Beyond Chip Card Migration

Convenience and Security in payment technology

Payment card usage is on the rise globally and with it the adoption of smart card technology. Globally, cards remain the preferred non-cash payment instrument with a market share of more than 55%[i]. Consider that even during the height of the financial crisis from 2008 to 2009 transaction volumes on debit and credit cards were still increasing by nearly +10% (compared to +15% from 2007 to 2008).

As card usage steadily increase so does the number of cards in circulation. By 2016, there will be over 10 billion cards in circulation (up from 7.4 billion in 2011[ii]). Among payment card technologies, chip cards currently represent 2.1 billion of the cards in circulation and will continue to grow over magnetic stripe card issuance. Global interoperability as well as the additional security (over magnetic stripe cards) underpins chip card adoption.

Initially introduced in the 1990s through EMVCo[iii] to combat card fraud, secure bank cards with chips were contact only. The contact plated module of the card requires direct contact with a reader terminal, typically dip readers, to communicate. At the same time, pure contactless chip cards were being introduced in other applications, predominantly public transportation for automated fare collection.

The more recent advancements in secure chip technology allow for near field (contactless) payments with both bank cards as well as mobile phones. The secure microcontrollers, called dual-interface chips, combine both the contact and contactless interfaces in a single chip. Thus a bank cards can be used in contactless mode to conveniently 'tap and pay' as well as in contact terminals and ATMs to leverage existing infrastructure.

Contactless chip cards contain an antenna to communicate using ISO 14443 radio frequency (RF) standards. In mobile payments, the same secure chip is combined with a Near Field Communication (NFC) chip for contactless communication using the same standard.

The dual-interface technology as well as increasing levels of chip performance enables new applications for bank cards emerging. These applications include student ID cards for campus access and payment as well as combinations with metropolitan area parking and public transit. Such cards can even be applied to loyalty activities, such as acting as an event ticket for sporting venues or amusement parks.

What started out as an improvement in payment security over ten years ago for many countries is now rapidly integrating into other facets of consumers' lives. This paper will focus on the key drivers of this evolution:

- *Fraud reduction and security*
- *Multi-purpose cards*
- *Contactless convenience*

Additionally, we will highlight some implementation case studies from around the world.

Fighting fraud by distributing security measures

As more and more advanced technology is at our disposal, crime designed to illegally use or break this technology also becomes increasingly sophisticated and dispersed globally. Therefore it becomes an imperative that countries must work together in ensuring payment security. Currently, the most widely adopted specification is from EMVCo which maintains these for both chip cards and terminals. However, it must be recognized that there is no single solution to successfully combat fraud but rather a series of measures that are can be taken across the system.

Effective fraud prevention is a combination of protective measures and risk mitigations. Protective measures are to secure the front-end, meaning card authentication and authorization, and the back-end processing system where transaction data are held. There are essentially three activities that a system needs to consider:

(1) Protect against counterfeit fraud through mutual authentication of device & terminal

(2) Risk management to reduce the danger of unauthorized payment (lost and stolen cards)

(3) Validate the integrity of the transaction through digitally signing payment data

Historically, payment security concepts placed a great deal of focus on securing the back-end system, in effect taking data and building walls around it. By its nature, storage and managing sensitive personal data centrally makes it prone to attackers who reap greater rewards from their efforts. Additionally, magnetic stripe technology was limited in the security it could offer so the reliance was made on the system.

However, in recent years security breaches at payment processors, such as Heartland Securities in 2009 which 130 million credit and debit cards were compromised and the more recent Global Payment breach in March of 2012 where 1.5 million credit card records were compromised, highlight the massive jackpot when hackers are successful with an attack on the back-end.

Likewise on the front-end, skimming attacks continue to abound with ATM scams or other card skimming scams reported nearly monthly. The cost to processors is high - $140 million for Heartland Security - as well as the cost to financial institutions that lose consumer trust and tarnish their reputation, thereby losing revenue.

The nature of compromises reaches across country borders and demands strong authentication and cryptography from the front-end through the back-end. Compiling to high levels of security, such as Common Criteria CC EAL 5+, ensures that the chips are robust against many different types of common attacks.

