Secure Remote Payment Council (SRPc)

White Paper Discussion: EMV Enhancements Post Implementation

September 13, 2016

Objective

This white paper is the fifth in the series developed by the Secure Remote Payment Council (SRPc). In this discussion, SRPc provides an EMV post mortem on the implementation addressing some of the problems that have arisen in the industry since the U.S. implementation of EMV chip cards, and the SRPC's response to remedy those problems and keep EMV implementation on track.

The Problem

Full-scale, United States implementation of EMV at the POS has effectively been underway since October 2015 but not without incident. The results have been both predictable and problematic. Many believe implementation has been executed in a locked decision making environment. The policy making organization was narrow and closed, with limited input from a broad range of stakeholders.

Latest statistics show that only 37 percent of all of U.S. merchants have implemented EMV[1] and thus avoided the liability shift to them. From the onset, when the dates were set for the liability shift, merchants and debit networks voiced their concerns about the short time frame to execute. Furthermore, the global card brands announced the dates for the liability shift without setting any dates for network compliance with Durbin routing.

One of the major benefits of EMV chip is that the chip protects against the creation and use of counterfeit cards. Yet the U.S. implementation of EMV opted for chip and signature rather than chip and PIN, which would also protect against lost and stolen cards, strengthen security and better deter fraud. For many years, debit cardholders have shown a preference for PIN-based transactions stating that PIN debit transactions are safer and more secure than signature debit. Some industry stakeholders have contended that the global card brands have de-emphasized PIN's advantages over signature largely due to their vast economic interest in support of signature.

EMV Standards

EMVCo creates and manages the standards for the interoperability and acceptance of secure payment transactions using the EMV chip. The governance for EMVCo lies primarily in the hands for the largest card brands in the U.S. market. These standards stifle competition and innovation, particularly in areas relating to enhanced payment transaction security. Furthermore, they create a disadvantage for the other debit networks, merchants and consumers alike, who have no control, input or authority over the decisions being made.

Many industry stakeholders believe that issues with EMV could have been avoided if a larger governing body had been in place. As requested numerous times in the past three years, the SRPc calls upon the industry to demand that EMV standards be governed by a truly open, consensus group that will lessen the likelihood that the standards can be used as a competitive weapon.

Several problems have surfaced in the implementation of EMV chip. It is not as fast, not as secure and the environment in which it operates looks different from implementations in the rest of the world. This white paper explores some of the major obstacles to the smooth implementation of EMV in the U.S.

[1] Source: The Strawhecker Group.

Delays in the Certification Process

Unforeseen delays in the terminal certification process queues and subsequent changes to the EMV specifications have impeded the rollout at many merchant locations.

While merchants have invested in EMV-capable payment terminals, lengthy delays in getting hardware and software tested and certified by appropriate organizations has stalled many companies from fully rolling out EMV. Depending upon the environment, the certification process may take upwards of one year to complete. Developers must test and certify that EMV rollout is meeting requisite security standards, but the queues to get certified are very long, as is the process to complete certification.

Card brands set the standard for certification in accordance with EMVCo standards. Separate certification is required for each of the major global card brands - MasterCard, Visa, Discover and American Express. Certification is required for each acquirer processor that connects to that card brand. Further certification is required for each unique terminal, merchant application and middleware, both up and downstream between the acquirer processors and networks. The combination of each of these elements creates a mind-boggling number of certification cases to be tested. Industry-wide, there were insufficient resources available to support the magnitude of certification that was required to be EMV compliant.

Very recently, the global brands announced modifications to the certification requirements that allowed organizations to certify to one acquirer processor and apply that certification to all other acquirer processors. These changes in the certification process are designed to streamline the process. Improvements to the certification process also include the use of better test scripts and recommendations on industry best practices before going live.

