The Migration of EMV Chip Technology

EMV Implementation in the U.S.
1. Introduction

Most of the world has fully migrated or is in the process of migrating to EMV chip technology for debit and credit payments. According to EMVCo, approximately 1.62 billion EMV payment cards are in circulation globally and 23.8 million POS devices accept EMV cards as of Q2 2012. This represents 45 percent of the total payment cards in circulation and 76 percent of the POS devices active globally [EMVCo2012].

Given the prevalence of EMV chip technology in the rest of the world, many questioned when the United States would move to EMV. U.S. financial institutions started issuing EMV chip cards to their frequently traveling customers; however, the country seemed to be a long way off from acceptance [Gemalto2011]. All of this changed on August 9, 2011 when Visa announced plans to speed up chip migration and adoption of mobile payments in the United States. Visa announced a three-part acceleration plan [Visa2011]. Following Visa’s announcement American Express, MasterCard, and Discover followed suit with statements of support for EMV migration and similar accelerated adoption policies.

1a. EMV Roadmap: Visa

> Expand the Technology Innovation Program to Merchants in the U.S.

Effective October 1, 2012, Visa will expand its Technology Innovation Program (TIP) to the U.S. TIP will eliminate the requirement for eligible merchants to annually validate their compliance with the PCI Data Security Standard for any year in which at least 75 percent of the merchant’s Visa transactions originate from chip-enabled terminals. To qualify, terminals must be enabled to support both contact and contactless chip acceptance, including mobile contactless payments based on NFC technology. Contact chip-only or contactless-only terminals will not qualify for the U.S. program. Qualifying merchants must continue to protect sensitive data in their care by ensuring their systems do not store security codes, track data or PINs, and that they continue to adhere to the PCI DSS standards as applicable.

> Build Processing Infrastructure for Chip Acceptance

Visa will require U.S. acquirer processors and sub-processor service providers to be able to support merchant acceptance of chip transactions no later than April 1, 2013. Chip acceptance will require service providers to be able to carry and process additional data that is included in chip transactions, including the cryptographic message that
makes each transaction unique. Visa will provide additional guidance as part of its bi-annual Business Enhancements Release for acquirer processors to certify that their systems can support EMV contact and contactless chip transactions.

> Establish a Counterfeit Fraud Liability Shift

Visa intends to institute a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions, effective October 1, 2015. Fuel-selling merchants and ATMs will have an additional two years, until October 1, 2017 before a liability shift takes effect for transactions generated from automated fuel dispensers.

Currently, POS counterfeit fraud is largely absorbed by card issuers. With the liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant’s acquirer. The liability shift encourages chip adoption since any chip-on-chip transaction [chip card read by a chip terminal] provides the dynamic authentication data that helps to better protect all parties.

1b. EMV Roadmap: American Express

Following Visa’s announcement of an EMV adoption roadmap, American Express published similar guidelines. The implementation milestones outlined in American Express’ policy match Visa’s with one notable difference in key dates: American Express will wait until October 2013 to grant PCI audits to merchants who process 75% of transactions via terminals supporting both contact and contactless EMV payments. In regard to the fraud liability shift, American Express will transfer liability away from the party that has the most secure form of EMV technology. Like Visa, American Express will give U.S. fuel merchants an additional two years before the fraud liability shift takes effect. American Express has not yet announced dates for which the liability shift will extent to ATM terminals [Amex2012].

1c. EMV Roadmap: MasterCard

MasterCard, too, outlined a plan that closely follows Visa’s roadmap. Like American Express, MasterCard is putting a liability hierarchy in place. This means that the party that implemented the most secure technology will be protected from financial liability for card-present fraud. Under MasterCard’s policy the fraud liability shift will extend to ATM’s on October 1, 2016; a year sooner than under Visa’s plan. Fuel dispensers, however, will have until October 1, 2017 to comply with the new requirements [MasterCard2012].
1d. EMV Roadmap: Discover

In full support of EMV adoption, Discover published an EMV Roadmap that closely matches American Express’ plan in terms of milestones, policy, and key dates. Discover will implement a fraud liability shift in effect October, 2015, giving fuel merchants an addition two years [Discover2012].

