ABnote™
Since 1795

Frequently Asked Questions About EMV

An EMV Guide

What is EMV?

EMV is an open-standard set of specifications originally developed in 1996 by Europay, MasterCard and Visa that defines requirements to ensure interoperability between chip-based cards and terminals. Today, EMVCo (www.emvco.com), owned by American Express, MasterCard, JCB, and Visa, manages and updates the specifications.

What countries have adopted EMV?

Most of the world, with the exception of the United States, has adopted or is actively adopting EMV. All of Europe, most of the Middle East, parts of Asia and Africa, Canada, Mexico, Brazil, Chile, and Canada have either migrated or in the process of migrating to EMV. Parts of Asia, Latin America, and the United States do not yet support EMV. The United States is the only G20 member nation that has not migrated a significant portion of the card base to EMV.

As of Q4, 2012, EMVCo estimates that 1.62 billion EMV cards have been issued globally, with consumer adoption rates ranging from under 20% to over 80%.

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	401M	49.2%	5.6M	78.5%
Asia Pacific	372M	26.7%	5M	50.5%
Africa & the Middle East	50M	28.6%	0.6M	76.7%
Europe Zone 1	755M	80.7%	11.7M	94.5%
Europe Zone 2	46M	15.5%	0.9M	73.2%
United States†				
TOTALS	1.62B	44.9%	23.8M	75.7%

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

† Figures do not include data from the United States.

How does this affect travelers with mag-stripe only cards (like Americans) who travel to Europe?

Although mag-stripe cards should work in regions that have deployed EMV, American travelers have reported issues when using a magnetic stripe card while traveling in Europe, Canada, or other regions that have adopted EMV. The most common problem is when trying to pay at a self-service kiosk such as gasoline, transit or parking. It is estimated that in 2008 banks lost $447 million in revenue because of international acceptance issues. [1]

How is EMV more secure?

With EMV, a microchip is embedded in the credit card or debit card – making it a "smart card". A chip not only holds significantly more information than a mag-stripe card, but can support end to end encryption as well as dynamic and static authentication, and offline and online authentication. Furthermore, the microchip is extremely difficult to copy or counterfeit, which helps to prevent replay attacks, a common approach taken by fraudsters when cloning mag-stripe cards

How exactly does it work?

With an EMV card, the chip not only processes the information, but defines the rules for payment, allowing the card to work online in conjunction with the terminal or offline. The process of an EMV transaction is similar to a mag-stripe transaction, but security is enhanced in all three areas – card authentication, cardholder verification, and transaction authorization –

- Card authentication online is managed through a dynamic cryptogram or offline with a terminal using Static Data Authentication (SDA), Dynamic Data Authentication (DDA), or combined DDA with application Cryptograph Generation (CDA).
- Verification of the cardholder is done through one of four different supported methods – offline PIN, online PIN, signature, or no cardholder verification method. The issuer can prioritize cardholder verification methods (CVM) based on the assessment of the relative risk. For example, no CVM is acceptable for unattended devices with low transaction amounts, such as parking.
- Transaction authorization is based on issuer-defined rules. Online transactions are initiated in a similar fashion as magnetic stripe cards – the information is sent to the issuer, along with a transaction specific cryptogram, and the issuer authorizes or declines the transaction. Offline EMV transactions take advantage of parameters that are defined in the card to determine whether the transaction can be authorized.

In a contact payment situation, the chip must come into physical contact with a terminal to initiate the transaction. The terminal enforces the rules set by the issuer through an offline protocol that includes reading and authenticating the data, verifying the user, and checking the floor limit of the card. The transaction is then declined or approved offline, or it moves online. When going online, the terminal sends a request to the issuer for authorization, including any optional authentication and verification defined by the issuer.

In a contactless payment situation, the steps are similar, but the transmission process is faster. In addition, some steps might happen when the card is no longer in the proximity of the reader.

