that will promote global interoperability and compatibility with EMV specifications. With the exception of MasterCard owned Mondex, virtually all stored value smart card schemes have or are in the process of adopting CEPS, with the eventual goal of global interoperability.

#### EMV Compliance

Due to the financial burden associated with excessive fraud and a relatively expensive or unreliable telecommunication system (used for card authorization) in parts of Europe, the Middle East and Africa, the card associations in those regions are requiring members to issue EMV-compliant smart cards by 2005. In addition, merchants will need to upgrade to EMV-compliant POS terminals. Those not compliant throughout the transaction chain will bare the responsibility for any fraudulent transaction that could have been prevented by chip technology.

It should be noted that while many countries around the globe have committed to adopting EMV-compliant smart cards and terminals in the future, it is **not** a requirement in most regions of the world, including the U.S. Therefore, merchants and acquirers in the U.S. are not reacting as swiftly as those in Europe, the Middle East and Africa.

#### Smart Card Payment Process

**Smart Card Purchase in Card Present Environment** – The consumer will hand their smart card to a merchant and the card is inserted into a card reader. The chip contains certain contact points that line up with the reader to transfer information. For cards that have both a

magnetic stripe and a chip, the card reader may be programmed to utilize the chip technology over the mag-stripe since the chip is more secure. If the smart card contains both credit and debit applications, the cardholder must first select a payment method. At this point the smart chip and the card reader communicate to determine several things, such as whether the terminal has on-line authorization capabilities, whether the card is authentic, and processing restrictions, e.g., expiration date. Next, the cardholder must enter a PIN, similar to a debit transaction, to authenticate the cardholder. The chip recognizes whether the PIN is correct, potentially eliminating the need for an on-line authorization.

Once the PIN is correctly entered, the card communicates to the reader the type of risk management checks that the bankcard issuer wants to be performed, such as the floor limit, random on-line processing, and a velocity check that determines whether an on-line authorization is necessary. Next, the terminal requests authorization via the Association network (if necessary)<sup>3</sup>, just like a magnetic stripe card. Upon approval, the reader and the chip may exchange additional information such as reward points or e-coupons for the next purchase. This information is then stored on the chip for future use, or could be used for the current transaction.

#### Smart Card Purchase in Internet Environment

– Prior to the initial use of a smart card for Internet shopping, the consumer must first attach a **smart card reader** to his/her computer and install the associated software. During the on-line purchasing process, the merchant's website order form will trigger the installed card reader software to go into action, and the software will request the web user to insert the card into the PC's smart card reader and to enter a password. The smart card validates or authenticates the password and provides the cardholder with an e-wallet, which stores his/her credit card information along with billing and shipping information. With the click of a

---

<sup>3</sup> Due to the increased security of a smart card, it is possible that not all transactions will require an on-line authorization. The bankcard issuer can place authorization parameters on the chip requiring random or periodic on-line authorizations as well as a floor limit.

---

button, the smart card fills the order form with the cardholder's information.

Once the customer confirms the purchase, the transaction is routed to the credit card issuer (or their designate) to authenticate the cardholder/smart card combination (i.e., a digital certificate of authenticity could be sent from the issuer to the merchant). Once authentication is

received from the bankcard issuer, the web merchant requests an authorization through the credit card network (if necessary), and the transaction then flows like a card-not-present transaction. Currently, authenticating the card with the issuer requires software integration between the merchant web site and bankcard issuers, resulting in a limited number of merchants for consumers to choose from.

---

# Smart Card Benefits

The benefits of a smart card over a mag-stripe card include the ability to store thousands of times more data, enhanced reliability, multiple functionality, reduced need for cash, and increased security due to advanced encryption technology resident on the chip. Currently in the U.S., smart cards perform limited payment functions and are primarily used for “*payment authentication*” purposes on the Internet. Specifically, the security features of the smart card enable the card-issuing bank, or a third party, to virtually guarantee to the merchant that a transaction is authentic; however, the merchant still processes the transaction using the 16-digit number. Some issuers are also using the smart chip to store loyalty information, such as the American Express and U.S. Virgin Megastores collaboration, and for electronic authentication to view account information on-line, like the FleetBoston Fusion card provides.

## Security Benefits and Features

The enhancement to security is one of the primary advantages of smart cards over the current mag-stripe card. The cards are tamper-resistant, but not tamper-proof, and they have proven to be difficult to counterfeit. Their storage capacity and processing power accommodates sophisticated security, specifically, encryption algorithms. Several algorithms are available at significantly varying cost to the bankcard issuer, including **Triple Data Encryption Standard**<sup>4</sup> (“3DES”), which is the security system employed on most smart cards issued in the U.S., and **Public Key Infrastructure**<sup>5</sup> (“PKI”), the anticipated future of smart card security. Anti-counterfeit measures

---

<sup>4</sup> An encryption algorithm that uses three separate DES (an ANSI standard that describes a symmetric algorithm for encrypting data) encryptions consecutively with at least two separate keys.

<sup>5</sup> An asymmetric (two key) system using pair of cryptographic keys, one that is private and one that is public. Messages encrypted with the private key can only be decrypted with the public key, and vice versa.

include detection of excessive exposure to light, heat, cold, and voltage, and the prevention of loading applications without authorization. Additionally, smart cards lock access to information after a pre-determined number of failed access attempts. Smart chips can also be combined with biometrics, such as a fingerprint, retina scan or a signature, to further enhance security.

A primary security advantage of the smart card is its ability to house a digital certificate<sup>6</sup> issued by a certificate authority, a third party that verifies the card's authenticity. The existence of the digital certificate, particularly in the case of Internet purchases, is expected to significantly reduce fraud since a third party is verifying the authenticity of a PIN-protected card.

Several issues have slowed the adoption of smart cards in the U.S., including the entrenched mag-stripe infrastructure, lack of standards (until recently), and the cost of a smart card compared to a mag-stripe card. The type of security resident on the chip is one of the key drivers to the cost of the chip, with PKI being the more expensive security. To put this in perspective, the difference in cost between a smart card with PKI and a smart card with 3DES is greater than the cost of a mag-stripe card today. The level of security to put on a chip is a cost/benefit decision that each smart card issuer must contemplate. For merchants and acquirers, chip card readers must be capable of decrypting the various security systems on the smart chip to be able to transact the payment.

## Multiple Applications

Another attractive feature of the smart card is its ability to house multiple applications that provide value to consumers and other parties involved in the payment process. Based on the processing memory capabilities of smart cards discussed earlier, the opportunities for smart cards are seemingly limitless. However, the applications that are the most frequently promoted include the following:

Credit/Debit Application – This application enables secure credit and debit purchases in both a card-

---

<sup>6</sup> A file digitally signed by a certificate authority, i.e., a trusted organization that issues certificates and takes liability associated with the validity of the cardholder's identity.

---

present and card-not-present environment. The payment application used at a POS terminal will entail information similar to that stored on a mag-stripe today; however, the additional security will significantly reduce counterfeiting and provide added risk management capabilities to both issuers and merchants via off-line controls. The bankcard issuer decides the level of security on the chip prior to manufacture, ranging from user ID/password to PKI. Some payment applications include an e-wallet for Internet shopping convenience. For purchases over the Internet, the Card Associations are testing secure payment systems that virtually guarantee to the merchant that the cardholder and card are authentic, a step that will significantly reduce on-line fraud and potentially reduce interchange rates. Today, these payment applications can only be used on the Internet via issuer-partner websites or with EMV-compliant storefront POS terminals.

#### Stored Value Application (also known as e-purse)

– This application provides secure payment for low-dollar purchases at storefronts, on the Internet, and at remote locations, such as parking meters or public pay telephones. Monetary value is stored on the chip and value is subtracted as purchases are made with the card. Stored value mag-stripe cards do exist today. However, they are used primarily as gift cards and pre-paid telephone cards in the U.S.; and require online access to a computer system to monitor the cash value of the card as it is used. Adding chip technology to stored value eliminates the need for significant back-end computing power. Additionally, smart chips can be easily restocked with money, either through an ATM or similar machine, or via the Internet, and have greater security than the stored value mag-stripe cards in circulation in the U.S. today. Outside of the U.S. the stored-value smart card is very popular.

Loyalty Application – The application that is expected to benefit the merchant and the consumer and drive smart card acceptance is a loyalty application in which consumers receive rewards and discounts in return for their loyalty to a merchant or group of merchants. The retailer receives the benefit of gathering consumer behavior information that can be analyzed and used to help manage the business and inventory more efficiently. A loyalty application is fairly easy to design and is based on counting and tallying occurrences such as dollars spent, number of visits, and items purchased. Because the concept is simple, the application requires little memory

and is easy to add on to today's popular chip sizes (i.e., 8K, 16K, 32K, and 64K).

Several card-based and paper-based loyalty programs are in place now in the U.S., but the primary advantage of the smart card is its ability to offer immediate, real-time, and off-line redemption to consumers. The chip's off-line memory storage capability is portable across disjointed networks such as independent distribution channels, storefronts, or between different merchants. This feature allows the application to be used for multi-merchant loyalty programs. Another benefit of the smart card is the opportunity to download e-coupons from the point-of-sale terminal or through the Internet, eliminating the need for consumers to cut, sort, and organize coupons, and for merchants to manage a paper coupon redemption process.

#### Improved Fraud Protection

For the past thirty years, fraud has not been a significant issue in the card-present environment in the U.S due to the country's reliable, low-cost telecommunications system that enables merchants to authorize all transactions without having to utilize a floor limit. However, it is in the card-not-present environment where purchases over the Internet and phone make up a disproportional share of disputes and chargebacks. According to Visa and MasterCard, card fraud is estimated at 6 cents for every \$100 spent, and in the Internet environment fraud is estimated at 80 cents for every \$100 spent. Smart cards are expected to significantly reduce, but not eliminate, fraud in the card-not-present environment.

The smart card, through the use of digital certificates and digital signatures that are housed on the chip, will allow issuers to confirm whether a cardholder did or did not make a purchase for which they are disputing. In addition, the requirement of a personal identification number (PIN) to be used on all transactions will also significantly reduce fraud. These features will help reduce fraud related to wrongful disputes, stolen and lost cards, stolen numbers, card skimming, altered cards, counterfeit cards and telefraud (which makes up approximately 80% of all card fraud). This fraud will continue to exist however, when the magnetic stripe on the smart card is used to effect payment. In addition, there is some fraud that smart cards will not be able to eliminate such as identity theft, intercepted mail, and false

---

applications, which make up over 20% of all card fraud.