With these announcements from the major card issuers, the United States payments landscape is no longer a future of magnetic stripe technology, but one of EMV chip technology and contactless and mobile payments. This paper will examine why the timing is good for EMV in the United States, and will discuss implementation and cost considerations for merchants and issuers.

2. Why EMV and Why Now?

There are many reasons why EMV chip technology makes sense for the United States. These are some of the major factors:

> Physical World Fraud

It is the consensus amongst observers – although there are no published fraud numbers in the U.S. like there are in other domestic markets – that physical world fraud in the U.S. is already above the global average and still on the rise. Furthermore, the lessons learned from the many migration activities worldwide clearly indicate that fraud migrates toward those regions which have not yet migrated to EMV chip technology (Malaysia to Thailand, UK to mainland Europe, etc.). Since the rest of the world has either already migrated to EMV or has firm plans to do so, if the United States did not move to EMV, it could become the primary target of fraudsters and fraud rates will continue to rise. The move to EMV will, in theory, prevent this from happening.

> Cardholder Inconvenience Abroad

With market penetration of EMV technology deployment growing around the world, in particular the nearly 100% coverage in the Single Euro Payment Area (SEPA) and soon to be in Canada, the magnetic stripe technology becomes more and more archaic. Tens of millions of U.S. cardholders have been inconvenienced abroad over the last few years by attendants at POS refusing to take their cards and even more by not being served at unattended terminals [Aite2009].
> Mobile and Contactless

Implementing EMV chip technology in the United States will speed up mobile and contactless payments and make them more secure. The devices that accept EMV chip cards are dual contact/contactless devices. By installing these devices to accept EMV, merchants are also readying themselves to accept mobile and contactless payments as well.

3. What is EMV?

EMV is based on strong cryptography (both symmetric and asymmetric) and elaborate key management; a fundamental EMV principle is to digitally sign payment data to ensure transaction integrity. As opposed to magnetic stripe technology, a chip is extremely difficult to crack; card authentication and PIN verification are performed automatically and objectively by the chip. An important aspect of EMV is its use of dynamic data. Each transaction carries a unique ’stamp’ which prevents the transaction data from being fraudulently reused, even if it is stolen from a merchant’s or processor’s database. EMV’s dynamic data feature basically says ’if you can’t prevent data from being stolen, make the stolen data useless’ because dynamic data is only useful for the sole transaction it characterizes, nothing more.

3a. Fraud and EMV

EMV has been tremendously successful in preventing fraud. Wherever EMV has been implemented comprehensively, including the objective PIN verification by the chip, significant fraud reduction ratios have been achieved and sustained.

The regularly published fraud statistics from many national banking and regulatory authorities such as the Banque de France [www.observatoire-cartes.fr], the UK Payments Administration [http://www.theukcardsassociation.org.uk], and Interac in Canada [http://www.interac.ca], to name a few, clearly prove the point. EMV reduces counterfeit and lost & stolen fraud in the world of physical points of sale (POS) and automated teller machines (ATM) as well as in card-not-present (CNP) scenarios where EMV provides strong, dynamic cardholder authentication.

In fact, EMV is the only available technology to prevent card payment fraud from happening in an efficient, systematic and globally interoperable way. Equally important, no other technology that is advertised as an alternative to EMV has the global deployment and support base and the maturity of EMV. In other words, EMV represents a mature ecosystem with established roles and benefits for all stakeholders:

> The underlying standards have been stable for more than a decade. Any necessary evolutionary changes have been carefully managed in a way that each new release or version is always backwards compatible with prior releases.
This ensures that the significant investments in software, hardware, communication networks and backend systems are protected.