What's going on in the United States – why haven't we adopted EMV already?

To date, the business case for adopting EMV in the U.S. has not been compelling from a cost perspective. EMV cards are marginally more expensive to produce, raising costs for issuers; and require EMV compatible terminals, a cost that would be borne by merchants and their acquiring partners. In addition, the US always processes transactions in an online environment. This means the authorization is always completed in real-time and validated by the host processing system.

It is estimated that the cost of replacing cards will be in the billions and the cost of replacing terminals will be even more. Although the total cost of reported fraud has been steadily growing in the United States, reaching $3.56B [2] in 2010.The U.S. also presents a more challenging situation than Europe or Canada, with roughly 8,000 banks, and a more complex payment infrastructure that includes over 14 Debit payment networks. And finally, there has been no United States government mandate.

What is the plan in the U.S.?

However this situation is changing, and will continue to change. The Durbin amendment, enacted in 2010 as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act, reduces the 1 - 2% transaction fee percentage that issuers can charge. Although this has increased profits for retailers, and potentially provides consumers with a savings, it reduces revenue for issuers, and changes the ROI when looking at the cost of fraud vs. the cost of implementing EMV. Furthermore, card fraud is actually increasing in the United States as it migrates from regions that have implemented EMV, so there is increasing pressure on issuers and merchants, as well as a more compelling cost justification.

The card schemes, including Visa, MasterCard, American Express and Discover have all recently announced changes in their liability guidelines and this affects issuers and merchants. Essentially if an

issuer has issued an EMV card and the merchant does not accept EMV cards, the merchant is liable for any fraud related to that transaction. The incentive is for both issuers and merchants to update their card platforms and acceptance infrastructure to support EMV card based transactions.

The increased interest and acceptance of NFC and mobile technology is also triggering demand for EMV as a more secure solution for contactless payment, as is competitive pressure from non-traditional payment entities, such as Google, PayPal, Amazon and others.

It is now viewed as a certainty that EMV will be adopted in the United States. The major issuers are planning for migration to EMV, and have defined key dates and milestones for this transition.

What are the key dates for the US market?

A number of American banks, including JPMorgan Chase, Wells Fargo, U.S. Bank, and Citi Commercial Cards have already begun to offer EMV enabled credit cards and/or dual chip and contactless payment cards to selected cardholders. Although migration to EMV in Europe and Canada took time – approximately 7 to 10 years from inception to completion – most experts feel that the United States will be able to move much faster. We will be able to take advantage of the experiences of other regions, and the expertise gained by all parties.

The target dates that have been defined differ by issuer, and are still subject to change, but some of the key dates are:

- October, 2013 – A partial liability shift (50%) will be implemented in the event of a data breach at the merchant, depending on whether the merchant is using EMV-enabled POS devices. The amount of protection will depend on the level of EMV supported (MasterCard)
- October, 2015 –Liability will shift to acquirers for fraud if the merchant does not have an EMV-enabled POS device. Fuel dispensers are not affected. (Visa)
- October, 2015 – Full liability shift will take effect if the merchant (with the exception of fuel dispensers) is processing 95% of its transactions on EMV devices. (MasterCard)
- October, 2017 – Liability shift takes place for transactions generated at fuel dispensers. (Visa and MasterCard)

There are also defined dates for PCI Audit relief based on the percentage of transactions coming from EMV-enabled devices, as well as ATM Counterfeit Liability Shift that MasterCard has defined.

What do issuers have to consider when migrating their card base to EMV?

