Everything you wanted to know about EMV (but you were too afraid to ask)

By Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

Very few people actually know exactly what EMV is and what it's exactly related to.

Putting it simply, EMV is everything - or almost everything - that rules the chip of your favorite credit or debit (or prepaid) card.

As you may have noticed, the payment card that your bank issued to you, bearing your name, the logo of the bank and one of the famor card brands (Visa,mastercard,etc...) has almost probably a *chip*. A small miniature microprocessor which is visible on the surface of the card and which bears several contactors, forming an interesting geometrical motif.

Why is there such a chip, you probably never asked yourself.

In this article, we will explain and underline all the aspects of EMV, the norm which defines the tasks that this chip must perform.

1 What is EMV in brief ?

EMV stands for Europay-Mastercard-Visa. Europay is no longer an independent brand, it is a part of Mastercard, but at the time EMV was created, in 1995, these three companies were the leaders of the market of payment card brands.

EMV was not created for a futile reason.Bank cards have existed since 1946, when the first bank-issued charge card was created by John Biggins. At first they were only plastic cards with some information engraved and then later they were equipped in 1960 (by IBM) with a magnetic stripe so that the cardholder information could be processed by automatic systems.

Magnetic stripe bank cards became the target of multiple attacks especially because they were easy to clone. In fact it was a child's play or almost to duplicate them.

Such fraud led to potential catastrophic losses for banks, which in turn asked the card brand compensation for the damages, as agreed by the policy of the card brands.

In France and Germany, some inventors, among them Roland Moreno[1] , issued several patents for using a

[1] Roland Moreno (11 June 1945 – 29 April 2012) was a French inventor, engineer, humorist and author who was the inventor of the memory card. (source: wikipedia)

microprocessor (‘chip’) inside a bank card to protect payment information and prevent fraud. As early as 1977 and 1978, Michel Ugon - a French engineer - patented the first microprocessor smart cards. This paved the way to using microprocessors in banking cards. French and German banks were among the first to use such technology with programs such as BZero for instance.

These programs were a bit primitive and lacked several security features. Hence there was a need for a global norm to regulate the use of these microprocessor-based bank cards. This was achieved by the creation of the EMV consortium in 1995.

The goal of the EMV consortium was to be a normative body - developing , publishing and maintaining standards - same as ISO, ANSI or AFNOR for example. As such the EMV consortium mission was to issue the EMV norm, to be implemented by any parties involved in microprocessor-based bank cards.

The “raison d’être" of the EMV consortium was to fight against bank card fraud by offering extremely secure standards and robust cryptographic protocols.

The EMV norm evolved quietly during the years. It is actually widely implemented all over the world. Most countries have deployed a domestic EMV scheme by 2020 and it remains the absolute standard for the security of chip-based credit/debit or prepaid cards.

2 An Overview of EMV technologies

EMV involves a rich field of technologies As we noticed, while the founders of EMV are mostly based in the USA, the technologies and patents behind chip-card technologies are almost all located in France and Germany. EMV is deeply associated with the microprocessor card ,e.g the ‘smartcard’, which is also called ‘chip card’, ‘carte a puce’ (French) or ‘Chipkarten’ (Germany).

EMV specifications are mostly functional and they do not deal with hardware-specific concepts such as mechanical or electrical systems. The card-specific requirements in terms of low-level communications, hardware and micro-electrical systems are found in norms such as the ISO7816 and in general in the ISO/IEC JTC 1/SC 17 working group set of norms, but usually *not* in the EMV.

EMV is also intimately linked with another norm, the “Global Platform", which describes the abstract secure management of applications in an environment.
EMV is often at an applicative level, describing the functional operation needed to perform bank transactions using the chip. This is usually described using APDUs (Application Protocol data Units) which are the way cards communicate with the outside world through communication protocols such as T=0 or T=1 for example.

EMV focuses on transactions between cards and terminals and between terminals and backend systems (EMV ‘hosts’) . Of course ATMs and EFT POS which process chips are covered by the norm.

Finally EMV designs bank cryptographic protocols (which are entirely original) to ensure the best resistance against cryptographic attacks.

The EMV ecosystem technologies are therefore made of embedded systems, micro-chips, tamper-proof secure microcontrollers and secure embedded platforms (JavaCard, Multos, Micro .NET etc..) EMV generates a lot of innovative research, such as trusted computing, trusted platforms, formal methods and formal proofs as well as highly advanced anti-intrusive electronics.