Here we will focus here on front-end card specific fraud which considers two scenarios: card present (i.e. in face-to-face transactions) and card-not-present (i.e. payment over the Internet).

Most common card attack scenarios

Card present	Card-not-present
Skimming at POS Criminals use fake readers to skim the relevant card holder data (name, PAN, CVC, etc.) from the magnetic stripe on the back of the card.	**Phishing** Criminals trick account holders into unwittingly divulging their online banking credentials either online through a fake website, via a false email message or over the phone to a bank employee impersonator or fake automated system.
Man-in-the middle Criminals use stolen card data to counterfeit a payment card and use it in an ATM for cash withdrawal or in a face-to-face transaction at a point-of-sale (POS).	**Malware** Criminals install malware (malicious software) on the account holder's computer that enables the fraudster to implement a range of schemes. The malware is installed through email, adware, fake antivirus schemes, and by visiting websites that fraudsters have developed to mimic well established, trusted sites, such as banks, retailers, and credit card companies.

Card present

Financial institutions report the highest incidence of fraud (70%) is from stolen or counterfeit cards and over 50% of that fraud occurs at the POS in face-to-face transactions.[iv] Countries that have implemented EMV, within four years, have seen the reductions in this type of fraud by 69%[v] (UK). Interestingly, since 2004 and over the same period, when Europe and Canada was migrating to chip cards, the U.S. saw an increase in card fraud rates of 70%[vi]. Thus indicating that fraud easily shifts geographically to locations with lower levels of card security, i.e. magnetic stripe.

Also in the U.S. physical tampering/skimming threats accounted for nearly 30% of the data breaches received by the U.S. Secret Service in 2010, up from 10% in 2007. For example, over $13 million (USD) in fraudulent charges and an estimated 2.5 times that of total fraud costs were uncovered through one of the largest global crime rings that operated skimming schemes in restaurants New York City in early 2012.

In October 2012, rogue PIN pad devices were discovered at 60 Barnes and Nobles stores in the US. The company described the breach as one where the devices had been tampered with and implanted with "bugs". This allowed the supposed organized crime ring to capture credit card and debit card PIN numbers. ***Gunter Ollmann from network security firm Damballa says chip-and-pin technology, which is widely deployed in Europe but not in the U.S., would have helped protect the consumers from the attacks at the bookseller that exploited the mag-stripe card format.***

When considering the migration path from magnetic stripe to chip cards, issuers must first consider the chip authentication method, especially for offline authentication, including:

- Static data authentication (SDA)
- Dynamic data authentication (DDA)
- Combined DDA with application cryptogram (AC) generation (CDA)

The difference between using symmetric cryptography for SDA cards and asymmetric (and symmetric) cryptography for DDA cards does not play a role in the hardware security of the chips; the level of tamper resistance must be the same. The main advantages of DDA can be seen in all the cases where the card transaction must be performed offline.

In early 2000, as many countries began their chip card migration, the initial infrastructure rollout focused on supporting offline authentication with contact cards. These contact DDA cards offered the advantage of the flexibility of card transactions being performed offline with additional security against card counterfeiting. Even though the online connectivity between readers and backend system devices continue to increase globally, the offline transaction scenario is not disappearing and is in fact considered a potential attack scenario. Hence, Visa Europe set a mandate that as of January 2015 when it will no longer accept SDA cards.

Cutting the online connection between reader devices and the backend is a possible, especially in wireless systems. In this scenario the SDA card sends static data, i.e., always exactly the same data sets, which can be intercepted by an attacker. The attacker can then write the data to a blank card which can be used in any offline transaction. While a DDA card sends similar static data, it additionally signs this data together with random values generated by the reader. This action proves that the DDA card possesses the correct private key of an RSA key pair. Since this private key is never sent by a DDA card, the attacker cannot know it.

For all these offline scenarios, whether they are required by the actual application, or are enforced by issuers, DDA is clearly more secure than SDA. During the card authentication phase the card delivers a proof of being genuine which can be verified by any reader device without any additional information from the backend system. While SDA and DDA cards have the same level of tamper resistance, the card data, especially cryptographic keys, cannot be read out by an attacker on DDA cards.