Because EMV provides a number of different options, with the goal to support implementation flexibility, issuers need to be aware of five key areas when determining their implementation methodology. These are –

- Card Interface – will it be a contact card, or a dual interface card? Although this decision will be driven by strategic business goals, it will impact the personalization of the card. Consideration should be given to where the card will be used – exclusively in the U.S. or in other regions, as typical usage and contactless standards will differ. Although there is an additional cost, dual interface cards undoubtedly offer the optimal flexibility and allow for potential other applications to reside in the chip (i.e. transit).
- Key Management Practices – as the security of the card has increased, the requirement for more robust key management practices and exchanging of keys between processers, card manufacturers, issuers, acquirers and associations becomes more complex.
- Offline PIN vs. Online PIN – There are a number of methods to support PIN, including plain text or enciphered text for offline PIN. Management of offline PIN also needs to be considered, as the PIN will need to be delivered to the user, and will have to be reset and unlocked.
- Personalization System – Because EMV cards require additional software and a hardware module for EMV data prep and key management, issuers need to consider the hardware and software and how it relates to the process of EMV issuance.
- Host System – Issuers will need to process the chip data, or use the data processing service from the payment brand. Some companies, like the payment associations offer on behalf services for processing of EMV data to make the host migration easier to implement.
- Transaction Authorization Process – Because an EMV transaction process uses dynamic data for authentication, in contrast to the static data used by a mag-stripe card, the issuer needs to consider the transaction authorization process and define parameters for both offline and online authorization.

How long does a standard EMV project take for Issuers and what are some of the key considerations?

Depending on the complexity of the project, the number of card products and BIN's being migrated a project can take anywhere from 3 months to 6 months to be implemented. Some of the key decisions an issuer has to make include:

- Chip product selection (SDA, DDA, CDA,)
- Centralized bureau services vs in-house personalization
- Card platform host upgrades, how extensive and whether to use on behalf services
- PIN management capability – offline vs online PIN
- Card profile decisions
- Internal testing requirements
- Gradual migration or large scale reissuance

There are a number of factors an issuer needs to consider. Partnering with an organization that has been involved in hundreds of EMV projects will allow an issuer to work with a company that has experience and can assist in determining some of these decisions.

What is the relationship between contactless and EMV?

EMV cards can support contactless transactions, and in fact, contactless communication protocol specifications have been defined by EMVCo. Since both contact and contactless transactions can take advantage of EMV cryptogram security, using EMV in a contactless situation provides additional security.

Although an EMV enabled card can be a contact only card, or a dual-interface card, contactless only cards will not be supported because issuers can perform certain updates only through a contact interface.

How do NFC mobile payments relate to EMV?

Secure mobile payments require a similar infrastructure to EMV, and EMVCo is actively defining the requirements for mobile transactions, collaborating with industry groups such as the NFC Forum, the GSM Association and GlobalPlatform.

Put simply, an NFC enabled mobile device implements EMV through the same process as a contactless card, with the payment application stored on the Secure Element (SE) of the smart phone.

There are a number of advantages with mobile contactless payment. Not only is it faster, but NFC enabled smart phones can support additional methods for cardholder verification, including the ability to add an offline passcode that is verified by the mobile device. Mobile devices can support more than payment, so issuers and merchants are able to provide value-added services such as coupons and loyalty programs. Furthermore, a smart phone can manage multiple payment cards and related services – something that's clearly attractive and beneficial to consumers.

How will EMV change in the future?

The high level strategy of EMVCo is to support secure payment transactions through any method, including what we have now and what we might have in the future. Although a good deal of this is unknown, there are several areas that are currently being looked at, and are likely to continue evolving:

- Enhancements to security and key management — EMV uses asymmetric RSA7 public key cryptography for offline transactions. In order to stay ahead of attacks, the key lengths are regularly increased, which then impacts performance. Therefore EMVCo has identified Elliptic Curve Cryptography (ECC) as an alternative to RSA, and is developing a plan for migration to ECC.
- Mobile Technology — As contactless payment and the use of NFC enabled mobile devices continues to grow, EMVCo will move forward with mobile related specifications, including defining architecture, establishing requirements for mobile handset requirements, user interfaces, and the secure element.

[1] Smart Card Alliance EMV:Facts at a Glance

[2] The Nilson Report, Nov. 21, 2011