Despite the fraud-fighting benefits of a smart card, a portion of disputes and chargebacks in the Internet world are the result of problems such as non-delivery of goods, defective merchandise, and ineffective returns processing. These are all issues in which the smart card will have no impact.

In order to dispute chargebacks on card-not-present transactions, merchants may still be required to endure the costly and time consuming process of utilizing AVS or CVV, utilizing a guaranteed delivery carrier, delivering goods to the cardholder's billing address only, and obtaining a signature from the cardholder at delivery – all in order to protect merchants in a potential chargeback dispute.

---

## U.S. Environment

The United States has been slow to adopt smart cards in comparison with the rest of the world, although over the past five years there has been a steady migration towards examining and testing chip card technology. The U.S. current mag-stripe technology and infrastructure is now thirty years old, but still very reliable, efficient, inexpensive to operate, and has enjoyed relatively low fraud levels. Consequently, in the U.S., there has not been a real need or demand for a change in the bankcard payment process. Outside of the U.S., several countries have had good reason to move from mag-stripe to smart card, with the primary drivers being high telecommunication costs, unreliable telecommunication systems for authorizations, and high fraud rates.

Despite the long-term success of the U.S. mag-strip system, thousands of companies have been pushing over recent years for a much improved payment system that offers the potential of almost unlimited functionality such as payment, loyalty, data storage, enhanced security, and security access/identification, just to mention a few.

The Card Associations, banks, the U.S. government, universities, and other chip related vendors and technology companies have made great strides over the past five years to test and examine consumer adoption patterns. For example, computer maker Compaq is contributing to the migration through its deal with FleetBoston to incorporate smart card readers into keyboards for use on the Internet. The U.S. government is planning to issue smart cards to every employee, including those in defense. Smart cards are currently being used for payment on board Navy vessels and at U.S. universities. At the recent Card Tech/SecurTech conference in May 2001, approximately 350 smart card-related companies took part as exhibitors.

Despite the lack of acceptance at merchant locations, and the existence of only a handful of smart card bankcard issuers, momentum is building in the U.S. for smart cards as a key payment technology. Smart card proponents hope that increased awareness through the current the Atlanta region. Consumers lacked a value proposition of carrying a pre-paid card (cardholders were denied the ability to earn interest on the money stored on the card) and

limited number of closed and open platform systems will help consumers adapt to having a smart card in their wallet and create demand for merchant acceptance. Smart card acceptance is certainly a "chicken or egg" dilemma, where most parties, including the card associations, feel that the issuer/cardholder side of the business must be smart card ready before the merchant side will follow.

### Initial U.S. Pilots

The initial foray into smart cards in the U.S. came in the form of two relatively large-scale open-loop pilots in Atlanta and New York starting in 1996. It should be noted that these pilots utilized a single-application *stored value* card, also known as *e-purse* or *cash cards*, rather than chip-based debit or credit applications.

**Atlanta Pilot** – Atlanta was the location of the first large-scale pilot during its hosting of the 1996 summer Olympic games. Three banks participated in the pilot including First Union, Wachovia, and NationsBank, with the three issuing approximately one million *Visa Cash* cards. Most of the cards were disposable (not re-loadable), but First Union did issue an estimated 250,000 re-loadable cards. In addition, at the Olympics opening ceremonies the 83,000 attendees were given smart cards loaded with \$5.

The banks signed 1,500 retail locations and deployed 5,000 terminals including 130 turnstiles at Metropolitan Atlanta Rapid Transportation Authority stations and 200 BellSouth pay telephones. Terminals were provided to merchants at no cost. During the pilot, June through December 1996, an estimated 670,000 *Visa Cash* transactions were conducted.

Overall, the Atlanta pilot received mixed reviews. While the testing of the chip technology itself proved to be successful, consumers and merchant adoption suffered from overall limited retail acceptance. Merchants did not have a compelling business case to accept the cards, as they were charged high discount rates for acceptance of a low-risk, prepaid card (1.20% plus a \$0.02 transaction fee). In addition, an insufficient number of retailers participated, which did not allow for ubiquitous acceptance in

there was the concern that, like money, if the card was lost, then so was the value stored on the card. Overall, the pilot proved that smart cards would need to have a better value proposition (such as

---

more than one feature/function) to cardholders and merchants, and that expanded merchant

**New York Pilot** – The second major U.S. pilot took place in New York City from October 1997 to December 1998 and was sponsored by Visa and MasterCard, with Citibank and Chase Manhattan being the card issuers. Again, a single-application *stored value* card was utilized (Visa Cash and MasterCard Mondex). While the focus of the Atlanta pilot was the operability of the chip technology itself, the main objective in New York, according to Visa, was to gauge consumer and merchant reaction to the system and to demonstrate interoperability between the cards. Targeted in the upper Manhattan area, more than half of the 1,300 merchants in the area including Burger King, Athlete's Foot, Rite Aid, Lechters, and Copy U.S.A. participated. Terminals were provided to the merchants free of charge along with training for store clerks.

Visa Cash and Mondex were positioned to consumers as alternatives to small cash transactions, although many small denomination merchants such as taxis, buses, parking meters, pay phones, vending machines, and parking lots were not included in the pilot. From the merchant's perspective, banks promoted the cash cards as a way to reduce cash handling expenses, although in actuality, chip transactions turned out to take about the same amount of time as normal cash transactions.

The two banks issued nearly 100,000 cards with 75% of the cards being reloadable via ATM machines and kiosks. Citibank also distributed between 3,000 and 5,000 personal ATMs developed by VeriFone so that cardholders could dial in using a standard phone line (not connected to a personal computer) and re-load value on the card without going to an ATM. During the pilot, only 30,000 cardholders ever downloaded money to their cards, which amounted to a total of only \$2.2 million (average of \$12 per card). By the end

Visa and MasterCard indicate that a smart card interchange rate priced below the current standard card present rates (**CPS Card Present Retail** (1.38% + \$.05) or **Merit III** (1.35% + \$.10)) is not being considered in the near term, although rates may change once enough data can be analyzed. Consequently, smart cards lack a major incentive for card present transactions (which make up over

participation would be required.

of the trial approximately one-third of the merchants originally participating had terminated their acceptance.

Despite the meager results of the pilot, important lessons were learned. The interoperability of Visa Cash and Mondex at a single terminal was considered a success. And again, it was clear that a stored value card, by itself, did not create a strong value proposition for consumers or retailers. A multi-application card would probably be required to foster smart card use and acceptance. The industry also learned that retailers and consumers are unlikely to use the cards without some type of incentive such as discounts or reward points. Finally, the requirement to download value onto the card proved to be cumbersome, time consuming, and confusing for several cardholders.

#### Current Situation for Card Associations

Globally, the card associations are focused on providing their members with payment products that meet their needs. In many regions, due to high fraud rates, that product is a smart card. In the U.S., the card associations are focused on the bankcard issuers and providing them with the support necessary to get payment cards into consumers' wallets, whether it is a smart card or an alternative product that enhances a mag-stripe's appeal. For high volume on-line merchants in the U.S., the associations are working through acquirers on secured payment solutions tied to smart cards that will benefit merchants, issuers and consumers. The expectation is that smart cards will reach a critical mass where brick and mortar merchants will begin to upgrade their terminals and accept the cards. Once a few national merchants upgrade, which will begin with Target in 2002, the hope is that other major retailers will follow.

70% of all bankcard transactions in the U.S.). Additionally, the card associations are reportedly not considering a decrease in interchange rates for Internet (i.e., card-not-present) purchases. However, consideration is being given to a change in chargeback liability, under certain circumstances, for Internet purchases that transact

---

using a smart card through higher security

#### Current Situation For Card Issuers

Presently, American Express is the leading smart card issuer in the U.S., with an estimated smart card base of nearly seven million. Three Visa members now issue smart cards, with the retailer Target expected to launch in the fall of 2001. Visa issuer Providian has announced its plans to

American Express utilized first mover advantage with a nationwide marketing campaign that appealed to the younger, Internet-focused market. American Express also promoted the card as a secure e-commerce payment method, packaged the card in a unique design, and offered very

Despite the success of the *Blue* marketing campaign, very few cardholders took advantage of the free PC card reader offered by American Express. A survey by Harris Interactive revealed that less than 1% of the *Blue* cardholders actually use the smart card and PC card reader combination to make purchases over the Internet

channels using digital certificates.

migrate nearly all of its 17 million accounts to chip cards next year. MasterCard plans to announce its other initial issuers in the near future and estimates issuing three million smart cards by the end of 2001. The issuers are targeting smart cards initially for Internet credit purchases rather than brick and mortar smart transactions or debit functionality.

attractive pricing (0% interest rate for six months). Consequently, American Express experienced a comparatively high response rate for its *Blue* card and actually ran short on chips or cards for a brief period. Visa and MasterCard soon thereafter accelerated their smart card rollout.

(i.e., cardholders are using the 16 digit number embossed on the front of the card, not the chip technology on the card). Additionally, the *Blue* cards do not contain a payment application, and therefore, cannot be used at smart card enabled POS terminals.

The chart below provides an overview of the smart cards offered by the current bankcard issuers.

Issuer	Feature/Functionality	Chip/Platform/Applications
<b>American Express Blue Card</b>  Launched 9/99  7 million cards issued	On-line wallet and smart card chip reader On-line account management and bill payment Free on-line Blue Loot rewards program Return protection on both on-line and retail purchases	32K chip on Java platform Original 16K chip on Multos platform Loyalty E-wallet
<b>FleetBoston Fusion Visa Card</b>  Launched 9/00  Less than 1 million cards issued	Chip reader that facilitates secure and automated on-line shopping at Fusion-enabled merchants Ability to download on-line coupons and electronic tickets (e.g., movie) On-line account management	32K chip on Java platform Visa Smart Debit Credit Smart Access Smart Loyalty
<b>Providian Smart Visa</b>  Launched 9/00  Between 1 and 2 million cards issued	Currently offered to premium customers Free chip reader offered to first 50,000 customers On-line account management and bill payment Optional rewards program with annual fee	32K chips on Java platform 8K chips with open platform Visa Smart Debit Credit
<b>First USA Smart Visa</b>  Launched 10/00  Less than 1 million cards issued	Free smart card reader offered to cardholders 5% cash back at select on-line merchants On-line account management and bill payment	32K chip on Java platform Visa Smart Debit Credit Smart Access
<b>Navy Cash JP Morgan Chase Smart MasterCard</b>  Currently in pilot with 175 Cards (5,000 cards by 10/01)	Mag-stripe debit card for use off ship Stored value chip for use on ship (USS Rentz) Payment features tied to sailor's primary bank account	32K chip on Windows for Smart Cards platform Smart Card Integrators e-purse
Sources: <i>American Banker, Credit Card News, CardFax, Card Technology, U.S. Navy, and company websites.</i>		

---

MasterCard's smart card program is gearing up and committed issuers will apparently be announced soon. In contrast to Visa and American Express smart cards that run on the JAVA operating platform, MasterCard smart cards

are expected to run on MULTOS, an operating system originally developed by Mondex International and now marketed by the MAOSCO Consortium (a group of 14 MULTOS vendors).