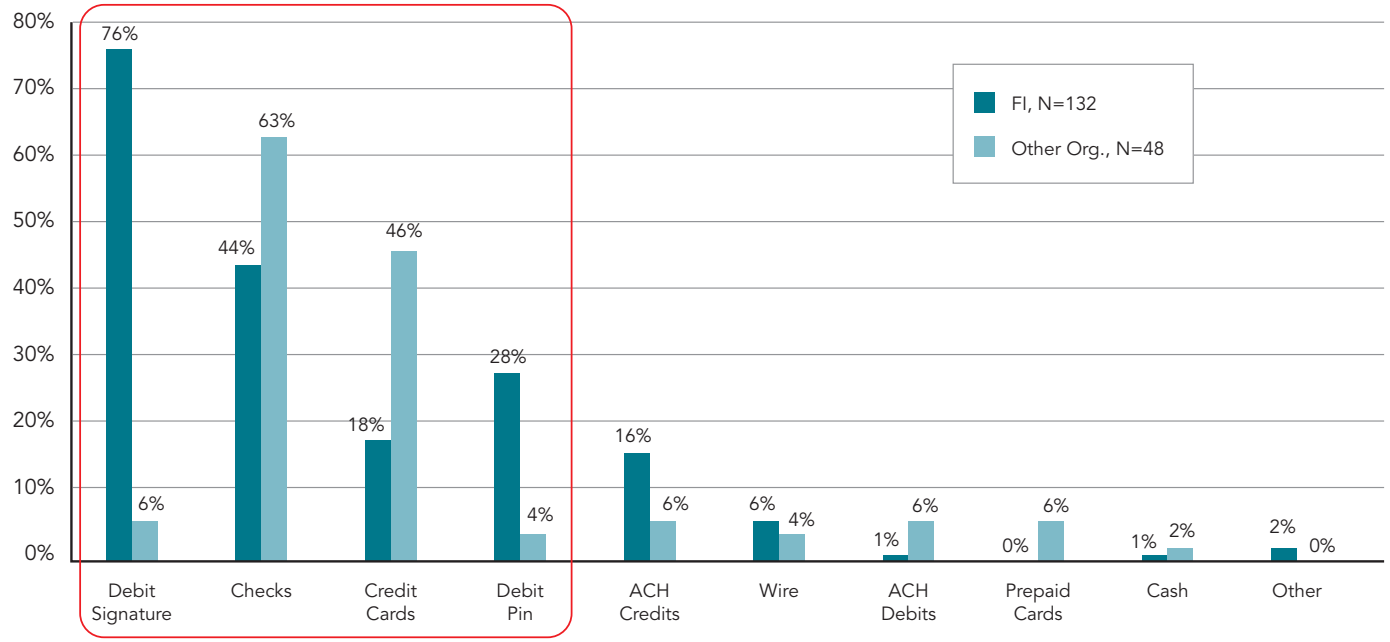
CDA enables the highest achievable security as well as providing a secure fallback in case the online connection is not available (e.g. by an attack or natural disaster). CDA combines DDA functionality with an additional application cryptogram at the end of the transaction to assure the data integrity until the transaction is complete. This prevents the type of fraud in which data is manipulated after the terminal authenticates the card.

Summary table of Authentication Methods

	Static Data Authentification	DynamicData Authentification	Combined Data Authentification
Card Authentification Offline	NO	YES	YES
RSA capability on card	NO	YES	YES
Issuer public key certificate	YES	YES	YES
Card public key certificate & Card private key	NO	YES	YES
Application data	Static signed application details on the card; signed with issuer private key	Signed dynamic aplication data from both the card & terminal with the card private key	"Dynamic signature" using card private key in addition to the "application cryptogram"
Terminal RSA cryptographic processing	Uses issuer public key to authenticate signed static application data	Uses card public key to authenticate signed dynamic application data	
Cardholder Verification	YES	YES	YES
Transaction Authorization	Final transaction cryptogram provided by card. Signature of critical transaction data with card unique DES key. online / offline		
Protection against copy & reuse of data	Limited	YES	YES
Protection against "man-in-the-middle" attacks	None	None	YES

Additionally, EMV specifications also offer an option of security enhancement for PIN transmission. In offline transactions, the reader device sends the PIN to the card in order to get verification. For DDA cards, the security enhancement is to send this PIN not in plaintext, but rather to encrypt it with the card's public RSA key. This option is not available for SDA cards. Transmitting the PIN in plaintext always has the risk of its interception by an attacker, especially in use cases where the connection is wireless. As seen from the table below, eliminating signature as well as additional PIN security would reduce fraud.