Existence of Multiple U.S. Common Application Identifiers (AIDs)

In the U.S. there are a number of debit networks in addition to the debit networks supported by the global card brands. This is unique in comparison to other markets in the world. Additionally, the merchant-centric debit routing rules required by Regulation II in the Durbin amendment created the need for a different processing environment in the U.S. After much debate, the industry settled on the use of Common Debit AIDs licensed bi-laterally by the global brands to U.S. debit networks.

Many of the delays in the certification process for debit stem from the lack of availability of the specifications supporting the U.S. Common Debit AID, which were not released until mid-2015. While the Global AID was available in advance, many merchants waited for the U.S. Common AID to be released so to mitigate the need to recertify. Resultantly many merchants did not meet the October 2015 timeframe for the liability shift. Others chose to implement credit only or debit with Global AID routing only, thereby limiting other debit networks from seeing certain transactions.

Offline Support Requirements

EMV implementation started 25 years ago in response to the non-zero floor limits set in Europe. The lack of online infrastructure in these geographies required the card to authenticate itself to the terminal and be able to verify the PIN without accessing a host computer.

Today, most of the complexity with the implementation of EMV stems from the requirement to certify the offline process. The difficulty is further exacerbated by the inconsistencies in the implementation experienced in other parts of the world.

As online processing becomes more prevalent, the payments industry is moving away from support for offline processing. In fact, Europe has moved to an online processing environment and the U.S. has never supported offline usage. Furthermore, few EMV cards issued in the U.S. have offline capability and all payment terminals are set to a zero floor limit, which means they go online for every transaction.

The global brands knew there would be no need for offline support in the U.S. but EMVCo standards are forcing merchants to certify their terminals and systems if the terminals are capable of supporting offline usage, despite the fact that feature will never be used.

These offline processing requirements in the U.S. are dead on arrival, and have caused unnecessary delays in the certification process. This is just another example of the EMVCo standards body making technical decisions for the economic benefit and in the interest of its own constituency.

Long Transaction Wait Time

The customer experience using the new technology has also had its challenges. Consumers have an expectation that payment technology will be easy to use, convenient and secure. Yet the option of "swipe, tap, insert or wave" causes confusion, particularly when the terminals have not been configured to support all of the new payment form options.

Both consumers and merchants are annoyed by the delays in the checkout process using EMV chip cards. To process an EMV chip transaction, the chip card needs to remain in the POS terminal for the transaction to complete the cryptographic processes required to authorize the transaction.

In April 2016 Visa and MasterCard announced amendments to their EMV chip implementations to address issues relating to throughput speed at the checkout. Visa Quick Chip and MasterCard M/Chip Fast have been introduced as "upgrades" that streamline EMV chip transaction processing. Customers will be able to dip their card and remove it from the POS (in two seconds or less), without waiting for the transaction to be finalized. This process will stop scripting from occurring at those POS devices that will support Quick Chip and M/Chip Fast.

No additional testing is required if the merchant is already certified. The enhancement requires a software modification to the merchant POS terminal. Visa is recommending that merchants across the board use Quick Chip to enable faster, less cumbersome processing. In general the change should be an improvement in consumer perceptions, but that implementation of Quick Chip will create an inconsistency customer experience in the way other cards work at the checkout. The key question is why was this problem not anticipated beforehand? There have been many other EMV implementations over the past 25 years. It's hard to believe this was the first to encounter such a problem.

Confusing POS Screens

The members of the EMV Migration Forum have gone through much effort the past three years to resolve and document the unique implementation aspects of debit EMV for the U.S. Many of the terminal hardware and software providers actually participated in crafting solutions - at least on paper. It thus seems all the more amazing that merchant POS terminals have been rolled out prompting consumers to "choose" a debit route when using a chip card, rather than giving merchants routing control.

The choices for transaction routing presented to the consumer at the POS depend upon what the card issuer has labeled and prioritized on the card for debit and credit - either through the debit networks or the global brands. Issuers are required by the global brand to prioritize their brands. That means when choosing the Visa Debit or MasterCard Debit AID, the transaction must be routed to the global debit network. This eliminates merchant choice and is particularly bad for the other debit networks. Furthermore, the language that is being used at the prompt screen is confusing, namely the consumer is given a choice of Visa Debit or U.S. Debit, the latter being presented as the option to select for cash back. For MasterCard, the options being presented are MasterCard Debit or U.S. Debit. This added screen prompt not only confuses consumers but runs the real likelihood that consumers will default to the first selection since they have no context for selecting "U.S. Debit."