## Reasons Why Issuers Are Moving Ahead With Smart Cards

The decision to move forward with smart card programs has not been an easy one for the initial issuers. Despite the enormous activity in the smart card industry, a profitable business case for issuers is not an obvious one. Based on interviews with American Express and the Card Associations, there are a few common drivers for issuers to move forward with smart cards:

1. **Decrease In Card Cost** – The advent and popularity of the smart chip in Europe and other regions for mobile telecommunication devices has many manufacturers specializing in this area. Smart cards for payment are built on the same technology as mobile telephone smart chips, which has significantly reduced the price of manufacturing smart cards. Obviously, the cost of a smart card to an issuer is dependent upon the volume purchased, but all-in costs (includes chip, plastic, mailing, security system, embossing, infrastructure, etc.) to large U.S. issuers exceeds \$20 per card, which contrasts to the average cost of \$0.50 to \$1.00 for a mag-strip card. (It should be noted that the commonly quoted \$3 for a chip card is only the price of a low functionality chip purchased in large volume and does not include other costs associated with getting a functional card into the cardholder's wallet.)
2. **Increase In Smart Card Usage In Other Industries** – The migration to smart cards in other countries is paving the way for technological enhancements and is providing knowledge and experience from which U.S. issuers can benefit.
3. **Standards** – The adoption of EMV specification by the Card Associations reduces the possibility to issuers that funds spent on smart card development could be at risk if

different standards were adopted. In addition, the aim of these standards is to ensure interoperability of smart cards with terminals and other devices on a global basis. Global interoperability will help drive smart cards to critical mass, cost efficiencies, and a long-lasting payment form.

4. **Issuer Differentiation** – Issuers are initially positioning their products as a technical advancement appealing to certain segments of consumers who are early adopters of such products. In the future, multiple applications that issuers develop and customize may help create differentiated card programs and a potential competitive advantage over other issuers. Issuers have compared the smart card application concept as being similar to the PC industry twenty years ago when there were few software applications for PCs, but over time, thousands of programs, applications, and games have been developed.
5. **Improved Cardholder Acquisition** – U.S. card issuers are increasingly experiencing lower response rates to card solicitations along with higher cardholder acquisition costs in an increasingly saturated market. Issuers are now experiencing response rates well below 1%. American Express claims to be quite impressed with its response rates during the *Blue* campaign. The initial card issuers are hoping that a new card product will increase the response rate and consequently drive down cardholder acquisition costs.
6. **Improved Loyalty and Retention** – Issuers hope that in the future, by offering a significant number of chip-based applications with the correct mix, they will retain cardholders longer due to the high switching costs of transferring large amounts of information from one card program to another. Further, by providing consumers with a mechanism where they can

---

put the applications that are important to them on the same platform as the payment application, customers are less likely to chase rates and switch cards.

7. **Superior Security for Internet Purchases** – There is little doubt that smart cards can help improve fraud rates on Internet transactions. However, the benefit lies mainly with the merchant since merchants have few chargeback rights on Internet/MO/TO transactions. Consumers also benefit from having fewer concerns about credit card information being potentially exposed to criminals during and after an Internet transaction. Issuers view enhanced cardholder confidence as a key to establishing a critical mass of cardholders and accepting locations. It should be noted that smart cards would not prevent merchant web sites from being infiltrated and exposing cardholder information. However, combining smart cards with other technologies that encrypt the card number or replaces the card number with another disposable number will reduce the probability that card numbers could be stolen.
8. **First Mover Advantage** – The initial issuers may experience the benefits of being a first mover, such as higher response rates, increased cardholder loyalty, and captured market share from other non-smart card issuers. First mover advantages can result in long-lasting benefits, but once a significant number of issuers have followed suit, this window of opportunity will likely be closed.

#### Current Situation For Merchants

At the moment very few merchants have invested in smart card capable equipment, and interviews with merchants, acquirers, and ISOs confirm that merchant focus is on alternative and emerging payment types such as PIN-debit, electronic benefits transfer (EBT), check truncation, gift cards, and other emerging payment types. Again, the decision to invest in smart card capable terminals is not an easy one and a profitable business case is not obviously apparent at this time. Merchants must consider the cost of upgrading their POS terminals and whether smart cards will result in enhanced revenue from incremental purchases, lower transaction costs, or reduced fraud and chargebacks. In addition, merchants need to know, with more certainty, that smart cards will significantly penetrate the U.S. cardholder base.

However, several large U.S. merchants are in the process of updating their POS systems and most realize it would be a mistake to not have their new systems be smart card capable. **Target** is the most recent major retailer to make the commitment to accept smart cards with all 990 stores smart card capable by the end of 2002. In interviews with Target, it was mentioned that the retailer's primary intent was to strengthen its relationship with Target customers through the use of a Target Visa card. Tests before the announcement utilized a non-chip card. Target confirmed that Visa's willingness to financially incur the lion's share of the expenses associated with a smart card issue and POS terminal upgrade (30,000 terminals) was a significant factor in deciding to move forward with a smart card.

**Rite Aid** was one of the first, large U.S. merchants to install smart card capable terminals (installing 25,000 terminals in all 4,000+ stores). The terminals are designed to handle the store's closed system, chip-based gift (stored value) card. These cards replaced the store's paper-based gift certificates. Currently, the POS terminals are not programmed to accept bank issued smart cards (nor is any other national retailer at this time), but the company remains committed to the smart card and is excited about the addition of future applications to their POS program.

#### Current Situation For Merchant Acquirers, ISOs, and Vendors

**Acquirers and ISOs.** A few acquirers and ISOs have added smart card readers (that attach to traditional POS terminals) and integrated smart card capable terminals to their inventories, but most are waiting to see how the cardholder side of the market will transpire. Currently, peripheral smart card chip readers are costing acquirers an incremental \$50 to \$150. Merchants can easily swap out their current PIN pads with one that accepts either magnetic stripe or chip cards. Once the merchant gets the new PIN pad along with a software download, the merchant can accept smart cards. However these readers are more of a short-term fix and will not make conventional terminals capable of handling the multi-applications that are expected to be forthcoming. Fully integrated smart card capable terminals are anticipated to cost 25% to 50% above current new conventional terminals.

**Terminal Manufacturers.** Most of the terminal manufacturers have smart card-ready terminals in

---

their inventory and have been deploying these terminals outside of the U.S. for several years now. The focus is now on being able to support the multi-applications that are anticipated.

VeriFone. Most of VeriFone's new terminals are smart card capable with the use of a chip reader peripheral. Several are also EMV compliant. The reader will allow for smart card debit/credit transactions, but other chip applications will require an upgrade to a fully integrated terminal. The recently released 3300/3350 terminals are integrated smart card terminals able to host multiple smart card applications. This design allows for new applications to be added while avoiding recertification of the terminal. Also, as various software vendors develop EMV-compliant applications, VeriFone will host these in a virtual library. Merchants can then download applications to their terminals as required, again without having to worry about recertification. VeriFone utilizes an **open architecture** strategy by certifying software developed by VeriFone and external vendors.

Hypercom. Most of Hypercom's terminals are smart card capable with the use of a chip reader peripheral. Several are also EMV compliant. A few of its ICE line terminals are fully integrated and these terminals were involved with the first smart card transactions processed recently at the employee cafeterias of National Processing Corp. (NPC), Visa, and Vital.

**Appendix A** illustrates a sampling of the popular POS terminals on the market and their capabilities to support smart cards.

**Processors**. Processors are working with the Card Associations to become EMV-compliant by identifying their infrastructure requirements and developing plans to meet these requirements. The processors are in agreement that infrastructure and system development costs will involve significant capital investment in order to process the multiple applications and handle the security requirements. First Data and Vital are in varying stages of updating their clearing and settlement systems for **EMV Full** support of Visa's Smart Debit Credit (VSDC) program. In July 2001, Vital processed the *first* U.S. smart card credit transaction with a Providian chip card used in NPC's corporate cafeteria.

MasterCard and American Express have developed their specifications for EMV compliance and are also coordinating with processors. Additionally, First Data and Vital are updating their

point of sale (POS) infrastructure for the **EMV Early** adoption phase of VSDC. This will include the ability to pass the card information from the chip, to the POS, to the processors' front-end networks, and then on to the issuer. The processors are also working with several EMV certified software application developers to help identify applications that will be most valued by consumers.

### Current Situation For Smart Card Closed Systems

Smart cards, via closed loop systems in the U.S., are helping to drive smart card awareness, usage, and infrastructure development. The parties that are being the most proactive in implementing smart card solutions are the Federal and state governments, universities, and a handful of corporations. In most cases, smart card technology is being used for identification and security access purposes. Chip technology is becoming a preferred method of implementation due its greater memory capacity and security features over magnetic stripe technology.

Public transit is a key opportunity for driving smart card usage in the U.S. with tens of millions of commuters using transit system everyday. In this case, the smart card provides benefits such as quicker boarding time, reduced costs related to fare collection, and diminished fraud. Several metropolitan areas including San Francisco and Washington, D.C. have already implemented smart cards technology with their transit systems. San Francisco accepts its TransLink card for all transit fare payments whether traveling by bus, rail, or ferry. The Washington, D.C. metro rail system has implemented SmarTrip, a permanent, rechargeable fare card embedded with a contactless computer chip that keeps track of the value of the card. SmarTrip has expanded from metro acceptance to local bus and rail. Other cities such as Boston, New York, and Philadelphia are also in various stages of implementing smart cards with their transit systems and also with parking meters.

The U.S. Federal government has begun implementation of chip technology as part of an overall mandate to reduce costs and move to a more electronic environment. The government plans to issue smart cards to all employees in the near future. These cards will be used primarily for identification and secure access (physical locations or to computer systems and files)

---

purposes. The military will use smart cards for secure access and cash handling on bases and other facilities. The military is expected to have completed deployment of over four million smart cards to all active duty personnel by the end of 2002. One of the first initiatives has been with the U.S. Navy, which is piloting a MasterCard smart card with JP Morgan Chase. The card features a mag-stripe tied to the customer's deposit account at virtually any bank or credit union, coupled with a stored value smart chip that is used for purchases on board ship and on military bases.

