What is EMV?

This paper provides a thorough explanation of EMV, its benefits, the impact to the financial services industry and the deadlines involved.

EMV and smart card technology

Since the introduction of chip card technology, smart cards have been seen as the ultimate replacement for the magnetic stripe cards used for credit and debit applications worldwide.

Magnetic stripe cards in the 21st century have been developed and enhanced to the point that there is now little or no scope for further security enhancements for the prevention of fraud. Subsequently the level of card related fraud continues to grow globally and as a result leading card schemes, Europay, MasterCard and Visa (EMV) have started looking at alternative technology.

Following their initial analysis, the concept of 'chip and PIN' card technology was introduced. This simply requires the embedding of a computer chip on the plastic card. This new approach offers a number of significant benefits to the cardholders, retailers and financial institutions including:

- Improved transaction processing
- Advanced security features
- Greater control of the security through advanced software application

In the late '90's, an EMV mandate instructed that all financial institutions move to chip card technology. Specifications were released for issuers, acquirers and software suppliers. These specifications formed the basis for conformance to the new EMV requirements. EMV, as the standard is now known, aims to ensure that:

- All cards and terminals used globally are compatible with each other
- The same terminal and card approval processes can be used worldwide
- The standards are fully open and published

These basic provisions ensure that there is a global acceptance and compliance with the standard.

The two main security features of EMV are:

- Card Authentication Method (CAM) - protects the card against counterfeiting
- Card holder Verification Method (CVM) - protects against lost and stolen cards. This involves online mutual authentication - the means by which an issuer can satisfy himself that a transaction has come from a specific and authentic card and that the approval/decline response has been sent by the authentic issuer.

Benefits of EMV smart cards

EMV smart cards have a number of secondary benefits to financial institutions:

- **Reduce costs**
  US cost models show that magnetic stripe cards cost US $12 to deliver to consumers and that credit cards are retained for 2 years. An issuing bank's ROI is 1.5 years, leaving only 6 months to profit from the customer. Smart cards cost US $16 to deliver, but the ability to update the cards without reissuing, increases the length of time a card is retained, and so increases the bank's profitability.

  EMV smart cards can be reconfigured after being issued. With the current magnetic stripe cards, a new card must be issued in order to change a customer's offline limits. However, with an EMV smart card, a script can be sent to the terminal which updates the configuration of the card. This allows different limit rules to be stored and applied by the card in offline mode thus saving the bank the cost of reissuing the card.

  The ability to enforce sophisticated offline limits means that more transactions can be performed offline, which typically is more cost effective than having to service transactions online. This secure offline processing can be particularly advantageous for peak periods such as summer sales, as it allows the bank to smooth peak usage efficiently – effectively supporting the same peak load with fewer resources.

- **Increase revenue streams**
  Chip cards provide the means to process multiple applications via the smart chip on each card. These "mini-computers" can provide the user with value-added services including loyalty schemes and e-purse – all via the one card. This provides the issuer with an infrastructure for new income streams.

With these benefits in mind, card industries are pushing for issuers and acquirers to become fully EMV compliant by offering incentives for early migration. Visa has also introduced the EMV Visa Early Option scheme (Chip card data managed by Visa), which is quicker and cheaper for organisations to participate in while they prepare for full migration.

For markets where fraud is relatively low and hence the cost of EMV implementation is difficult to justify, card organisations have a three pronged approach:

- EMV TIFT initiative: When the card is acquired at an EMV terminal, the interchange rate payable by the acquirer to the issuer is decreased by 10 basis points of the transaction value
- Liability shift to non EMV party: In the event of a disputed transaction, the party who has not implemented EMV is liable for the cost of the transaction.
- Financial incentives where each EMV region is offered funds to help banks offset the costs of migration to EMV

Impact of EMV

As with the advent of any new technology, there are some affects on infrastructure and deployment:

- **Personalisation**
  Issuing institutions must have the capability to personalise chip cards and load them with the payment application. This will typically require an upgrade to the card embossing/encoding applications. An alternative for low volume issuers is to consider outsourcing card production to a third party processor or partner bank.
- **Payment network interfaces**
  EMV compliant systems need to process larger payment network messages which includes the additional security information generated by the chip. This may require an upgrade or reconfiguration of the interface between the issuing system and the payment networks.
- **Card management**
  The card management system should be capable of interpreting and performing authorisation based on the additional security information (Authorisation Request Cryptogram) generated by a chip based transaction. The card management system must also be able to generate post issuance updates on the chip as well as issuer security information before performing any post issuance updates.
- **Device upgrade**
  Institutions will need to upgrade their banking devices, such as ATMs and POS terminals. ATMs with card readers will need to be deployed with EMV compliant software. Similarly POS terminals that support chip cards will need to replace all existing POS terminals.