As more and more merchants discover this implementation they are appalled and are demanding that their vendors provide a better implementation - one that preserves the merchant's Regulation II debit

routing rights. Merchants must be able to make changes at the POS terminal to relabel the routing options presented on the card, so that the merchant controls of routing options for those transactions in accordance with Regulation II in the Durbin amendment. However, depending on how their terminals were configured for EMV, merchants that opt to remove or suppress confusing screens may trigger a lengthy and expensive re-certification process.

Unfortunately, the damage is done as non-global network volumes are impacted, merchant costs are increased and the real pain of yet another terminal change is implemented.

EMV Changes

Almost three years ago when the uniqueness of the U.S. debit market was evident, numerous solutions were put forth. One of these solutions was to ask the global brands to allow EMV transactions to be processed in a gateway fashion just as magnetic stripe already were. The global brands declined this solution. Another was to ask the global brands to join the U.S. debit networks in a consortium to own and govern AIDs multilaterally with issuer and merchant involvement. Again, the global brands declined. In both cases, the global brands indicated that world-wide interoperability of EMV would be adversely affected and that the changes would take too long to implement. Yet, the past few weeks we have seen swift movements by the global brands on topics such as "Faster EMV" and fewer certification tests. It seems that the previous arguments about length of implementation don't really apply when the global brands feel the need for speed.

SRPc's Point of View

The SRPc proffers the position statements on the EMV post mortem:

- Make U.S. EMV governance an open, consensus one.
- Support merchant choice for debit transaction routing.
- Support the full capability and security of EMV chip in the form of a PIN.
- Consider how EMV chip technology and development could be leveraged to deter the shift of fraud to the card-not-present (CNP) world.

If the global brands are going to make changes / additional investment to the EMV chip, why not make the process safer as well as faster? The SRPc recommends using the computational and cryptographic powers of the chip to protect the PAN on the card and tokenize the PAN by means of encryption. By putting the PAN in the cryptogram, effectively replacing the PAN with a dynamic token, the PAN is protected at the source, (i.e., the card). The PAN would be decrypted to verify the cryptogram but only the issuer would see it. In addition, putting different data in fields (or suppressing fields with sensitive data) protects the PAN from exposure over communication networks.

Call-to-Action

The problem of protecting the PAN was not solved with the original implementation of EMV in the U.S. As long as the card brands are going to make changes to the chip to enable a faster transaction and improve the EMV experience, they might as well add safety improvements too. These safety improvements include using the computing power of the chip to protect the PAN on the card and supporting the use of a PIN with every transaction.

Let's use this as an opportunity to ameliorate some security problems with EMV implementation:

- Take the PAN off the card for security reasons, e.g., to protect against counterfeiting.
- Add a PIN to the EMV transaction thereby making the whole transaction safer.
- Proactively find ways to contain CNP fraud losses borne by merchants e.g., by using user authentication techniques to protect the cardholder, not just the card.
- Allow all payment card networks including U.S. debit networks to become token service providers.

About the Secure Remote Payment Council

The Secure Remote Payment (SRPc) is a nonprofit, inter-industry trade association that supports the growth, development and market adoption of debit based internet eCommerce and mobile channel payment methods that meet or exceed the security standards for pinned based card present payments. It will accomplish this by encouraging and supporting those activities that accelerate the implementation, adoption and promotion of these payments. The SRPc's members include merchants, financial institutions, merchant processors, issuer processors, payment brand companies, payments authentication hardware providers, payments authentication software providers and payments consultants. This document does not necessarily express the views and opinions of every member of the SRPc. For additional information, visit http://www.secureremotepaymentcounci.camp8.org/ .