

The Joy of EMV

Testing times ahead in response to new US payments standard?

Andrew Mould
Managing Partner
Ascort, LLC

Andrew Mould is a Managing Partner at Ascort, LLC based in Sausalito, California. He has worked with NonStop for almost 30 years, starting in the government sector and then the financial industry. In 1992 he co-founded SoftSell Business Systems, which later became Ascort, to provide testing products for the NonStop platform.

There's a change coming to the US Payments industry which will affect all readers of this magazine in one way or another. For the general US public, EMV is the beginning of the end for magnetic stripe cards, and will change the way we make payment for goods and services. For the merchants, processors and banks that accept and handle these payments it means a change to their infrastructure and to their responsibilities in the case of fraud. For NonStop professionals who work with payments processing applications within these institutions it means yet more software

changes required in order to support the new standards within the transaction chain; and all this in a very short period of time - next April. Yes, April 2013!

So how does EMV change the way payments get made, and how disruptive will this be to us in the NonStop world?

A brief history

The EMV standard (and name) grew out of a 1994 European initiative by Europay, MasterCard and Visa to take advantage of the benefits offered by integrated circuit-based ("chip-based") payments technologies. The first specifications were published in 1996 and primarily detailed the interoperation between the chip-based cards (aka "smart cards") and the terminals where they could be used to purchase goods or withdraw cash. These cards offered higher security, and were increasingly used in place of magstripe cards.

Today the specifications are maintained by EMVCo, a joint operation between American Express, JCB, MasterCard and Visa. The adoption of EMV technology has been widespread and as of December 2011, in Western Europe, 84% of the payments cards issued were EMV cards and 94% of the terminals were EMV enabled. The technology has also been adopted for use in proprietary card schemes operated by non EMVCo members, such as Link in the UK, and Interac in Canada. As of last December, there were 1.5 billion EMV cards in existence worldwide representing a 45% adoption rate, excluding the US. The key words here are "excluding the US".

The US payments industry is late to this party, but with a vast number of terminals and around a billion general purpose cards in circulation there has been great resistance to following the rest of the world. But they're being forced into adoption of EMV in order to ensure the cards they issue are usable abroad, and to prevent

the fraud that EMV counteracts from relocating to the US. They also see an opportunity to use EMV to move the industry towards the "next big thing", namely Near Field Communication (NFC) and mobile-payments. As a result, in August 2011 Visa announced their EMV plans, and they were followed by announcements this year from MasterCard and Discover. For all of the card schemes, the target date for acquirers to be processing EMV transactions is April 2013. There are incentives in place to encourage US adoption, including reduced PCI reporting requirements, and a shift in liability to the merchant / acquirer for fraudulent card use when older non-EMV cards are used.

The nice thing about standards...

While Visa, MasterCard and Discover agree on the timescales, they disagree on some of the implementation details. In the UK the EMV rollout was dubbed "Chip and PIN" in reference to the fact that users were required to enter a secret PIN in order to locally authenticate and facilitate card authorization without an online connection. Chip and PIN is widely, though not exclusively, used in Western Europe over the alternative "Chip and Signature" where cardholders must sign something. In the US Visa is adopting Chip and Signature whereas MasterCard and Discover are aiming for Chip and PIN. The rationale for just using signature is that the use of online authorization in the US makes the additional complexity and expense of offline PIN unnecessary. Whether this leads to interoperability issues and confusion for the consumer remains to be seen.

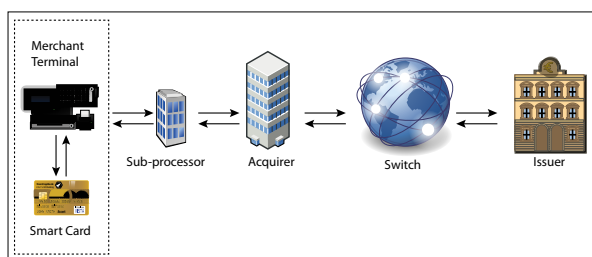
How does EMV change things?

Magnetic cards use static data making them a tempting target for fraudsters. The information on them can be obtained through a variety of mechanisms and the cards duplicated and re-used fraudulently. EMV prevents this type of attack by guaranteeing that every transaction is verifiably unique. Even if the transactional data was captured it could not be re-used in the same manner, and from a practical perspective it is hard if not impossible to clone a smart card.