Colleges and universities across the country are integrating smart cards for identification, stored value purchases, and secure access purposes. Pennsylvania State University is one of the pioneers with a model program called the **id+** card. The card's access feature is utilized for admission to sports events and access to health services, academic records, library services, computer accounts, long distance phone service, and dormitories. The card also has on-line debit functionality at ATMs and at the POS for local merchants through partnerships with seven participating financial institutions. At the University of Central Florida the smart card is being used as an ATM card, stored value card, and as a student

ID. Students are able to make purchases at local area merchant locations, participate in the meal plan system, and use vending machines, copiers and even the campus laundromat.

Corporations and business campuses are also beginning to use chip card for secure access to buildings and computer networks, with Sun Microsystems being one of the early adopters.

In combination, government, campus and corporate programs are putting smart cards in the hands of millions of Americans, along with helping to build smart card infrastructure and to accelerate smart card standards adoption. As these systems prosper and grow, smart card proponents believe that these closed systems will expand to an open system architecture, similar to the closed ATM networks in the 1970s and 1980s.

Bankcard issuers are hopeful that this previous exposure will help generate consumer demand for smart credit cards or at least offer little resistance when bankcards are re-issued as smart cards. It should be noted that Provident has recently announced that current credit cardholders will be issued smart cards in the near future and that a magnetic stripe only card will not be an option.

---

# Global Market Place

Today, nearly two billion smart cards are in use worldwide for transportation, telecommunications, banking, healthcare, and other industries. MasterCard and Visa make up only 54 million of these cards, of which the majority are stored value/e-purse chip cards. MasterCard projects annual global smart card growth of 127%, which estimates a Visa/MasterCard smart card base of about 278 million by year-end 2002.

There have been four common drivers behind the conversion to chip-based payment cards in countries outside of the U.S.:

- 1. Telecommunications Infrastructure:** Telecommunication networks with frequent outages and high usage fees have created an environment that is inadequate for an efficient on-line authorization service. This situation also makes it difficult to have a zero floor authorization policy, which can lead to increased fraud rates.
- 2. Excessive Fraud:** Fraud such as card skimming, counterfeit cards, identity theft, and lost and stolen cards have created significant losses.
- 3. Concentrated Number of Banks:** In countries with a concentrated financial services industry (i.e., only a few primary banks), issuers tend to also be the bankcard acquirer. This situation has allowed banks to subsidize the high cost of issuing smart cards with the cost savings derived from a reduction in fraudulent transactions that fall on both the issuing and acquiring sides of the card business.
- 4. Association Mandate:** The card associations' regions of Europe and the Middle East/Africa are requiring members to upgrade to EMV-compliant cards and merchants to upgrade to EMV-compliant POS terminals by 2005 for credit and debit transactions. This initiative has spurred other countries outside of these regions to explore and commit to smart cards for credit and debit transactions.

At the moment, there are no global interoperability standards for *stored value* smart card transactions so many countries have their own smart stored value applications. As noted earlier, EMV standards apply to credit and debit transactions, but not stored value. CEPS standards are specific

to stored value applications, and several countries have made the commitment to this standard. It remains to be seen whether CEPS becomes a global standard. Since most smart cards around the world are single application cards and not EMV-compliant, it is expected that issuers will heavily weigh the benefits of a globally interoperable smart card and the drawbacks of upgrading an already effective proprietary chip based system. This decision will not be an easy one for many issuers and regions.

## Europe

Several countries in Western Europe have smart card programs, although most accept stored value/e-purse transactions only. Countries with stored value smart card programs (along with a magnetic stripe-based credit card system) include Austria, Belgium, Denmark, Finland, Germany, Greece, Ireland, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, and Switzerland. The justification behind these stored value programs has been to reduce the need for small change in consumer's wallets, reduce theft at the cash register, and to eliminate the need for physical currency conversion throughout the region.

**France** – During the late 1980s and early 1990s French merchants experienced high card fraud and consequently paid high discount rates to acquirers. In an effort to reduce these costs, France became the first country to adopt smart cards as a primary form of payment in 1992. Since then, fraud has decreased by over 70%. The current smart card utilizes a debit application, unlike most countries that utilize a stored value application. The French government played a key role in the adoption of smart cards, mandating the conversion to smart cards and being involved as an owner of a chip and a terminal manufacturer. Today, France is planning to upgrade the existing chip-based infrastructure to be EMV-compliant.

**United Kingdom** – This country has recently experienced a surge in card fraud and is in the process of replacing their magnetic stripe cards with smart cards at a pace of about one million cards per month.

Throughout Europe, the upcoming January 1, 2005 EMV deadline has spurred countries to move quickly toward compliance with the belief that the longer any one country waits to adopt smart cards, the more susceptible it becomes to being a target for fraud (i.e., fraud perpetrators will migrate to countries without smart card programs).

---

## Latin America

Brazil is the largest smart card issuer in Latin America with over 19 million multi-application cards issued. The cards and systems are not EMV-compliant; however, most issuers and acquirers are currently modifying their systems and replacing cards to be compliant. Visa International plans to replace all 22 million magnetic stripe debit and credit cards with smart cards in 2001, while MasterCard began a similar effort in late 2000.

Stored value/e-purse smart cards are currently used in Argentina, Brazil, Colombia, Mexico, Puerto Rico, and Venezuela. Additionally, Mexican banks voted as a group to adopt EMV-compliant smart cards, and the implementation is expected to begin this year with 50 million cards projected to be in circulation within five years. The Mexican Bankers Association expects the introduction of smart cards to save banks up to \$20 billion (mostly through fraud reduction), which dwarfs the estimated implementation cost of \$100 million.

## Canada

Canada experienced substantial growth in credit card fraud over the past several years, despite its PIN-based Interac debit payment system. To combat this problem, Canada will convert to EMV-compliant cards and readers over the next three to five years. Seven of Canada's largest banks are currently working with Visa, MasterCard, American Express, Mondex, and Interac to develop smart card standards. The group is focusing on the creation of standards for its PIN-based debit cards and ensuring that Canada's point-of-sale terminals have software capable of handling multi application credit and debit cards. Prior to the decision to switch to smart cards, Canada piloted several e-purse type programs.

## Asia Pacific Region

Australia, Japan, and Taiwan have all completed several smart card pilots. Australia's comparatively low fraud rate has not created an urgent need for smart cards. However, the escalation of magnetic-stripe fraud rates in Japan has prompted a leading association of acquirers to announce plans to facilitate the conversion of Japan's POS terminal infrastructure to accept smart cards by 2003. In Australia, several issuers are now considering multi-application cards for

credit, debit, and other significant value-added applications.

Taiwan has experienced a recent surge in fraud (a ten-fold increase over the past five years) primarily in the area of card counterfeiting and skimming. For this reason, Taiwan is experimenting heavily with smart cards and may be the first country in the Asia Pacific region to adopt EMV standards. The governments of Singapore and Malaysia have joined Taiwan to support the development of smart card systems as a national standard in order to help defray the smart card development costs.

## Smart Card Applications Around the Globe

Besides being used for payment at brick and mortar sites, smart cards have been used for other purposes around the globe. Some examples include the following:

**Mass Transit** – Smart cards are being used in **Rome** and **Paris** for fare collection and for making retail purchases. The cards will operate in contact (for retail purchases) and contactless (transit ticketing) modes. The cards will combine transit ticketing with a bank issued stored value/e-purse application that can be used at vending machines, newsstands, and pay telephones.

**Health Insurance** – **Canada, France, Germany,** and **Italy** are making strides in their implementation of national health insurance smart cards. With 80 million cards in circulation, Germany boasts the largest card-based health care program. Currently, the cards are memory-only (no chip) but will soon be upgraded to smart cards with chips. The current cards contain a public data area on the magnetic stripe that houses medical and insurance information and allows for payment processing.

**Data Storage** – Several national governments are considering smart cards as a replacement for paper documents and forms of identification.

**Mexico** plans to use smart cards as a more secure way to monitor and track registered vehicles. **China** intends to issue chip-based identification cards to take the place of the paper identity documents that adults currently carry.

**Malaysia** is issuing 19 million smart cards to its citizens that will replace the country's national identification card and driver's license. The card will also carry a passport application, electronic purse, digital signature applications, and an ATM withdrawal function.

---

**Mobile Communication – Hong Kong** remains on the cutting edge of smart card applications in mobile communication. One example is the China Mobile Communications Corporation, which launched a mobile banking smart card that allows its customers to pay bills, check account balances, and transfer funds using their smart card on a mobile phone.

**Secure Access and Loyalty** – Also in **Hong Kong**, Citibank issues a smart card that supports revolving credit, stored value, and contactless building access applications. The chip card will also house a loyalty application that allows cardholders to earn points at participating restaurants, hotels, and shopping malls.

---

# Key Challenges For The Smart Card

Despite the momentum of smart card development in the U.S. and the support of thousands of organizations and companies, there are a few major hurdles to ubiquitous use and acceptance in the U.S. In general, a clear value proposition must be presented and accepted by consumers, merchants, issuers, and acquirers. Smart card ubiquity is dependent upon consumer acceptance, merchant participation and upgrade of their POS systems, mass card issuance that will drive unit cost reduction, and the development of multiple value-added applications. Other key issues include the following:

**Profitable Business Case** – Despite the anticipated multi-applications of smart cards, no applications have been declared “killer applications” that will 1) guarantee enhanced long-term profitability to issuers and acquirers or 2) provide extreme value and convenience to consumers and merchants. The business case appears more favorable for Internet transactions where fraud and security issues inhibit increased usage of the current payment system. The smart card can significantly reduce these concerns and help increase Internet purchases above their current 3% of all bankcard purchase volume.

**Replacing the Current POS Terminal Base** – Currently there is an installed terminal base of eight to ten million stand-alone POS terminals in the U.S. This does not include the integrated cash register and PC terminals that larger merchants utilize. The majority of these systems will need to be replaced or upgraded with a PIN pad in order to support smart cards. At the current rate of terminal replacement, this could take five to six years. Some terminals can be upgraded for the short term, but most will only be able to process basic smart card payment methods – credit, debit, and stored value. will be unable to handle the multi-applications that are anticipated in the future. Each merchant must decide whether they believe the future benefits of a smart card multi-applications will justify the cost of terminal upgrades beyond simple peripherals. Fully integrated smart card terminals will probably cost merchants \$1,000 to \$1,500 (or 25% to 50% above current conventional terminals). Integrated

cash registers are expected to be even more costly to upgrade.