Payment Types with the Highest Number of Fraud Attempts[viii]



FI indicates Financial Institution

It is well known that the protocol for PIN verification on the card is vulnerable to man-in-the-middle attacks, since the response of the card to the reader is not authenticated. To be more explicit, the reader asks the card for PIN verification and the response "yes/no" is sent without security measures. This enables a man-in-the-middle in the communication between card and reader to intercept a "no" response and replace it by a "yes", so that the PIN verification is effectively bypassed.
For DDA cards, this protocol flaw can easily be fixed: since every DDA card has its private RSA key pair, it can sign the response (together with a random number of a reader in order to avoid replay attacks) and the attack is no longer possible.

Card-not-present (CNP)
There is a great deal of emphasis placed on card-not-present fraud, especially in the context of EMV migration. One reason is because worldwide e-commerce sales are predicted to reach $963.0 billion by 2013, growing at an annual rate of 19.4%. However, in 2012 in Europe and the US, the leaders in e-commerce globally, online retail transaction represented only 8.8% of all retail transactions. The second reason is due to security measures on the merchant side of websites not being consistent, with some not even requiring CVV codes. For instance, in the UK CNP fraud now accounts for 62% of all fraud on UK issued cards, up 30% from 2004. Measures such as 3D Secure, an XML-based protocol for authentication in Internet based card payments, are showing a steady decrease in online fraudulent transactions.

Although not used today, in the future the public key cryptography capability of DDA chips will be a good starting point for secure Internet card transactions. The public key offers in general more flexibility in various scenarios. When public key infrastructure is available, all card data can easily and securely be transmitted in an open network (i.e. card data does not have to be sent in plaintext to the merchant). It can be encrypted and signed so that fraud by intercepting the data and using it in another context is not possible. Every entity possessing a valid key pair then becomes a natural point for end-to-end security applications.

What is unique is that sensitive master keys are not needed in the complete payment process at all. They are only necessary for personalizing and signing the cards. These keys can be stored separately from the backend. Therefore, it is possible to design a distributed backend system. One part is responsible for personalizing cards while the other one is involved in the payment process. A corruption of the payment backend or a terminal does not lead to a disclosure of sensitive master keys or corruption of cards.

General advantages of public key infrastructure:

- Enables offline transactions
- Secret key at backend not necessary for transaction; can be secretly stored at other location or even be destroyed
- No secret data on terminal necessary
- Distributed Backend possible
  - Break of backend does not compromise cards
  - Break of terminal does not compromise card or backend
- Credentials like PIN can be transmitted encrypted to the card