> The standards are complemented by an efficient certification regime executed by EMVCo and the payment systems making sure the cards and devices interoperate worldwide.

> There are a tremendous number of industry suppliers from around the world providing a vast portfolio of certified components. This ensures global competition on price and product quality and innovation.

> Thousands of banks, processors, and domestic and international payment systems in almost every country on the globe have integrated EMV into the fabric of their daily operations; a total of more than 1.62 billion EMV cards and more than 23.8 million EMV compliant POS terminals have been deployed so far. [EMVCo2012]

**EMV Security**

From a real-world fraud-prevention standpoint, EMV is significantly more secure than traditional magstripe cards. Through the use of advanced encryption, embedded card risk analysis capabilities, and online and offline authentication, most of the traditional methods used to steal card data or to clone cards using magstripe technology are rendered worthless, or at the very least, very difficult to accomplish. That said, as with other major EMV rollout initiatives in the UK, Canada, Australia and other countries around the world, the migration to EMV Chip and PIN/Chip and Signature in the U.S. will occur in stages, with merchants, banks, processors and others working loosely towards a singular goal, but at their own speeds.

What this means is that best case card security scenarios—no magstripe fallback, DDA or CDA offline authentication only, smartcard onboard risk analysis capabilities, no manual PIN entry—can’t be assumed. There will be an interim period while the infrastructure is being built, likely spanning several years, where prudent security practitioners will continue to invest in additional security measures such as point-to-point encryption products that ensure Track 1 and 2 data are encrypted prior to transmission and advanced tokenization techniques that replace card data with a random value, thereby protecting merchants from storing unsecured card data while also potentially releasing significant portions of their infrastructure from PCI scope.
3b. When the Card is Not Present

EMV is also helpful for authentication when the card is not present, i.e. online or over the phone. EMV cards and the EMV back-end authentication infrastructure are very well suited as a base for strong, dynamic cardholder authentication using onetime- passwords (OTP). The card can verify the cardholder’s PIN offline, either with the help of a small hand-held card reader device (e.g. Barclays PINsentry [Barclays2013]) or by using a ‘keyboard’ integrated into the card (e.g. MasterCard’s Display Card [Mastercard2010]) and then produce an OTP, which is displayed on the device or on a small display embedded in the card.

During an online transaction, the cardholder transmits this OTP to the issuing bank who is then in a position to verify the OTP using its EMV back-end authentication system. This constitutes dynamic two-factor authentication (2FA) on the base of something you have and something you know. Handheld readers have been distributed to tens of millions of cardholders in Europe and Asia.

When these devices are used, online banking fraud has experienced significant reduction [Silicon.com2008].

It is worth noting that weak authentication in the non-face-to-face world is at the root of much of the negative news on data breaches and identity thefts. Indeed, identity theft has ranked first among complaints to the U.S. Federal Trade Commission for 11 consecutive years, with 1.34 million in 2010, twice as many as in the next category, which is debt collection. Much of that theft could be avoided if authentication in non-face-to-face situations would not only be based on something you know (i.e. something could be stolen from a database) but would be made much stronger by, for example, using OTPs generated by EMV cards.

4. Benefits of EMV to Issuers and Merchants

Issuers are generally liable for card fraud related to face-to-face transactions and therefore benefit from the reduction of direct fraud cost in this channel. One of the most understated aspects of the migration to chip, however, is the
productivity increase on the merchant and acquiring side of the equation. Significant savings result from replacing signed paper slips by electronic records simplifying the handling of fraud, in particular the retrieval of payments records while dealing with chargeback requests. Likewise, the checkout process at the POS, cash handling in general and the cashier’s after-hours balancing procedures are streamlined and shortened.

When CNP fraud is included in the equation, the picture gets even more attractive for the merchants. Merchants are liable for CNP fraud unless they are participating in strong authentication programs based on 3DSecure technology. These programs can be enhanced by the dynamic data features of EMV which also helps to dramatically reduce maintenance and continuous auditing cost for PCI DSS on the merchant side.