The manner in which this security is achieved is by using cryptographic techniques together with local processing power on the smart card's chip. When a card is introduced to a terminal the card is powered up and the terminal will send requests to the card, in a classic client-server manner. The card and the terminal negotiate the processing of the transaction based on the value of the transaction and rules specified by the issuer (stored

on the card) and acquirer (stored in the terminal). The negotiation is based on risk tolerance and will determine how the cardholder should be verified (signature or PIN or maybe not at all), and how the transaction should be authorized (offline by the card, or online via the network).

If online authorization is required then the terminal will request that the card generate an Authorization Request Cryptogram (ARQC) by encrypting various data elements using a unique encryption key, known only to the card and its issuer, and a symmetric encryption algorithm. The EMV standards include algorithms that specify the data elements to use and the manner in which they are combined and encrypted, though issuers and card schemes may implement these differently. A key feature is that the data elements include an incrementing transaction counter maintained by the card, so guaranteeing the uniqueness of the cryptogram. The terminal will then embed the cryptogram as “additional data” in an otherwise regular payments message and send the message to the card processing network.



When the issuer receives the authorization request it will verify the authenticity of the transaction by validating the ARQC, and then generate a response back to the terminal. The response will itself contain an Authorization Response Cryptogram (ARPC), which the terminal passes back to the card to complete the loop.

Card issuers also have the ability to include “scripts” as part of their response data, using still different encryption schemes. These scripts can be used to update data on the card, such as the PIN, or the processing rules, or even completely disable the card.

Whereas this may all make card use more secure, it’s not hard to imagine that this comes with increased costs for the supporting infrastructure, including the cards, the terminals, the card management processes, the transaction processing, and most importantly from our biased perspective, the testing of all of the above.

Testing EMV

We’ve gone from using static data to having dynamic data maintained automatically by a miniature updatable card-based computer that exchanges messages with multiple parties, encrypted with multiple personalized keys and cryptographic algorithms. That’s a lot of change for one iteration, with many elements to be tested and certified, including:

1. **On-chip EMV kernel certification.** This is generally done by manufacturers, but some institutions create their own software stack for devices, or use 3rd party

kernels, which must be certified.

2. **On-chip issuer applications.** Smart cards can contain multiple applications, permitting “dual-use”. All applications require testing before deployment, verifying operations such as PIN management, script processing and key expiry.
3. **Terminal testing and certification.** Terminal vendors must verify that the terminal and card interoperate correctly and in a secure manner, and validate that messages sent from the acquiring terminal to the acquiring processor are correct in both content and format.
4. **Issuer provisioning applications.** The personalization overhead for each EMV card is much higher than for magstripe cards, and additional data elements must be stored in order to perform authentication.
5. **Acquirer & switch processing.** Acquirers must ensure they can receive and process transactions with EMV data by April 2013. Meeting this mandate means that the message formats between acquirers and switches must all support transmission of EMV data in both requests and responses.
6. **Merchant Certification.** Merchants and transaction acquirers will have to work together to ensure that merchant terminals are installed and interface correctly with acquiring processors. From October 2012 there are reduced PCI compliance reporting requirements for merchants who install EMV terminals.
7. **Issuer processing.** In addition to ensuring transactions containing EMV data can be received from the switch and authenticated, issuers must also make certain that they can generate and reply with valid ARPC values and downloadable scripts for the card applications. Performance testing of the servers must also be conducted to ascertain the impact of the additional cryptographic processing.

So EMV testing means different things to different people. Some testing, such as card interoperability and security testing, will be performed by laboratories sanctioned by EMVCo and some will be performed by the institutions along the payments path using tests designed by themselves and the card schemes. Similarly some of these areas have no impact on NonStop payments applications, and the impact of others will be dependent on the specific payments applications running on the NonStop and the business needs of your organization. For example, if as an issuer you don’t issue EMV cards, you won’t be impacted technically at all; your business might be though, as a result of the liability shift. As with any other change, modifications to add support for EMV require a full regression test.

It is along the transaction path in items #5 - #7 where NonStop systems tend to be most impacted, and more so along the edges than in the middle. This is because EMV is designed to provide end-to-end security, and therefore

the sole responsibility of the processors in the middle (the acquirer and switch in our diagram) is to accurately pass the EMV cryptograms along. Since they have no business requirement or capability to understand the content of this field, modifications to existing applications to achieve this should be simple. Associated changes in business logic to capture and process card type information for billing and fraud resolution will still require testing.