Multi-purpose cards ring in new opportunities

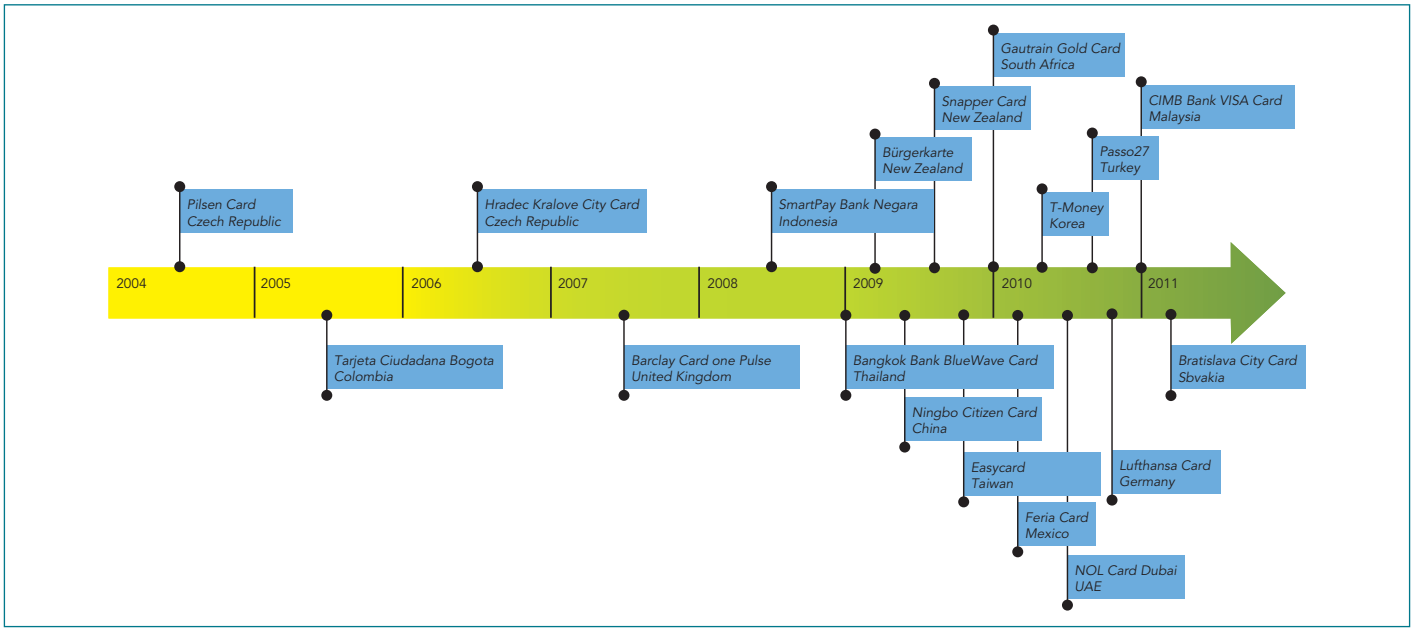
As many countries around the world have completed their chip card migration with contact cards, they are now considering ways to leverage the latest in dual-interface technology to support new applications of payment cards. This will capture additional revenue (over cash) and improve consumer preference for bank cards (top-of-wallet effect).

What is critical for a multi-purpose card to be successful in improving the consumer experience is the performance of the chip. Simply stated, all chips are not created equal. Performance is a function of how quickly the chip is able to handle all the data processing for a speedy transactions, typically <300 milliseconds for transport cards and <500 milliseconds for standard payment cards, as well as from how far away it can communicate with the reader (>4cm). Compatibility with POS terminals is also a factor in the speed of a transaction; NXP secures over 90% of the POS readers worldwide as well as over 25% of banking chip cards so is able to establish benchmarks.

As chip card technology has advance and the performance and security measures have consistently improved, more and more multi-purpose card combinations are possible. With the speed of chips used in bank cards now reaching <300 milliseconds, this allows bank cards to provide convenience and swift movement through transport turnstiles as well as contactless Point-of-Sale (POS) terminals in convenience stores or fast food restaurants as well. An American Express study found contactless transactions to be 63% faster than cash and 53% faster than using a traditional credit card. (end note reference: "The What, Who and Why of Contactless Payments," Smart Card Alliance Paper, Nov 2006.

The illustration below highlights the fact that bank cards or underlying bank payment infrastructures are being leveraged with government or local ID functions as well as public infrastructure, most commonly public transport. This allows banks to form new types of loyalty programs to acquire new customers as well as capture new, lesser value, regular spend.

Bank cards with additional applications



In early examples of the Barclays OnePulse in London and T-Money application on multiple bank issued cards in Korea, one can see the bankcard capture spend in regular, smaller value (<US$15) public transport. The Barclaycard OnePulse is a three-in-one credit card: built-in Oyster card, standard Visa credit card, and contactless payment. For Oyster travel, cards are pre-loaded with either a season ticket (e.g. a Travelcard or bus pass). Contactless purchases under £15 use the Visa contactless system by waving the card over a reader at participating merchants. The chip in the card contains risk management logic for security; prompting a (contact) chip and PIN transaction on occasion. Standard consumer protections associated with credit cards apply to contactless transactions as well to protect consumers in the event of unauthorized transactions.