5. Benefits/ Considerations for EMV in the U.S.

In the United States, the scene on the security and fraud side is becoming dramatic which is the consensus among observers. Although in the U.S. there are no published fraud numbers like in other domestic markets – physical world fraud in the U.S. is already above the global average today and is on the rise. The lessons learned from the many migration activities worldwide clearly indicate that fraud migrates toward those regions which have not yet migrated to EMV chip technology. The rest of the world has either already migrated or has firm plans to do so. Without the migration plan specified by Visa, the United States would certainly become the primary target of fraudsters, and fraud rates would continue to rise.

A second fraud topic is the theft of personal payment data from merchant and processor data bases. The direct and indirect fraud cost and the cost of trying to protect against these breaches by means of implementing protective measures according to PCI DSS requirements goes reportedly into the tens of billions of dollars [MAG 2010]. In spite of this effort and expense, these massive data compromises continue to occur (e.g., Sony, 2011). On the backs of these high-profile attacks, data clearly shows a growing trend toward breaches occurring in smaller retail sites, albeit for smaller overall gains. But regardless of whether one gets 1 million records from one breach, or 1.5 million from ten breaches, the outcome is the same.

The current security situation in the U.S. card payment industry has already raised significant concerns with the cardholders and the media. As a consequence the U.S. regulators (represented by the FFIEC) are investigating, and they have published a Supplement to the 2005 Guidance entitled ‘Authentication in an Internet Banking Environment’ [FFIEC2011] to ‘reinforce the Guidance’s risk management framework and update the Agencies’ expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment’.
Politicians have turned to the issue, e.g. U.S. Senator Robert Menendez, D-N.J. in a June 15 2011 letter to the head of the OCC which called for a deeper investigation into the breach, asking that the bank’s customer notification policy be reviewed. “As Citigroup’s primary regulator with jurisdiction for data security issues, I hope that you also believe this to be unacceptable for consumers,” Menendez says. “Over the last six years, there have been 288 publicly disclosed breaches at financial services companies that exposed at least 83 million customer records. ... This problem is widespread and must be properly addressed by all parties [Bankinfo2011].”

It is the consensus of industry experts that the industry will be unable to prevent every attack. The use of dynamic data as specified by EMV, however, will make sure that the data that could potentially be stolen is useless to the criminal. The migration to EMV in the United States would therefore put many of the issues mentioned above to rest.

5a. U.S. and Travelers

One of the biggest benefits of the U.S. migrating to EMV is payment interoperability with most of the world.

Market penetration of EMV technology deployment has been growing around the world since 2003. Here are the latest numbers as published by EMVCo as of Q2 2012 [EMVCo2012]:

<table>
<thead>
<tr>
<th>REGION</th>
<th>EMV CARDS</th>
<th>ADOPTION RATE</th>
<th>EMV TERMINALS</th>
<th>ADOPTION RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada, Latin America, and the Caribbean</td>
<td>401M</td>
<td>49.2%</td>
<td>5.6M</td>
<td>78.5%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>372M</td>
<td>26.7%</td>
<td>5M</td>
<td>50.5%</td>
</tr>
<tr>
<td>Africa &amp; the Middle East</td>
<td>50M</td>
<td>28.6%</td>
<td>.6M</td>
<td>76.7%</td>
</tr>
<tr>
<td>Europe Zone 1</td>
<td>755M</td>
<td>80.7%</td>
<td>11.7M</td>
<td>94.5%</td>
</tr>
<tr>
<td>Europe Zone 2</td>
<td>46M</td>
<td>15.5%</td>
<td>0.9M</td>
<td>73.2%</td>
</tr>
<tr>
<td>United States**</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTALS</td>
<td>1.62B</td>
<td>44.9%</td>
<td>23.8M</td>
<td>75.7%</td>
</tr>
</tbody>
</table>

*Figures reported in Q4 2012 and represent the latest statistics from American Express, JBC, MasterCard and Visa, as reported by their member financial institutions globally.