EMV deadlines by region

Region	Visa	MasterCard
EU	1 January 2005	1 January 2005
Middle East	1 January 2006	1 January 2006
Asia Pacific	1 January 2006	1 January 2006
Caribbean	1 January 2010	1 January 2005
Latin America	1 January 2008	1 January 2005
Africa	1 January 2006	1 January 2006
South Africa	1 January 2006	1 January 2005

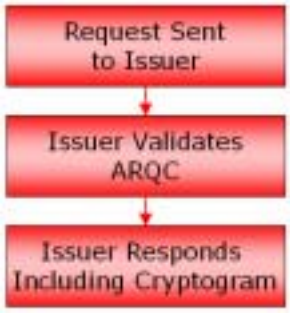
EMV card technical information

This section provides additional technical background and details the processes that take place when an EMV card is entered into an EMV terminal.

1. Card entered into terminal
2. Terminal interrogates it to see which applications are present. Data on an EMV card is organised in structures similar to the directory structure of a PC. The interrogation process is not dissimilar to a PC program searching a PC directory structure to determine which files it can read.
3. Terminal software will offer the terminal operator the selection of available applications.

For this example we will use a Visa terminal that communicates with the Visa VSDC (Visa Smart Debit Credit) application.

4. Terminal will default to VSDC application as this is the only application common to both terminal and card
5. Card holder performs purchase
6. Terminal can perform purchase offline (if it is below a floor limit) or online.
   Floor limits are defined by two fields – counter and amount - stored on the card. These fields are used to limit the risk associated with offline transactions
   - The *counter* represents the number of transactions that can be performed offline before the card must be used online. Each time an offline transaction is performed, the counter is decreased by one. Once the count reaches zero the next transaction must be performed online. If this is not possible the terminal will decline the transaction. Whenever the card is used online, the counter is reset to its original maximum value.
   - The *amount* field represents the financial risk that the card issuer is willing to take on offline transactions. Each time a transaction is performed offline, the card will reduce the offline amount by the transaction amount until no offline limit remains. At this point the card will again request the terminal to perform an online authorisation. Again, if the terminal is unable to perform an online authorisation it will decline the transaction.
7. In order to perform transaction online, card generates an ARQC. (ARQC is unique to each transaction and is supplied by the card to the terminal)
8. Terminal application uses this value as part of authorisation request
9. ARQC forwarded to acquiring bank
10. Acquiring bank forwards message to issuing bank through Visa payment network.
11. Issuing bank receives message through Visa network
12. ARQC will have been encrypted by card using a derived key based on card details
    The issuer's authorisation software will also derive this key from card details and its own issuer key. This will



only be possible if the card was issued by this issuer using the correct issuer key. If not, the card will be detected as fraudulent and declined. If the card is not fraudulent, the derived key is used to decode the message digest which can then be used to ensure the message contents are valid. This provides further security as if the message contents have been tampered with, the message digest will not match the message and the transaction will again be declined on the assumption of fraud.

13. Issuer authorises transaction by responding to acquirer through the Visa network.
    Part of the response message will include an issuer cryptogram which the card can use to ensure that the response is from the expected issuer. This is important as part of the response can include "post issuance updates" which allows the issuers' authorisation software to update information stored on the card. Currently this post issuance update functionality is primarily used to reset the offline counter and amount fields following an online transaction.

14. Acquiring bank will receive authorisation response through visa network and forward it to acquiring terminal.
15. Terminal will advise card of response
16. Card will verify issuer based on issuer cryptogram
17. Card produces an audit cryptogram to be recorded by terminal.
    The audit cryptogram is a secure value which provides evidence of the activities performed by the card and the terminal. This value can be used to prove the card was present during any disputes and will form part of the information passed to the issuer in the clearing file.