Another example, the German Lufthansa Senator Card, combines loyalty and identity functions in a card targeted toward travellers. As this segment of consumers typically spends more, it provides travellers a convenient way of collecting related points for hotels and rental cars. With similar payment terms as credit cards, additional Welcome Bonus Miles, integrated travel insurance, and every euro spent on the card equal to one award mile, it becomes a more widely used card.

An emerging segment for dual-interface multi-purpose cards is a student card that combines bank debit or e-purse payment and campus access. The cards provide all the student identification information necessary to access all campus facilities like cafeteria, library, sport venues, etc., thereby replacing an ID card. Off-campus, they can be used as a standard bank debit card because they are linked to a student bank account. This provides an opportunity for a university to reduce card issuance and handling costs, and a bank to provide additional benefits to student account holders.

These new partnership models vary from country to country. For example, in China banks are almost exclusively issuing dual-interface cards to support new customer experiences. What is clear is that these types of models provide benefits for all parties while also sharing costs and will continue to increase in the future. No consistent model applies globally, each type of multi-purpose cards has its unique proposition in each region, each country and sometimes even each city.

Contactless future of payments

The benefits of contactless transactions are two-fold: increasing the speed of transactions for consumer convenience and reducing the mechanical wear-and-tear on infrastructure that leads to lower ongoing maintenance costs. http://www.atmmarketplace.com/article/194927/Five-reasons-to-keep-an-eye-on-contactless. A CVS study found that contactless transactions take one-third to one-half of the time of traditional card reader transactions. Another marketing firm, Simon-Kucher & Partners, found that it takes 12 seconds for a contactless transaction to be completed, but 27 seconds to make a chip-and-pin payment. Even at the ATM, contactless PIN entry could speed up transactions as well as drastically reduce the number of cards inadvertently left in dipping card machines.[xiii]

In a recent Visa Contactless Barometer[x] report, consumers indicated that they view contactless cards as a stepping stone to mobile payments. Contactless owners value the convenience and ease of contactless payments, but the current relatively low acceptance levels in some markets is still preventing usage from becoming an everyday habit. This is supported by the current contactless reader market penetration rates, which were only 8% in 2011.

However, it is expected that within the next five years chip card reader penetration and card issuance will come together. By 2017, globally chip card reader penetration is expected to be 53% with 86% of this global figure in the US and 78% in Europe. Many readers are enabled with contactless functionality already and simply require a software update to activate it. Contactless payment with dual-interface cards (as opposed to pure contactless cards) is growing dramatically. By 2017, dual-interface cards are expected to represent over 50% of the banking chip cards in circulation.[xii]

There are often concerns about the security of the contactless interface. While contactless chip card technology provides increased advantages in card reliability and user convenience, it also introduces new challenges with respect to privacy and security. The main difference between a contact only chip card and a chip card equipped with a contactless interface is the possibility of unintended readout processes.

With a contact card the user actively puts the card into the reader and demonstrates willingness to do the transaction. With contactless cards there is no such declaration of intention. If no additional logical protection is present on the contactless interface an attacker could read out the data on the card without knowledge of the user. Hence, it is essential that payment cards are personalized such that not all information can be read out, especially the card holder name. Combining the cardholder name together with the accessible information from the card (e.g. the Primary Account Number), an attacker could successfully complete a Card Not Present transaction. In other contactless applications, such as electronic passports, additional protection mechanisms have been introduced. It is only a matter of time before these safeguards are applied to payment protocols too.

Also, contactless transactions can be experienced with near field communication (NFC) technology, of which NXP is a co-founder. NFC is a set of standards for smart phones and mobile devices to establish radio communication with each other by touching them together or bringing them into close proximity of other NFC enabled products or devices. While contactless transactions with a smart phone or mobile device create convenience, it also raises misguided perceptions about the lack of security. A reference platform for security in mobile has been established by taking the same security standards of CC EAL +5 as used for ICs in bank cards and passports. This Secure Element is a chip component that offers a highly secure environment for storing confidential data and conducting contactless transactions using NFC.