** Figures do not include data from the United States.

It’s true that tens of millions of U.S. cardholders have been inconvenienced abroad over the last few years by attendants at POS terminals refusing to take their cards and even more by being unable to buy gas at unattended terminals or transportation tickets at ticket machines (and therefore being forced to join the usually long lines at the...
few remaining - if any - attended ticket booths. U.S. media are more and more frequently covering the issue, not only via the trade press but also in daily newspapers.

The New York Times, as another example, published a feature article in its popular travel section on June 8, 2011 stating: `Until businesses change their minds, American travelers will continue to encounter payment issues abroad. The problem is two-fold. Even though most European cash registers are equipped to handle American cards, some cashiers simply don’t know how to process them. And many automated ticket kiosks like those commonly found at train stations, gas pumps and parking garages simply don’t accept cards without a chip and PIN` [NewYorkTimes2011].

The negative trend vis-à-vis acceptance of magnetic stripe cards will be aggravated by the recent resolution of European banks - at the request of their regulators at the European Central Bank - to eliminate the magnetic stripe from European cards altogether and/or to allow merchants generally to reject magnetic stripe card based transactions. Europeans on the other hand will resort more and more to cash when they come to the U.S. when their debit and credit cards no longer work because of the absence of the magnetic stripe [NewYorkTimes2011].

Although the traveler payment problem has been felt for quite some time, it is hopeful that it will be resolved as the U.S. continues the EMV migration.

5b. Costs

The business case for implementing EMV technology has changed for the better over the last couple of years:

> The direct cost of fraud in the U.S. is on the rise. Additionally, the industry needs to fully acknowledge that the cost of fraud is not limited to the direct net fraud losses; fraud management expenses contribute rather substantially to the overall fraud cost. Visa suggests that indirect fraud costs are “at least equal to direct fraud losses, and can often be much higher” [Visa2009]. Visa also claims that “opportunity costs, which include the behavior of cardholders subsequent to experiencing fraud, vary considerably — but can easily account for more than 15 percent of total fraud costs.”

As said before, the cost of the alternative measures that the U.S. payment industry uses for detecting and mitigating fraud as described above have been growing significantly. For instance, as a result of the well known mass data compromises, millions of cards had to be reissued, and customer service costs for issuers and merchants have been increasing. Most of this can be avoided through a proper and comprehensive implementation of EMV. Consequently, Visa has waived significant parts of PCI maintenance and continuous auditing for those merchants who perform
more than 75 percent of transactions in EMV mode outside of the United States, and will now do the same for U.S. merchants.

> The cost of chip cards has decreased considerably over the last couple of years as a result of growing card production capacities, maturing card manufacturing technology and the decreasing prices of the integrated circuit chips. Certainly, the financial industry has benefitted in this regard from the fact that EMV chip technology is very similar to the technology supporting billions of mobile phones.

> Similarly, the cost of payment and POS devices has come down significantly. Furthermore, a substantial proportion of POS devices in the U.S. market already contain chip-reading hardware capabilities onto which EMV software can be downloaded. This situation improves with every new EMV capable device shipped as part of the standard POS device maintenance cycle.

> Most of the big issuers, acquirers and processors in the U.S. are already issuing chip cards and/or are acquiring EMV transactions based on the fact that they are operating in EMV territory abroad and have had to adapt as a result. They are at least familiar in principle with the impact of migrating to EMV, and most of them have modified at the very least their international issuing and back end systems to integrate EMV.