Testing at the edges becomes a lot more interesting. From a messaging perspective the acquiring sub-processor (the processor that handles the merchant) cares no more about the cryptograms than any other mid-way processor along the chain. However as the entry point to the payments network, they have a responsibility to certify the merchant before the merchant is given network access. Merchant certification is not a new activity, but EMV does add significant complexity due to the need to include the dynamic data – i.e. the product of the smart card to terminal interaction. Simple inspection / comparison of field data becomes impossible and sophisticated simulators must be used as responders to inspect and verify the data. This problem is compounded by the variety of card schemes, since the way they derive the cryptograms may vary.

A similar situation exists at the issuer, though rather than responding to incoming requests, as is the case with merchant certification, simulators must now generate test payment messages. Again it is no longer appropriate to simply provide lists of static card data. Instead, the messages from the switch must include data that simulates the card-terminal interaction in order to provide dynamic data for internal testing. The issuer does however have ultimate control of the application running on the card, and so knows exactly what algorithms to expect. An important factor here is that the anticipated increased longevity of smart cards over their magstripe ancestors may necessitate support for multiple versions of EMV standards.

So what's the good news?!

Being late to the party has its advantages, and with much of the world having already migrated to EMV, there is plenty of expertise and information to be found. With all the foreign vendors at the recent Cartes tradeshow in Las Vegas, it felt like a European invasion. If the tradeshow had been held at The Venetian or Paris casinos, the illusion would have been complete.

There is also plenty of expertise closer to home. Canada's migration is well underway, and in the Americas as a whole, outside the US, the EMV card adoption rate is 41% and EMV terminal adoption rate is 77% as of last December. Finally it should be noted that the overseas departments of your own company may have already gone through their own migration - we at Ascert have noticed an increased desire by organizations to re-use automated test scripts and VersaTest drivers from their overseas colleagues.

Where next... what about NFC and mobile?

It's impossible to ignore the buzz around mobile payments


– paying with our smart phones. There is a battle currently being waged for control of this “mobile wallet” with multiple participants offering differing schemes, such as PayPal's Mobile Wallet, Google Wallet and ISIS (a consortium founded by US wireless providers AT&T, T-Mobile and Verizon Wireless). And that is before Apple's rumored entry into the space!

Currently ISIS appears to have most industry backing, which probably should not be surprising given its founders' position and power in the mobile market. The ISIS solution uses “secure elements” inside each phone, which are the equivalent of the chips inside EMV cards. ISIS uses NFC technology to communicate with the merchant terminals, but it uses a card emulation mode to emulate an EMV device. This means from the NonStop perspective the heavy lifting will have been performed in this current rollout of EMV, and for the acquirers and switches additional changes to the NonStop to support this form of mobile payment should not be required.

ISIS is therefore embracing the current payments standards and technologies in place. How it also extends and adds new value to the payments ecosystem remains to be seen. A key difference from smart cards will be the number of applications that will run on the secure elements and how those applications interact. We can surely expect all the card brands to fight to get a place in the mobile wallet.

And finally...

EMV doesn't solve all the problems facing the payments industry, but it does help. Recent breaches at acquiring processors have resulted in details being leaked for millions of cards. EMV would not have prevented exposure of those card details, but it would reduce the number of places the information could be fraudulently used. Maybe one day its adoption might even eliminate those places – but not yet. Fraudulent activities will find the weakest link, and the need to stay ahead of it remains as one of the drivers for these changes in the US.

Change is good – it's how we evolve. And where there's change, there's opportunity. For the merchants and banks, smart cards and smart phones can run several applications enabling multi-purpose cards and marketing / affinity tie-ins. For card users fraud is reduced, card convenience is improved, and they get to realize tangible benefits from the new relationships the new technology facilitates. For IT professionals, it's a time to evaluate and update systems and practices. And all of this requires testing – oh what a joy! 

Ascertainment was founded in 1992 as a supplier of advanced testing software and services for the NonStop platform. Ascertainment's native and off-platform solutions allow a wide-range of testing activities for the NonStop from functional through performance testing, managed directly or via HP Quality Center as part of an enterprise testing environment. Solutions built on Ascertainment's VersaTest technology are used for testing payments systems throughout the world, with the first EMV project being undertaken in 1998 for a UK bank. Ascertainment is an HP Partner and member of HP Software's Enterprise Management Alliance Program (EMAP)