**Consensus on Standards** – There are several smart card standards that are still evolving, and until the industry makes decisions on key standards, smart card penetration levels may remain low in the U.S.

**Alternatives to Smart Cards** – A few key technologies exist today that can be considered threats or substitutes for a portion of anticipated smart card functionality, and may be less costly to implement than smart cards.

- **Disposable credit card numbers** provide security to consumers when shopping over the Internet and are comparatively inexpensive to implement.
- **Message-based payment systems** where a user name and password identifies an account (such as X.com's PayPal) are easy to use, inexpensive to implement, and portable across many payment platforms and entry formats.

Today, chips are imbedded on platforms other than a plastic card, and this fact puts into question what platform will evolve in the U.S. For example, chips can be embedded in cell phones, personal data assistants (PDAs) or other forms not yet developed. Will this cause the entry of new competitors in to the bankcard industry? Interviews with the card associations lead us to believe that they will be flexible in providing chip and payment options for what U.S. consumers will demand as a chip platform.

---

## Conclusion

Smart cards have begun to penetrate consumers' wallets in the U.S., and there is a large movement of companies that are encouraging adoption as the primary choice of payment. So far, the chip has been slow to evolve and its use has predominantly been limited to closed systems such as universities, the government, and corporations. In the bankcard industry, chip functionality has been limited primarily to the Internet, and the current chips in the market do not provide much more functionality than authentication. The key to widespread smart card acceptance will be the development and implementation of multiple applications that add real value to consumers and merchants.

Acquirers and ISOs, in order to benefit from this opportunity, need to stay attuned with current happenings in the smart card industry. Acquirers and ISOs need to understand the capabilities,

features, and limitations of the smart card capable equipment that is available. Acquirers need to consider how well terminal solutions will fit the needs of their merchants over future years as new smart card applications are developed. Also, acquirers need to stay in touch with their merchants to gauge their readiness and desire to accept smart cards.

Smart cards still have some major hurdles to clear in the U.S. before ubiquitous acceptance, but they are making a presence and gaining traction. We cannot look into a crystal ball to determine at what time this level of acceptance will occur or what primary applications will emerge. However, acquirers and ISOs need to prepare for what appears to be the ultimate replacement of magnetic stripe cards in the not-too-distant future, and should plan accordingly through organized education and lobbying efforts to ensure their voice is heard.

---

# Glossary of Smart Card Terms

(printed with permission from *Get Smart*, Chuck Wilson, 2001)

**Acrylonitrile Butadiene Styrene (ABS)** – Plastic material used to make the body of some types of integrated circuit cards. It is formed through injection molding, enabling the dimensions of the card and the hole into which the chip module is inserted, to be precisely controlled.

**Acquirer** – An institution (or its agent) that obtains card transaction information from the card acceptor.

**Advanced Encryption System (AES)** – A potential *DES* replacement that is still in development. AES is a publicly defined, symmetric block cipher designed so that the key length is variable.

**Aggregate Information** – Demographic data, domain names, and other collected information that is not linked to or identified as personal information.

**Algorithm** – A detailed set of instructions, mathematical routine, or computational rules specifying the procedures to perform a task. Examples of public key algorithms include *RSA* and *ECC*. Also referred to as a *cipher*.

**American National Standards Institute (ANSI)** – The national standards-setting body in the United States. ANSI is an ISO member.

**Anonymity** – A situation in which one's activity is not directly associated with, nor identified to the individual.

**Application** – A program designed for end-users providing a commercial use or purpose for using a device, e.g., an integrated circuit card used for access control, electronic purse, data logs, etc.

**Application Programming Language (API)** – It is a set of standardized routines, instructions, or computer tools used by an application developer for building software applications. Generically, an API is the interface by which an application program accesses the operating system. In smart cards, the API is that component of a microchip that manages the message exchange between the microchip and the card reader. An interoperable API is critical to smart card application development, acceptance and growth.

**Application Protocol Data Unit (APDU)** – It is the packet of data exchanged between two application programs. The basic command unit of a smart card.

**Association for Biometrics** – A non-profit organization that aims to promote the awareness and development of biometric-related technologies.

**Asymmetric Digital Subscriber Line (ADSL)** – The technology transforms the twisted pair of copper wires that run from a consumer's telephone to the local telephone exchange into a digital line. It is referred to as asymmetric because it is generally configured to move data quickly from the exchange to the consumer's computer, rather than the other direction.

**Asymmetric Key Cryptography** – See *public key system and encryption*.

**Attempt** – A submission of a sample to a biometric system for verification or identification.

**Authentication** – A validation process in which the identity of a person or his proxy (e.g., an identification card) is verified. In *electronic commerce*, authentication is the process whereby a card or terminal verifies the authenticity of the message. In *biometry*, authentication is referred to as *verification*. In biometrics, it is a validation method that grants or denies access using a person's unique physical traits.

**Authorization** – The process to grant an approval or guarantee given to a user to honor a transaction, permit use of a resource, or enable access.

**Authorization Code** – A specific value issued and stored with the transaction data to allow confirmation that a valid authorization occurred.

**Automated Fingerprint Identification System (AFIS)** – An automated biometric system that compares fingerprint images to a very large database of images for purposes of identification. While AFIS has some civil applications, it is primarily used by law enforcement.

---

**Autonomy** – Right of self-governance. This refers to one's moral independence and the exercise of control over one's decisions and personal information.

**Biometry** – Method of validating the user by electronically measuring a unique human characteristic such as fingerprint, voice print, iris scan, or hand geometry with the objective of verifying or identifying a specific individual from amongst a population of individuals.

**Biometric Data** – Information that is extracted from a biometric sample and used to build a reference template or to compare against a previously created *biometric template*.

**Biometric Template** – The biometric reference pattern of the *cardholder*, e.g., one's base fingerprints, recorded retina scan, etc.

**Biometric System** – An automated system that acquires a biometric sample from an individual, extracts data from the sample, compares the data with the biometric reference pattern (*template*), makes a match determination, and issues an accept or reject message.

**Bit** – The basic data element in data processing.

**Blowfish** – Invented by Bruce Schneier, it is a block cipher with 64-bit block size and variable length keys (up to 448 bits).

**Brand** – An encapsulation of an actual, experienced value. It represents a relationship customers have come to know and value. A brand offers a consistent message that suggests organizational experience and competences. Indeed, one's brand is defined by the perceptions of others.

**Browser** – Software that enables someone to navigate or search through web sites of the Internet such as the World Wide Web. Microsoft's Internet Explorer and Netscape's Navigator are examples of browsers.

**Brute Force** – A programming method that relies of the computer's processing power to generate all possible outcomes, one after another, until the solution is realized. The term is also applied to *exhaustive search* attacks in which a hacker attempts to find an encryption key.

**Byte** – The formation of a character or symbol made up of bits. A typical computer character is made of eight bits. However, 16-bit, 32-bit and even 64-bit are increasingly more common.

**Card Accepting Device (CAD)** – Device that is used to communicate with a smart card during a transaction. It may also provide power and timing to the smart card chip. Also called a card reader.

**Cardholder** – The person or entity with whom an account relationship is established and to whom a card is issued. For financial transaction cards, a cardholder is associated with the *Primary Account Number (PAN)*.

**Card Number** – For *credit cards* this is the same as the primary account number. In other applications this may only be a card retailer.

**Card Reader** – See *Card Accepting Device*.

**Card Verification Code (CVC)** – An anti-fraud mechanism in which a three-digit code is encoded on track 1 or track 2 in the "discretionary data" field of a magnetic stripe of a MasterCard. Its purpose is to inhibit any potential alteration of the card, and to enhance the electronic authentication of the card. The Visa version of a CVC is called the *card verification value* or *CVV*.

**Card Verification Value (CVV)** – This is the Visa version of the *CVC*.

**Certificate Authority** – A trusted third party that develops and issues a *digital certificate* to individuals or organizations enabling them to prove their electronic identity to others. It is usually a source that is trusted by all participants in a transaction.

**Certification** – The process that validates that a transaction occurred.

**Code Division Multiple Access (CDMA)** – A digital wireless transmission technique that uses mathematical codes to transmit and distinguish among multiple wireless conversation sessions. CDMA assigns each subscriber a unique code to place multiple users on the same wideband channel simultaneously. Both the mobile stations and the base station track the codes on the same frequency channel in order to distinguish among the conversations. CDMA is a form of *spread spectrum* technology.

**Challenge-Response** – This is a form of authentication in which one device (terminal, card reader, etc.) sends a "challenge," generated randomly. The device or card being authenticated performs a computation of the challenge, processes it, and returns a response to the challenger. Meanwhile, the

---

challenger computes its own solution for comparison to the results from the challenged unit. If the results match, the challenged unit is considered genuine.

**Chargeback** – An issuer-generated reversal of all or a portion of an amount previously posted to a *cardholder* account. This occurs when a cardholder disputes a charge that appears on his or her bankcard statement. The reversal amount is “charged back” to the acquirer who in turn usually charges back the merchant.

**Check Digit** – Suffix used to test the validity of a number.

**Chip** – A small square of thin, semiconductor material, such as silicon, that has been chemically processed and etched with a specific set of electrical characteristics such as circuits, storage, and/or logic elements. Also known as an *Integrated Circuit (IC)*.

**Chip Card** – An *integrated circuit card ICC* or *smart card*. All three terms are used interchangeably. The *chip* is embedded in the plastic surface of the card.

**Cipher** – The general rule, method, or calculation for encrypting or decrypting a message. An *algorithm*.

**Ciphertext** – Encrypted output of a cryptographic *algorithm*.

**Clearing** – The processing of financial transactions between the *Acquirer* and *Issuer* for reconciliation, billing and statement use.

**Clear Text** – Data in its original, unencrypted form (same as plain text).

**Closed System** – A system where the *Issuer* and *Acquirer* of the card are the same party. The party that provides services issues the cards. It is used as a proprietary system.

**Chip-Secure Electronic Txn Protocol (C-SET)** – Refers to a *SET* transaction initiated with a chip card housing the *digital certificate*.

**Codification** – The process that protects the data during a chip card transaction.

**Coercive Force** – The strengths of the reverse magnetic field required to de-magnetize a given piece of magnetic material, expressed in “oersteds.”

**Combination Card** – This is initially a chip card that contains both contact and contactless functions on a single IC chip that can communicate between the chip and chip card reader. Sometimes referred to as a “combi” card, the contact and contactless interfaces are usually not connected.

**Common Electronic Purse Specs (CEPS)** – A set of standards for electronic purse applications advanced by Visa International and supported by 90% of the operators of *stored value systems*.