5c. Moving at the Same Pace

With their announcements, Visa, American Express, MasterCard and Discover are urging issuers and merchants to move at the same pace, which is positive for the United States. In order to optimize the business case of the two market sides, issuers and acquirers / merchants / ATM providers have to move in lock step. In order to achieve this, the stakeholders are well advised to consider forced replacements of cards and devices outside of the normal replacement cycles. The additional investment has a clearly identifiable return. It is even more important to initiate the migration of the ATM installed base synchronously with the cards and devices. If ATMs are not made EMV compliant in sync with the POS devices, the life of the magnetic stripe technology will be prolonged and ATMs become the single point of failure (or fraud for that matter) in the card payment system. This is clearly demonstrated by the cross border fraud migration problems encountered in other parts of the world; the U.S. should benefit from these lessons and not commit the same mistakes.
5d. Contactless and Mobile Payments

Contactless and mobile payment transactions are based on the EMV specifications. This relates to their functionality and transaction flow as well as to the associated security fundamentals. As a result, a mobile transaction is no different from a card transaction at the POS. Enabling the device side to perform contactless and mobile transactions means to implement these new features and security measures and change hardware and software of the devices.

The penetration of contactless terminals supporting proximity payments in the U.S. market is still very low today [at present, only about two percent of the roughly 7 million card-accepting merchant locations in the United States have been equipped with contactless POS terminals since the U.S. contactless-payment rollout began seven years ago [NFCTimes2011]]. This means that the bulk of the hardware and software upgrades are still in front of the industry in order to make contactless and mobile payments a success. It would only take a small incremental investment to also provide EMV contact transaction capabilities in these new devices and thereby open up the U.S. acceptance infrastructure for the globally accepted EMV standard represented by more than 1.62 billion cards as of today.

In other words, the U.S. migrating to EMV devices supporting EMV contact and contactless would bring mobile acceptance as a bonus. The issuing side can then decide whether to issue dual interface cards (contact & contactless) and/or support mobile payments.

6. Summary and Resources

Before Visa’s announcement, there was already a lot of support for EMV in the United States. Wells Fargo, JPMorgan and U.S. Bancorp, State Employees Credit Union, United Nations Credit Union, Silicon Valley Bank and others had started (or have announced to start) issuing EMV cards to their cardholders. In August 2011, Visa announced plans to accelerate the United States’ migration to EMV payment technology and mobile payments. American Express, MasterCard, and Discover have announced plans similar to Visa’s in support of EMV migration. These announcements significantly changed the payments landscape in the United States from a future of magnetic stripe payments to one of EMV contact and contactless and mobile payments. Moving to EMV will significantly reduce fraud, has the potential to make CNP transactions secure, and will make U.S. payments interoperable with most of the rest of the world. Because
of lower costs of terminals and cards, as well as Visa’s TIP program, migrating to EMV will be easier and less costly than it was a few years ago.


References:

- [Visa2009] Payments Cards and Mobile, September/October 2009 Fraud Supplement
Contact

For more information on this white paper or to reach Gemalto directly, please refer to contact information listed below.

Gemalto, Inc.
Arboretum Plaza II
9442 Capital of Texas Highway North, Suite 400
Austin, TX 78759

Phone: 888.343.5773


About Gemalto

Gemalto (Euronext NL0000400653 GTO) is the world leader in digital security with 2012 annual revenues of €2.2 billion and more than 10,000 employees operating out of 83 offices and 13 Research & Development centers, located in 43 countries.

We are at the heart of the rapidly evolving digital society. Billions of people worldwide increasingly want the freedom to communicate, travel, shop, bank, entertain and work – anytime, everywhere – in ways that are enjoyable and safe. Gemalto delivers on their expanding needs for personal mobile services, payment security, authenticated cloud access, identity and privacy protection, eHealthcare and eGovernment efficiency, convenient ticketing and dependable machine-to-machine (M2M) applications.

Gemalto develops secure embedded software and secure products which we design and personalize. Our platforms and services manage these secure products, the confidential data they contain and the trusted end-user services they enable. Our innovations enable our clients to offer trusted and convenient digital services to billions of individuals. Gemalto thrives with the growing number of people using its solutions to interact with the digital and wireless world.