February, 2012

Thoughts on EMV

In keeping with its mission as "a cross-industry trade association[1]", the Secure Remote Payment Council (SRPc) endeavors to promote interoperability. Open standards, best practices, and broad involvement from every sector of the payment ecosystem are critical to an improved security environment all participants can enjoy. Payment schemes that rely heavily on proprietary knowledge, monolithic architectures, or centrally-mandated methods and standards are anathema to the SRPc's mission.

As the council prepares to facilitate a pilot of eCommerce and mobile technologies "that meet or exceed the security standards for pinned-based, card-present payments[2]" it is exposed to many technology approaches that attempt to achieve this goal. It has been the council's desire to be impartial as it constructs a platform by which each approach may be understood and evaluated by a wide range of constituencies, endeavoring to limit its role to "a venue for the introduction of new eCommerce payment initiation solutions and a standardized process for their validation[3]."

There are, however, alternatives to this approach. It is the belief of some that the application of security technologies *should* be centrally mandated and controlled. This to insure the benefits of such technologies can be consistently applied and relied upon in an environment which, most would agree, is only as secure as its weakest link.

An example of a security technology that follows this model is EMV. While EMV has become a significant part of the payments landscape in many regions, it remains nascent in the US. It is the desire of the SRPc in this letter to contrast EMV, a proprietary standard governed by a small number of global payment brands, to the council's own activities and mission. The council does this to emphasize the risks inherent in EMV's monolithic scheme and to offer an alternative philosophy that, for payments that do not occur in a face-to-face environment, is more inclusive and less proprietary, and therefore more robust, less risky, and more likely to be universally adopted.

While there are many aspects of EMV that benefit from close analysis, including the cost of industry adoption whose estimates range from $8.6 to $13.4 billion[4], one issue exemplifies the contrast of EMV's approach to that of the SRPc. This is the likely effect of the EMV architecture in the US payments environment, one that contains many constituencies. In short, EMV places significant emphasis on the actions of the chip, to the point that much of the behavior and effect of a payment transaction is

[1] "SRPc Mission Statement", *Secure Remote Payment Council*, December 20,2011, <http://secureremotepaymentcounci.camp8.org/Default.aspx?pageId=661217>
[2] *Ibid*
[3] "SRPc Key Activities", *Ibid*
[4] Contini, Darin, *et al*, "Mobile Payments in the United States: Mapping Out the Road Ahead", *Federal Reserve Bank of Boston,* March 25, 2011, <http://www.bostonfed.org/bankinfo/firo/publications/bankingpaypers/2011/mobile-payments-mapping.pdf>

controlled by it[5]. The involvement of the traditional downstream elements of the payment chain is deemphasized. Therefore, the interplay of payment brands, processors of transactions, and providers of infrastructure in a competitive environment are likely to be significantly altered in an EMV-dominated scenario.

To see this, we must consider some of the components of the EMV architecture. For a complete description of the EMV standard, please refer to <emvco.com>. EMV is "a global standard for credit and debit payment cards based on chip card technology[6]." Such technology employs an "embedded microprocessor" that "contains the information needed to use the card for payment, and is protected by various security features.[7]" The microprocessor runs software (termed an "application") resident in non-volatile memory on the chip that dictates how a payment is to be acquired and processed in conjunction with an EMV terminal and downstream payments processing. The application is, therefore, the expression of the acceptance policies and rules of its publisher[8], an issuer, though in practice this is a payment brand by proxy. These policies and rules, compared to the current US payment acceptance environment, are not normative. They may include terminal actions, data formats, and consumer actions unique to the issuer and payment brand. Such anomalies may significantly limit how the subsequent transaction is processed.

This is in sharp contrast to the current acceptance technology in the US: magnetic stripe cards. Acceptance of these cards is ubiquitous and common. The technology employed has little regard for the strategic intent or competitive strength of individual members of the payment chain, whether they be merchants, payment brands, issuers or infrastructure providers. Many payment brands can "ride" on a single card, their acceptance being placed on even footing with their competitors by the broad adoption of standards, such as ISO 7811 and 7812, across an ecosystem that currently includes nearly all payment card production and encoding.