A Secure Element itself contains a secure processor, tamperproof storage and execution memory. Its sole purpose is to enable secure transactions. The Secure Element contains applications (e.g. applets) which rely on secure keys running inside the secure processor. These secured applications and keys, residing in the tamperproof storage, make it possible to securely communicate using the same higher-layer cryptographic protocols used in the payment industry today.

There are several ways a mobile transaction works using the secure element:

1) In card emulation mode, the NFC enabled smart phone appears to an external reader much the same way as a traditional contactless smart card.

2) A physical smart card is typically implemented as an applet and is installed in the secure element in either the embedded secure element or UICC.

3) Service provider applications will interact with the applets in the secure element or

4) Applets will interact with the external contactless reader using ISO14443 APDU commands along with the existing higher level cryptographic protocols used for physical smart card payments.

When using a mobile device as a contactless payment card the mobile device is operated in card emulation mode and behaves exactly like a contactless smart card. The form factor mobile device gives some additional possibilities to protect the contactless interface against unintended readout of the user credentials. The card emulation and the contactless interface can only be switched on when the card is going to be used (typically via an application on the mobile device). With this no unintended read out is possible when the application is not activating the contactless interface (of course this assumes a trustworthy application on the phone, not affected by any malware).

Summary

A secure transaction concept should focus on distributing security measures and ensuring safe passages of encrypted data, starting with authentication. The weakest link in the chain can break the whole system. The IC chips used in cards, mobile devices, and readers are capable of adding increased levels of security around data. Relying on the online connection during transaction in order to establish transaction security makes the backend a single point of failure with the potential of very serious damages if any attack on it succeeds.

Multi-purpose cards bring new opportunities for banks and others to create enhanced experiences for customers. Unleashing the technology will create new partnership and loyalty models for banks to grow their customer base as well as take advantage of the global trend towards cards usage over cash. Performance metrics on the chip, such as those demonstrated by NXP's SmartMX family of products, support such changes to the card holder model.

As contactless payment convenience rises in popularity with both dual-interface cards as well as mobile devices, additional security considerations are being taken into account to protect consumers against identity theft and negligent fraud. This includes protocols for what data is transmitted and also how it is transmitted through contactless cards and mobile devices. Additionally, as fraud is migrating to card-not-present scenarios and Internet retail transactions continue to grow, Public Key Infrastructure (PKI) will play an increasingly important role to securing data flow.

NXP is the leader in creating trusted smart life solutions that authenticate identities, secure transactions and provide convenient interactions. Its strong global market positions in readers, e-government, automated fare collection, bank cards and mobile help to bring forth end-to-end solutions and security on which the industry relies, both now and for the future.

---

i World Payment Report 2011, CapGemini and RBS

ii PAYMENT CARDS Smart Cards, EMV, and Contactless/Dual-interface Penetration into Mag-stripe, ABI research, July 2011

iii EMVCo is the organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002 and with JCB and American Express joining the organization in 2004 and 2009, respectively, EMVCo is currently operated by American Express, JCB International, MasterCard Worldwide, and Visa, Inc.

iv 2012 Payment Fraud Survey, Federal Reserve Bank of Minneapolis, April 12, 2012

v Chip and PIN: Success and Challenges in Reducing Fraud, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012

vi Chip and PIN: Success and Challenges in Reducing Fraud, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012

vii http://www.enterprise-security-today.com/news/Embarrassed-EMC-Buys-NetWitness/story.xhtml?story_id=12300DQHE456

viii 2012 Payment Fraud Survey, Federal Reserve Bank of Minneapolis, April 12, 2012

ix Khan, Imran, Annual report on Internet commerce, Goldman Sachs, 2012

x Dec 2011, The Barometer canvassed perceptions of contactless technologies across the UK, Poland and Turkey, based on surveys of 1,700 banked individuals and in-depth panel sessions with around 500 contactless card owners per market.

xi Berg Insight

xii IMS Payments Report, 2012

xiii http://www.atmmarketplace.com/article/194927/Five-reasons-to-keep-an-eye-on-contactless

Date of release: January 2013

Document order number: 9397 750 17374

Printed in the Netherlands