**Conditional Access** – A provision of access to a network, computer, or digital appliance (e.g., TV) based on pre-selected criteria such as authenticating a subscriber's identity to a digital service provider.

**Confidence Interval** – A term used in statistics to define probabilities. It represents the interval within which a specific random variable will fall, given a level of confidence or probability. Confidence intervals are used to define statistical risk measures.

**Confidentiality** – Preventing unauthorized individuals or processes from gaining access to documents, transactions or messages. Refers to keeping data private in an electronic exchange.

**Connector** – A point of electrical connection between an integrated circuit card and its external interfacing device that permits a flow of energy current between the two. ISO standard IC cards have eight *contacts*, although it is common to only use six.

**Contact** – See *connector*.

**Contact Card** – An *integrated circuit card* that must be inserted into a card reader where data can be transferred through the use of metallic connectors or contacts.

**Contactless Card** – An *integrated circuit card* that communicates with an antenna by means of a radio frequency signal. There is no need of physical contact between the card and a *card reader*.

**Cookie** – Data generated by a web server and stored in the user's computer. Web servers automatically regain access to relevant cookies whenever the user re-establishes a connection to them, such as when making a web site selection.

---

**Corporate Card** – A card issued to a company for use by an employee for business related transactions. (E.g. purchases, logical access, physical access).

**Coupler** – An electronic system used to read a *smart card*. It is usually designed for integration into a machine such as a parking meter.

**Credit Card** – A card that enables the *cardholder* to make transactions against a credit account established with the *Issuer*, whereby the Issuer has agreed to make available a specified amount of funds to the cardholder.

**Credit Limit** – Maximum amount that can be borrowed by a *cardholder* at any one time on an account.

**Cryptographic Key** – Parameter used in conjunction with an algorithm for the purposes of validation, *authentication*, encipherment, or decipherment.

**Cryptography** – A system for encrypting and decrypting data for a specific audience. It usually involves an *algorithm* for combining data with one or more *keys*. The security of a cryptographic system usually depends on the secrecy of some or all the keys, rather than upon the secrecy of the algorithm.

**Data Capture** – The electronic recording of information for subsequent use and information processing.

**Data Encryption Standard (DES)** – An ANSI Standard that describes a symmetric algorithm for encrypting data. Originally, the algorithm operated with a 56-bit secret key. IBM and the National Bureau of Standards developed it in the 1970s. It is also known as the Data Encryption Algorithm (DEA).

**Data Integrity** – Refers to the assurance that information exchanged in an electronic transaction is not alterable without detection. See *non-repudiation*.

**Debit Card** – A card used to make transactions that is linked to the cardholder's direct deposit account.

**Decryption** – Converting encrypted information back into clear text (or plain text). Also known as decipherment.

**Dedicated File (DF)** – Memory organization for microprocessor cards. A DF is a logical entity that holds a number of *elementary files*. In multi-purpose cards each DF will normally correspond to a distinct application.

**Decision Threshold** – An adjustable level at which a *biometric system* accepts or rejects *biometric data* depending on whether the match score falls below or above the threshold.

**Degrees of Freedom** – The number of statistically independent features in biometric data that are free to vary in the calculation of a statistic.

**Diffie-Helman** – A commonly used, *public-key algorithm* for key exchanges.

**Digital Cash** – A term commonly used to refer to *stored value* functions. Also refers to *electronic cash*.

**Digital Certificate** – An electronic document signed by a trusted third party verifying one's digital identity. It usually contains the user's public key, information about the certificate authority, and additional information about the certificate holder.

**Digital Optical Laser Card** – A portable card that passively stores information in the form of high-density marks or bars.

**Digital Signature** – A block of data created by a sender's private key that is used to authenticate a transaction or message by the sender. The digital signature is generated using a cryptographic algorithm and information that identifies the user, including a cryptographic key.

**Digitized Signature** – A computer application in which one's written signature is digitized and captured in a computer repository.

**Digital Wallet** – See *electronic wallet*.

**Discount Fee** – The fees charged by financial institutions to merchants for processing *credit card* payments. The discount fee is usually based on the average purchased amount (called average

---

ticket) and the transaction volume. The discount fee includes the interchange rate charged by the card association (e.g., Visa or MasterCard), the processing fees, and an array of bank service fees.

**Disposable Card** – A prepayment card that cannot have value reinstated. Also referred to as a *non-replenishable card*.

**Electrical Erasable Programmable Read Only Memory (EEPROM)** – The chip's non-volatile memory whose contents can be loaded or deleted after the manufacture of a chip card. Memory contents can be erased via an electric charge, and new data can be reloaded into EEPROM, as often as needed.

**Electrical Programmable Read Only Memory (EPROM)** – A non-volatile memory technology that can be written to only once before being erased using ultra-violet light, after which it may be written to again. It is often used for disposal cards such as telephone cards.

**Electronic Business (e-Business)** – A term used interchangeably with *electronic commerce*.

**Electronic Cash (e-Cash)** – Authenticated units of value (e.g., dollars) represented by an electronically stored code. The term is often used to describe an *electronic purse* application. Also referred to as digital cash.

**Electronic Commerce (e-Commerce)** – The paperless exchange of business information and transactions over information networks through use of computer processors. It includes inter-company (e.g., the *Internet*) and intra-company functions that enable commerce and that use or interact with a computer.

**Electronic Module** – See *micromodule*.

**Electronic Purse (e-Purse)** – An application in a card where electronic cash (value) is stored. See *stored-value card*.

**Electronic Wallet (e-Wallet)** – Generally refers to integrated circuit card or super smart card capable of executing a variety of financial transactions and identification functions. More sophisticated than an *electronic purse*, a wallet may include debit, credit, cash card, and other functions. Also called a digital wallet. Outside of smart cards, this term could also refer to a PC software package that contains account information for presentation for transaction payment (as used on the *Internet* with *SET* or *SSL*).

**Elementary File (EF)** – Memory organization for *microprocessors* – the smallest logical entity that can be secured in the operating system. The file contains data.

**Elliptical Curve Cryptography (ECC)** – First proposed by Miller and Koblitz in 1982, this asymmetric algorithm uses three points of an elliptical curve to calculate complex key pairs. It appears to be more efficient than the *RSA* algorithm, making it faster in that it can use shorter keys to achieve similar levels of security.

**Embedding** – The placing of the micromodule in the cavity of the card body. After an electrical test occurs, the embedded module is then encoded. See *ABS*.

**Embossing** – The action of raising letters or logos on the surface of a plastic card.

**EMV** – The joint project of Europay, Master Card and Visa to define global specifications for *smart cards*.

**Encoding** – The writing of system, issuer and cardholder data into the *smart card* chip or a *magnetic stripe*

**Encryption** – The use of cryptographic *algorithms* to encode clear text data (e.g., PINs) to prevent anyone outside the intended recipient(s) from reading that data. By reversing the process via an electronic key (*decryption*), the intended recipient can reconstruct the original clear text. It provides the basis for *confidentiality*, *data integrity*, *authentication* and *non-repudiation*.

**Equal Error Point** – In a *biometric system*, the equal error rate occurs when the decision threshold is set so that the proportion of *false rejections* equals the proportion of *false acceptances*.

**Exhaustive Search** – A hacking method used to compromise an encryption key by using massive computer power. For example, *DES* uses a 56-bit binary key. Thus, there are 256 possible *DES* "keys". A powerful computer can attempt to "break" *DES* by an exhaustive search attack trying all combinations until successful. Also referred to as a *brute force* attack.

**Expiry Date** – The date after which a card, account, or application ceases to be valid for transaction use, unless an exception process is used to gain permission. Also known as expiration date.

---

**False Acceptance** – A situation in which a *biometric system* incorrectly verifies an imposter against a claimed identity. It is also called a Type II error.

**False Acceptance Rate** – This is the probability that a *biometric system* will incorrectly verify an imposter.

**False Rejection** – A situation in which a *biometric system* incorrectly rejects a legitimately claimed identity. It is also called a Type I error.

**False Rejection Rate** – This is the probability that a *biometric system* will reject a legitimate claimant.

**Flash Memory** – A type of non-volatile memory that can be erased and reprogrammed in units of block memory. It is a variation of EEPROM which, unlike Flash memory, is erased and rewritten at the byte level – a slower process. The microchip is organized so that a section of memory cells are erased in a single action or “flash”.

**Float** – The value of funds tied up in the payment process, reflecting the value of payment processing time.

**Floor Limit** – The dollar value limit for a single credit card transaction – above which an *authorization* transaction is performed, and under which there is no authorization transaction.

**Frequency Division Multiple Access (FDMA)** – A wireless transmission technique that divides radio channels into a range of radio frequencies. It is used primarily in the traditional analog cellular systems. With FDMA only one subscriber is assigned to a channel at a time.

**General Packet Radio Service (GPRS)** – A packet-switched, wireless communications service that promises data rates up to 114 Kbps and continuous connection to the Internet for mobile phone and PC users.

**Globalstar** – A mobile satellite phone system launched in October 1999 using 48 low-earth-orbiting (LEO) satellites to provide global phone service.

**Global System for Mobile (GSM) Communications** – A digital mobile phone that uses a chip card to identify the user to the phone service provider through use of a SIM card. It is the European Telecommunications Standards Institute (ETSI) standard for digital cellular telephones that employ integrated cards for identification and security. GSM digitizes and compresses data, then sends it down a channel with other streams of user data, each in its own time slot. It is deployed in over 120 countries, and used by over 100 million subscribers, making it the most widely used of the three *PCS* transmission technologies.

**Hash Function** – An algorithm that turns messages or text into fixed strings of digits for purposes of security. A one-way hash function is typically used to create a message digest in the formation of a *digital signature*.

**Hash Value** – A fixed-length value created mathematically from a string of text to uniquely identify data. It is used to ensure that a transmitted message or transaction has not been tampered with.

**Hologram** – A unique optical image that gives the image a three-dimensional effect. Generally, it is placed on credit and debit cards as a security feature to prevent fraudulent card copies.

**Hybrid Cards** – There are three uses of this term in the chip card environment: (1) to refer to an environment in which smart cards function in a closed system that has open system attributes; (2) to describe a combination contact and contactless card (see *combination cards*); and (3) to describe chip cards that also contain characteristics of obsolete technologies, e.g., *magnetic stripes*, bar codes, etc.

**Identification** – In *electronic commerce*, it is a process that validates the *cardholder's* identity. It is the one-to-many process of comparing a submitted biometric sample against all the *biometric templates* on file to determine if there is a match.

**Information Privacy** – The ability of an individual to maintain personal control over the uses and distribution of information about one's self.