The fact that EMV is responsible to ensure the safety of around 842 million chip cards all over the world underlines how sharp and advanced the technologies behind it must be.

3 Can EMV be defeated?

There is a taboo in the small EMV world which consists of the denial about fraud involving EMV. Since EMV was created to push the responsibility of fraud from the card brands to the merchants and banks, it is assumed that “it is *not* possible to fraud an EMV card". In other terms, it is *impossible* to clone and hack a EMV certified chip-based bank card.

Nevertheless recently, some publications have demonstrated that such assessment should be taken relatively.

EMV cards were supposed to be unclonable until the differential power attacks (DPA,SPA. . .) appeared at the end of the 90’s. The principle was extremely simple: monitoring the power consumption of a smartcard to extract the cryptographic secrets stored inside its ultra-protected memory. Once these secrets were leaked, cards could be cloned!

Of course the EMV group imposed anti-DPA and anti-SPA measures from the providers but this demonstrated how relative were the bold statements of the EMV consortium.

As per 2020, cloning a EMV banking card is reputed to be totally infeasible and irrealistic. Nevertheless some flaws have been found in the meantime in the cryptographic protocols designed by EMV. Especially their initial card verification scheme, the SDA, the static data authentication system have found to be extremely vulnerable to several attacks and therefore was quickly replaced by the DDA, the Dynamic Data Authentication algorithm, which in turns was found to present some problems and was replaced by the CDA, the Common Data Authentication scheme.

There was never any publically known malevolent attack against bank cards using the flaws in SDA and all the problems were raised by skilled cryptographers from well-established universities or laboratories. Nevertheless some experts mentioned that there had been ‘probably’ several frauds involving the flaws from the SDA algorithm, but for ‘political’ reasons they were never acknowledged by the banks and by the EMV consortium.

As per 2020, the flaws of EMV stay a taboo and banks will usually simply refuse to speak about poorly implemented domestic EMV schemes (especially the recent US EMV migration, considered to be a fiasco . . .) . The world of EMV is a closed world and . . . “what happens in EMV, stays in EMV"

There are growing rumors about a so-called ‘Brazilian scheme’ or a ‘Brazilian method’ involving massive counterfeiting of EMV chip cards. The principle could consist in replacing ‘applets’ (e.g. embedded bank applications) by modified one (involving potential complicity in some card personalization centers) and modification of the PSE, the Payment System Environment.

Besides, with the rise of potential Quantum Computing and the deprecation of 3DES, several concerns have been raised about the fact that EMV is deeply dependent with RSA (which would supposingly be cracked ‘easily’ by quantum machines) and with 3DES which could be broken in the next years following cryptanalysis advances.

As a result EMV accelerated their migration to full AES (removing 3DES) and the elliptic curves cryptography.

So far nobody has ever proved that any criminal groups concretely managed to counterfeit EMV cards and so, as of 2020, they are considered to be unclonable and unhackable.

4 The politics of EMV

With almost a billion of EMV certified payment cards all around the world, EMV is a major financial actor, while being a normative body. The EMV norm is a powerful instrument of ‘politics’ for the major card brands inside EMV and they have created the system of the ‘EMV deadlines’ where bank from countries are being pressurized to provide, before a given date, a domestic EMV implementation, agreed by their respective national central banks. Failure to comply with such norms would result in EMV no longer willing to take the burden of the fraud for these non-compliant banks.

Such a ‘political strategy’ acts as a ‘EMV steamroller’ all over the world and can be a very strong instrument for financial power. In other terms, EMV may be perceived as a very strategic norm with a lot of economical and social implications.

The PCI council is another strategic norm for payment cards (ruling everything in payment cards which is not specifically chip-based such as networks etc. . .) and there is a clear rivalry between the two organizations.

Recently EMVCo started to extend their activities card-not-present transactions (which would become card-present throughout the web therefore) by issuing the 3Dsecure EMV specifications, allowing to pay goods online with a chip-based credit card (and using actively the chip during the online payment)

5 Conclusion

The Europay-Mastercard-Visa norm (EMV) is a badly known but very complex and powerful norm which rules over almost a billion payment cards worldwide. The technologies involved are very strong and innovative.

Here we only wanted to give a brief overview of EMV. We invite the reader to consult the EMVco website to have more information about the norms and the specifications, which are mostly open to the general public.