While EMV, as it is currently defined, could be implemented to achieve this goal there are several factors that work against this ideal in practice. For instance, it is possible for an EMV chip to have more than one application resident in its memory. Therefore, more than one payment brand could be present on the same card. However, the terminal must select an application before processing, as the application controls the terminal's behavior once the transaction is commenced. Therefore, the terminal must be aware of the applications that it could discover on any chip card presented to it, and then employ a method of choosing the appropriate application[9]. This implies an application management process that requires a universal directory of applications, their publishers, and their intended uses in order to maintain interoperability, especially from the cardholder's perspective. Publishers, terminals,

[5] "A Guide to EMV, version 1.0", *EMVCo, LLC*, May, 2011, http://www.emvco.com/best_practices.aspx?id=217, p. 17
[6] "About EMV", *EMVCo, LLC,* December 20, 2011, <http://www.emvco.com>
[7] *Ibid*
[8] "A Guide to EMV, version 1.0", *EMVCo, LLC*, May, 2011, http://www.emvco.com/best_practices.aspx?id=217, p. 17
[9] *Ibid*, p. 18

and issuers would need to be continuously synchronized to this directory. This application management process could prove to be complex to manage.

As an alternative, a payment brand may negotiate with another brand who already publishes an application to have its brand included as an option. For instance, a debit brand network (i.e. Shazam, STAR or ACCEL/Exchange) could contract to be included in the application published by another brand (i.e. VISA or MasterCard). However, the included brand would be subject to the publisher's requirements and limitations, and may even have to pay royalties to it. It is unlikely the publisher would allow the included brand to compete with it in a meaningful way. Of additional and critical concern, is that the "included brand" would be extremely limited in their ability to innovate, creating an ecosystem that could eventually affect competition.

It has been suggested that a payment brand could still leverage the application of another brand by using the routable payment data embedded in its application. In most deployments of EMV operating today, traditional ISO 7812 data is still used to identify and route to issuing banks and accounts. If such data is available, unencrypted, to the merchant or acquirer processor, it would then be possible to route the transaction via another brand than the one that published the application. However, The SRPc believes some payment brands may prohibit this behavior for strategic reasons.

The emphasis of EMV on the chip and its multiple applications also impacts the issuer. The applications discussed above, as a practical matter, must be loaded onto the chip during the issuing process. For the majority of low cost chip cards, the load process "fuses" the application in place. Once fused, it cannot be altered. Therefore, EMV requires issuers (and by complement, merchants) to make decisions regarding which payment brands will be placed on cards or terminals in advance of issuing. Such decisions cannot be reversed or modified once issuing has occurred.

The risk of this "lock-in" can be seen in a recent operational problem with EMV cards in Germany. Dubbed the "Y2010" problem, some 26 million EMV cards were rendered inoperable after the turn of the year 2010[10]. The error was partially attributed to the chip[11]. The chip manufacturer posted a EUR10 million reserve against its 2009 earnings in anticipation of claims of loss[12]. This scenario demonstrates the risk of pre-determined functionality that is difficult to remediate in the field.

Securing payments is a laudable goal, one the SRPc is dedicated to advancing in the realm of payments that are not made face-to-face. However, we are also dedicated to the adoption of methods and technologies that are inclusive, flexible, standardized and open. While EMV incorporates many state-of-the-art security techniques, its architecture and promotion do not necessarily advance these principals in a broadly participatory manner. *We call on the industry to carefully review the ramifications of EMV, understand its inherent risks and come together to ensure EMV is open to all market participants in an equitable manner.*

[10] Kroger, Michael; Seith, Anne. "Klebefilm-Trick hebelt 2010-Fehler aus", *Spiegel Online*, January 6, 2010
[11] *Ibid*
[12] "Gemalto books EUR10 million provision against German date-change fiasco", *Finextra,* January 13, 2010