**Infrastructure** – The hardware, software, networks, services and processes to support a business endeavor.

**Initialization** – Setting data fields on card.

**Insult Rate** – The percentage of occasions a valid user is rejected for a service, e.g., alleged erroneous billings or erroneous rejections of valid users by biometrics.

---

**Integrated Circuit** – An electronic circuit designed to perform processing and/or memory functions. Also referred to as a *chip*.

**Integrated Circuit Card (ICC)** – A card into which one or more *integrated circuits* are embedded. Also referred to as a *chip card* or *smart card*.

**Interchange Rate** – The rate charged by the card associations (e.g., Visa and MasterCard) to the merchant banks for credit card transactions at a merchant location.

**Integrity** – The assurance that a message or transaction is accurate and complete.

**Interdependency of Demand** – Mutual dependency by two entities to achieve their goal such that each party needs the other to succeed.

**International Data Encryption Algorithm (IDEA)** – A 128-bit key symmetric cipher, patented in the U.S. and most European countries by Ascom-Tech. It is purported to run a thousand times faster than RSA.

**International Organization for Standardization (ISO)** – An international federation of national standards organizations. The U.S. organization for standards setting is *American National Standards Institute (ANSI)*. Headquartered in Geneva, Switzerland, the ISO mission is to promote development of standardization and to facilitate international exchange of goods and services. Note: the acronym, ISO, is taken from the initials of the French name.

**Internet** – The global, de-centralized, public medium (the network of networks) connecting hundreds of thousands of computers and serving millions of computer users. No government or any other centralized authority controls the Internet.

**Internet Commerce** – *Electronic commerce over the Internet*. Internet commerce is narrower in scope than electronic commerce because it excludes all activities outside the Internet.

**Internet Open Trading Protocol (IOTP)** – A universal set of guidelines for communications among e-commerce products, permitting interoperability for electronic payments, independent of the payment mechanism used.

**Interoperability** – The ability of application and products (e.g., *smart cards*) manufactured by different companies to operate seamlessly with applications and products (e.g., smart card readers) of another company.

**Issuer** – The institution or organization identified on the card issued to the *cardholder*.

**Java Card** – Sun Microsystem's smart card *operating system* for multiple applications.

**Key** – A string of characters or numbers known only to the sender and the intended recipient to create a value used in a cryptographic *algorithm* to decode an encrypted message, to encode plain text, or authenticate a message.

**Key Management** – The process by which cryptographic keys are provided for use between authorized communicating parties and whereby those keys are subject to secure procedures until they have been destroyed.

**Kilo (K)** – Denotes thousands (from the Greek word, *chilioi*); in computing, it refers to kilobytes, or 1024 bytes.

**Kiosk** – A standalone, remote station, usually consisting of a microprocessor with a touch screen, used for delivering information.

**Laser Card** – See *Optical Memory Card*.

**Local Area Network (LAN)** – A data communications network that enables the exchange of programs and data files among users that are physically connected to the local network, without the use of modems. It is usually a network of PCs linked together to share information. Generally, users of a LAN are located in the same building or cluster of buildings as there are distance limitations, usually no more than one kilometer in radius.

**LUC** – Invented by Peter Smith, LUC is a *public key algorithm* that uses Lucas functions instead of exponentiation.

**Magnetic Stripe** – Magnetic material in the shape of a stripe on which signals can be stored electromagnetically.

---

**Match Score** – In biometry, the match score is a computation of the degree to which a biometric sample matches a previously stored template. An accept or reject decision is based on the relationship of this score to the established *decision threshold*.

**Memory Card** – *Integrated circuit card* capable of storing information, but not having calculating capability, i.e., no microprocessor. Typically, memory cards contain a storage capability over a hundred times greater than a magnetic-stripe card.

**Metcalfe's Law** – Named after Robert Metcalfe, founder of 3Com Corp, this postulate states that the value of any network ( $V_n$ ) increases in proportion to the square of the number ( $N$ ) of the people using it, so  $V_n = N^2$ . Metcalfe's observation underscores that a network's value grows in proportion to the number of uses and information sources connected to it. Thus, 1,000 people attached to a network are 100 times more useful as one with 100 people connected to it. This postulate demonstrates that the interconnection growth increases value exponentially.

**Micromodule** – The electronic unit on a smart card formed by a chip and a contact plate, connected by fine wires and encapsulated in a drop of epoxy resin. The micromodule is inserted into the cavity in the card body to form a finished card.

**Microprocessor** – A single silicon *chip* that contains a computer processor, and may include registers and cache memory. It provides programmed intelligence.

**Minutiae** – They are the data points of a fingerprint that uniquely describe the print's layout in digital terms. These are the small details found in finger images such as ridge endings or bifurcations.

**Mobile Commerce** – A shortened form of mobile electronic commerce, it is the exchange of business information and transactions over networks using a mobile communications device.

**Mondex** – A true cash-equivalent, card-to-card, stored-value scheme supported by MasterCard International

**Moore's Law** – Gordon Moore, co-founder of Intel, postulated in the 1960s that computer processing power will double every 18 months, at a constant level of cost. It has proven accurate for 30 years, making it a very stark statement about the size and scale of the current information revolution.

**MULTOS – Multiple Application Operating System**. An operating system for multiple applications

**MULTOS Executable Language (MEL)** – The *Applied Programming Interface (API)* for *MULTOS*.

**Non-replenishable Card** – A prepayment card that cannot have value reinstated. Also referred to as a *disposable card*.

**Non-repudiation** – A cryptographic situation in which someone who digitally "signs" a document using his digital signature, ensuring document *integrity* and authenticity, cannot claim that he didn't originate the document, or that the document was altered after he signed it. Non-repudiation is deemed essential to a trading partner's willingness to rely on electronic communications as authentic and true.

**Non-volatile Memory** – A semiconductor memory that retains its content when power is removed.

**Off-line** – Computer-based data files and operations residing on the integrated circuit chip can operate separately from the central processing unit.

**On-line** – Direct access to computer-based data files and operations systems via computer terminals; it has implications of interaction, or more specifically, from the issuer's card processing host.

**Online Privacy Alliance** – A coalition of over sixty companies and trade associations globally who advocate the posting of and adherence to privacy policy at Websites.

**On-line Transaction Processing (OLTP)** – A type of computer processing in which the computer responds immediately (in real time) to user requests. Each request is considered a transaction.

**Open Card Framework (OCF)** – A system architecture supported by an industry consortium that enables the development of globally interoperable smart card solutions across multiple platforms. It enables computer users to access secure information on a network by using a smart card as a network access device.

**Open Platform** – This is the evolved name for the *Visa Open Platform*. It is a set of specifications for the issuance of multi-application cards.

**Open Standard** – A non-proprietary, technology standard that is publicly published so that any vendor, manufacturer or application developer can use it; indeed, they would be encouraged to use it.

---

These open standards present a uniform and consistent methodology or specification to achieve a common action or result.

**Open System** – A card system that involves multiple issues of cards that can be used to access services or purchase products at multiple service providers. An open system requires the processing of interchange transactions, usually by an independent ‘system operator’.

**Operating System** – A collection of system programs that control the basic operating functions of a computer or processor.

**Optical Memory Card** – Also known as *laser cards*, because a low-intensity laser is used to burn holes of several microns in diameter into a reflective material exposing a substrata of lower reflectivity. Generally, it has several megabytes of memory. The card is written once, and information cannot be erased. These appear to have found a market in the health care industry.

**Optical Scanner** – A device that “reads” text, illustrations, or three-dimensional objects and translates that data into a format that a computer can use. Optical scanners digitize the image, and represent it as a bit map.

**PCMCIA – Personal Computer Memory Card International Association.** Association founded to standardize PC cards – which are typically used in laptop computers, and referred to as PC cards. It can also stand for **People Can’t Memorize Computer Industry Acronyms**. Not all PC cards are smart cards.

**Personal Communications System (PCS)** – A collective term for three digital transmission technologies: *TDMA*, *GSM* and *CDMA*. It is sometimes referred to as digital cellular.

**Personal Computer Smart Card (PC/SC)** – A set of PC specifications for an open, platform-independent, and application-neutral environment for the purpose of integrating smart cards with personal computers. The PC/SC specifications are published by the PC/SC Workgroup that was formed in 1996, and whose members in 1999 included: Bull, Gemplus, Hewlett-Packard, IBM, Microsoft, Schlumberger, Siemens Nixdorf Information Systems, Sun Microsystems, Toshiba, and VeriFone.

**Personal Digital Assistant (PDA)** – A compact, mobile (usually hand-held) special purpose digital appliance for information storage or retrieval, computing and networking. A typical PDA, such as PalmPilot, electronic organizer / planner, or hand-held PC, can function as a telephone, fax, or microprocessor. PDAs with built-in micro-browsers act as portals to the Internet.

**Personal Identification Number (PIN)** – Code the customer possesses for verification of identity when using a card. It is usually a numeric code, most often associated with debit cards and smart cards.

**Personalization** – Electrical personalization is the process of initializing a card with data that ties it uniquely to a given cardholder and account. Graphical personalization modifies the visual aspects of the card with personal data (name and photo) or logos.

**PIN Pad** – A keypad for entering *PIN* values.

**Polyvinyl Chloride (PVC)** – A plastic material used to make plastic cards, including *smart cards*.

**Portal Company** – A Website at which many consumers start their Internet browsing, or where they go to get helpful information.

**Primary Account Number (PAN)** – Series of digits used to identify a customer account or relationship.

**Privacy Partnership** – In 1998, eight *portal web companies* joined with *TRUSTe* to raise awareness about online privacy. This is a grass-roots initiative to educate the Internet community about privacy. Its original eight members (now grown to dozens of participants) are: America Online, Excite, Infoseek, Lycos, Microsoft, Netscape, Snap and Yahoo!

**Private Communications Technology (PCT)** – Microsoft’s counter to SSL.

**Private Key** – In *asymmetric cryptography*, the key that is known only to the user.

**Programmable Read Only Memory (PROM)** – A *read-only memory* (can’t be altered) that can be written to only once.

**Protected memory** – *Memory cards* with password protection to safeguard information contained in the *chip*.

---

**Protocol** – A set of rules or conventions governing the interaction of processes, such as describing how to transmit data over an information network.

**Protocol Data Unit** – A packet of data passed across the network.

**Proton** – An *electronic purse* system embraced by an array of stored-value operators, including Visa and EuroCard.

**Pseudonym** – An alias, “handle”, or “call sign” used by individuals to shield their identity. It is an identifier that is insufficient in directly associating to an individual, but usually can be indirectly associated.

**Public Key** – The term “public key” has two uses. First, it is a truncated use of *public key system*, referring to the public key / private key pair. Second, it might be used to only refer to the individual public key, apart from *private key*. To eliminate confusion, it is easier to use the term, *published key*, when referring to the individual public key.

**Public Key Infra-Structure (PKI)** – Based on the *public key system*, it is the structure required to issue, maintain, and revoke public key pairs used to encrypt data and to authenticate individuals participating in *electronic commerce*.

**Public Key System** – Also known as *public key cryptography*. It is an asymmetric or two-key system, using pairs of cryptographic keys, one that is private, and one that is public. If encipherment occurs using the public key, decipherment requires application of the corresponding private key and vice versa. It is an encryption scheme introduced by Diffie and Hellman in 1976 in which messages are encrypted with the recipient’s *public key* and can be decrypted only with the recipient’s *private key*.

**Published Key** – In *asymmetric cryptography*, it is the key that is published by the user to others for their use in verifying signatures and encrypting messages. It is sometimes referred to as the *public key*, although this is confusing since the overall system is also referred to as the public key.

**Random Access Memory (RAM)** – A volatile memory used in integrated circuit cards like a microprocessor’s scratch pad; it requires power to maintain data.

**RC4** – A symmetric *cipher* developed by RSA Data Security known for its high speed.

**Read Only Memory (ROM)** – Non-volatile memory that is written once, usually during chip production. It is used to store operating systems and algorithms employed by the microprocessor in an integrated circuit card during transactions. Also referred to as firmware.

**Reduced Instruction** – A microprocessor that is designed to perform a smaller number of computer instructions so that its Set Computer (RISC) can operate at a higher speed. RISC architecture usually results in performance improvements.

**Routing** – The process of selecting the correct interface and communications path segments for a packet of data being transmitted through a network.

**Routed Infrastructure** – The Internet’s routing system that enables messages to pass from one computer to another until the message reaches its intended destination.

**RSA** – A *public key* cryptographic *algorithm* developed by mathematicians Ron Rivest, Adi Shamir and Leonard Adelman in 1977 (RSA is ANSI standard X9.44). It is one of the most popular public key algorithms. Its US-only patent expires in 2000.

**Secure Electronic Transaction (SET)** – A paymenting *protocol* based on public key infrastructure for use over the Internet. SET involves the use of *digital signatures* based on *public key* encryption, to authenticate all participants in a card-based payment transaction.

**Secure Socket Layer (SSL)** – A software-based, session-layer encryption protocol that use data encryption and reliability checks to provide secure TCP/IP connections. Developed by Netscape, SSL connections are usually initiated with a web browser through the use of a special URL prefix.

**Security Access Module (SAM)** – A dedicated *microprocessor* unit that enables active authentication by calculating and comparing authentication *algorithm* results.

**Self-Programmable One-Chip Microcomputer (SPOM)** – An architecture for single chip *microprocessors* to handle securely multiple applications using self-programming operations in a non-volatile memory. The SPOM was patented in 1978 by Michael Ugon at Bull CP8.

---

**Set-Top Box** – An electronic control device that interfaces with a digital appliance, usually a television set. The Set-top box connects to communications channel such as telephone, satellite or cable. Its name was derived from the common placement of the device on the top of the television.

**Signature Panel** – A space on a card bearing the *cardholder's* signature.

**Signature Verification** – A behavioral biometric that analyzes the *way* an individual signs his or her name. The measurable signing features include speed, velocity and surface pressure.

**Skimming** – Electronically copying the card data from one card to another.

**Smart Card** – An *integrated circuit card* with memory and a *microprocessor* capable of making decisions.

**Spam** – Unsolicited, unwanted junk e-mail.

**Spontaneity** – A requirement of *electronic business* that enables its conduct when participants desire, without pre-coordinated effort.

**Spread Spectrum** – A transmission technology that spreads information contained in a particular signal over a much broader bandwidth than the original signal.

**Stored-Value Card** – A stored-value card is one that stores electronic cash (value) for small dollar transactions. See *electronic purse* or prepayment card.

**Subscriber Identity** – A device used in the *GSM* application to link a phone number to a specific person instead of linking the number to a specific phone set.

**Subscriber Identity Module (SIM)** – A special type of smart card for *GSM* systems holding the subscriber's identification number, thus enabling him to call from any *GSM* device. The SIM can encrypt the transmission.

**Super Smart Card** – A card-shaped device that has an on-board keypad, LCD's and batteries, as well as one or more integrated circuit chips capable of storing and processing data.

**Symmetric Key Cryptography** – Cryptographic processes in which encryption and decryption make use of the same secret key. Its opposite is *asymmetric key cryptography*.

**Teledisco** – An initiative backed by Boeing to surround the globe with a broadband network of satellites to support voice, data and video communications in a fiber-like environment. Teledisco is expected to require at least eighty low-earth-orbiting (LEO) satellites, and will not be commercially ready prior to 2004.

**Threshold** – The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold that is adjustable.

**Time Division Multiple Access (TDMA)** – A digital transmission technique that divides channels into time slots to obtain greater capacity. It is a common technique employed in digital mobile phones. Its standards include *GSM*, North American Digital Cellular, and Personal Digital Cellular.

**Timestamp** – In a *digital signature* an organization of a document or transaction can electronically testify that the document existed at the stated time.

**Token** – A token is similar to a *key* in that it is an object used to secure data or one's identity. A hardware token usually refers to a device like a physical key or smart card that enables its owner to logon to a network via an encrypted password.

**Transaction** – A business or payment event for the exchange of value for goods or services.

**Transform** – A change in form, but not in value.

**Transmission Control Protocol / Internet Protocol (TCP/IP)** – The de facto standard Internet protocol. Developed by DARPA for inter-networking, it is really two protocols, TCP and IP, working at the network and transport layers, respectively.

**Triple DES (3DES)** – An encryption *algorithm* that uses three DES separate encryptions consecutively with at least two separate keys to render DES less vulnerable to an *exhaustive search* attack.

**Trusted Third-Party** – See *Certificate Authority*.

---

**Trustmark** – An online seal or service mark, awarded by TRUSTe to Websites that agree to post their privacy practices openly on their Websites, and adhere to the procedures that ensure their privacy promises are realized.

**TRUSTe** – A non-profit, third-party oversight organization created to strengthen trust between consumers and the online web sites that they visit. TRUSTe provides a branded symbol that signifies good privacy practices.

**User Identity Module** – A mobile phone standard that incorporates smart cards inserted into the phone handset.

**Value Chain** – The set of activities, functions, and business processes that an organization performs to create, deliver, and support its production of goods and services. Competitive advantage is achieved when an organization can acquire or perform the activities in its value chain more cheaply than its competition.

**Verification** – In biometry, verification is the process of comparing a submitted biometric sample against the biometric reference template to authenticate the claimed identity.

**VeriSign** – Mountain View, CA-based VeriSign, Inc. is a leading provider of *public key infrastructure* and *digital certificate* solutions used by businesses, consumers and web sites to conduct secure communications and transactions over the public Internet and private networks.

**Very Small Aperture Terminal (VSAT)** – A Ku band-based satellite dish of 1.2 meters (four feet) or 1.8 meters (six feet) used by businesses and consumers for voice, data and video reception.

**Visa Cash** – Visa's stored-value scheme.

**Visa Loyalty Program** – Visa's seven partners in creating software specifications for loyalty and payment applications on the same card include: Chip Applications Technologies, Cyberpro Technologies, De La Rue Card Systems, IBM Corporation, VeriFone, Inc., Smart Card Solutions LLC, and Welcome Real-time.

**Visa Open Platform** – A collection of specifications and technologies that enable financial institutions to develop and issue multifunction cards. It enables applications and keys to be loaded securely onto a smart card even after the card has been issued to the cardholder. It is based on *Java Card* technology.

**Visa's Smart Path** – A global initiative by Visa International to assist its member banks to use chip card technology and alternate delivery channels such as the Internet.

**Voice Recognition** – The process of verifying a recorded voice pattern against a pre-recorded voice template to validate one's identity.

**Volatile Memory** – A memory device that does not retain stored information when power is interrupted (e.g., RAM).

**Website** – A set of files, referred to as pages, on the *World Wide Web* that are linked together and maintained by an organization, company, government agency, or an individual.

**Watermark** – A technique that helps guard against counterfeit *magnetic-stripe* cards by using a unique, fixed pattern encoded on the magnetic stripe.

**Windows for Smart Cards®** – The multi-application, smart card *operating system* introduced by Microsoft.

**Wireless Application Protocol (WAP)** – A wireless transmission protocol that empowers a mobile phone with the capabilities of a network-accessible smart phone.

**World Wide Web (WWW)** – That portion of the Internet that supports specially formatted documents using hypertext (HTML or XTML), featuring "pages" of text, sounds, and images. Also referred to as the Web.

**Write-Once, Read Many (WORM)** – A storage medium in which data cannot be altered or erased once it has been written.

**X.509 Public Key Certificate** – The most widely used standard for defining *digital certification*.

**X-Tec** – A technique to deter the copying of information on a valid *magnetic-stripe* to a counterfeit magnetic stripe by measuring the variations in the magnetic characteristics and comparing them to the measurements recorded on the stripe.

---

**Zones** – Areas of *integrated circuit card* storage designated for free access, specific applications that may each have a different level of access.

# Appendix A

## Smart Card Functionality of Popular POS Terminals

Manufacturer	Terminal	Integrated Smart Card Terminal	Requires Optional Chip Reader	EMV Compliant	Reads Magnetic Stripe	Stored Value Capable	Loyalty Capable
Hypercom	T7P		✓	✓	✓		
	ICE 4000	✓		✓	✓		✓
	ICE 5000	✓		✓	✓		✓
	ICE 5500		✓	✓	✓		✓
	ICE 5500P		✓	✓	✓		✓
	ICE 6000		✓	✓	✓		✓
	ICE 6500		✓	✓	✓		✓
IVI Checkmate	eN-Counter 4000	✓		✓	✓		
	e-Touch 3000		✓	✓	✓		✓
Ingenico	e <sup>N</sup> -Crypt 1200	✓		✓	✓	✓	✓
	Elite 510	✓		✓	✓		
	Elite 730	✓		✓	✓	✓	✓
	Elite 735	✓		✓	✓	✓	
	Elite 770	✓		✓	✓		
	Elite 780	✓		✓	✓		
VeriFone	3350	✓		✓	✓		✓
	2650		✓	✓	✓	✓	✓
	2250		✓	✓	✓		✓
	1450	✓		✓	✓	✓	✓