Finding the Best Route for EMV in the US

1/23/2013

Exploring EMV Implementation Strategies that Preserve Network Routing Options and Satisfy Government Regulations

ABSTRACT

Recently the Debit Working Committee of the EMV Migration Forum (EMF) has suggested developing a new US Debit ICC (Integrated Chip Card) Application for all chip cards issued in the US. The purpose of the new application is to allow the US debit networks and merchants to comply with regulatory requirements while supporting multiple routing options for all debit transactions.

This paper presents three ICC Application strategies that would use BIN/card prefixes, interchange agreements or fees, or other methods to determine the routing path for all online debit transaction requests (including EMV), as is the case in other countries in which EMV is currently supported. These alternatives may eliminate the need for a new Debit ICC Application, saving US EMV stakeholders time and money as we work together to achieve the business objectives outlined by the Debit Working Committee of the EMF.

This paper also describes challenges related to transaction routing and EMV data validation that must be addressed, regardless of the ICC Application strategy that is selected.

Contents

Finding the Best Route for EMV in the US

Exploring EMV Implementation Strategies that Preserve Network Routing Options and Satisfy Government Regulations

EXECUTIVE SUMMARY

One of the many EMV migration concerns expressed by US merchants and acquirers is how EMV transaction routing will be determined.

The Debit Working Committee of the EMV Migration Forum (EMF) identified the business objectives of EMV migration for US stakeholders. A primary requirement was that merchants, merchant acquirers, and processors "must be able to make routing choices as prescribed by Durbin" (which requires that a debit acquirer must have a choice of two ways to route a transaction to the Issuer). To achieve this and other business objectives, the committee suggested developing a single US Debit ICC (Integrated Chip Card) Application for all EMV cards issued in the US.

> Multiple US networks. Regulatory requirements from EMVCo and the US government.
>
> How do we guarantee interoperability while preserving the ability to route transactions according to the business interests of all EMV stakeholders?

Typically, ICC Applications are not used for EMV transaction routing; instead, routing is determined by the BIN/card prefix, interchange agreements or fees, or other methods. In addition, there are other issues related to transaction routing that a new ICC Application will not resolve.

And developing a new ICC Application, or modifying an existing ICC application or profile, would require considerable time and expense.

Fortunately, there are several ways in which the business goals established by the committee may be achieved. This paper presents three ICC Application strategies that will serve the business needs of EMV stakeholders in the US and, when combined with the best practices suggested, will ensure global interoperability, comply with EMVCo and payment association specifications, comply with various US regulations (including Durbin), and still allow the routing flexibility required by acquirers and processors.

Option 1: Each US Issuer uses one or more existing ICC Applications of its choice, or

Option 2: US EMV stakeholders use an existing (common) Debit ICC Application, or

Option 3: A new US-Specific Debit ICC Application is available to all US EMV stakeholders

On January 18, 2012, MasterCard announced that it will allow US debit networks to license their Maestro ICC Application. As a result, all US networks and Issuers can select Option 1 or Option 2, and the need for a new US Debit ICC Application (Option 3) could potentially be eliminated.

Regardless of the ICC Application strategy that is selected, each Issuer must be able to validate the EMV data in online transaction requests. Because the Application Identifier (AID) — which indicates the ICC Application that was selected by the chip card and the terminal for tasks such as risk management and cardholder verification — is not carried in most online transaction request messages, it can be a challenge for the Issuer's authorization system to know what key and algorithm to use to validate the EMV data. This paper presents two EMV data authentication strategies that Issuers can follow to make the EMV data validation process more efficient.

- Each US Issuer uses **unique values** to identify each ICC Application on a card, or
- Each US Issuer uses **common values** to identify each ICC Application on a card.

Finally, this paper suggests best practices that may streamline EMV migration in the US while meeting stakeholder objectives.

Who Are US EMV Stakeholders?

Stakeholders include, but are not limited to:

- The US debit networks
- Terminal vendors
- Merchants and acquirers
- Chip card providers
- Issuers
- Processors
- Payment associations

What is the EMV Migration Forum (EMF)?

Many US stakeholders felt that there was a need for a central entity to coordinate and promote EMV migration in the US. This task has fallen to the Smart Card Alliance, which has set up an independent, cross-industry organization called the EMV Migration Forum (EMF). The EMF, founded in mid-2012, has a membership of over 100 organizations. Several internal EMF committees were formed to address immediate migration issues that are unique to the US market.

CONCERNS RELATED TO EMV TRANSACTION ROUTING

Visa, MasterCard, Discover and American Express have announced roadmaps for EMV migration in the US. One concern related to US EMV migration is the ICC (Integrated Chip Card) Application Selection process, mandated by EMVCo. Specifically, US stakeholders are concerned that the resulting ICC application selected by the terminal would conflict with the Durbin amendment requirement that acquirers must be able to route transactions via at least two debit networks.

In most countries, there is only one national debit network and all domestic debit transactions are routed through that network. In the US, however, there are many debit networks and many existing transaction routing agreements. The business model for these networks centers on high transaction volumes. Similarly, financial institutions prefer to route transactions using processors with which they have negotiated the most favorable rates.

How can flexibility in transaction routing be preserved for merchants and acquirers?

Because the existing ICC Applications, already certified by EMVCo, are provided primarily by payment associations, there is a common misconception that transactions using those ICC Applications must be routed to networks affiliated with the application-owning payment network.

This is not the case. For example, even if the card and the terminal use a MasterCard ICC Application to determine cardholder verification methods, etc.; this does not mean that this ICC Application (or its identifier) must be used for routing, nor does it mean that the transaction must be sent to MasterCard or a MasterCard-affiliated network. Instead, the routing path for an online debit transaction request (including EMV requests) is determined based on BIN/card prefix, interchange agreements or fees, or other methods. All networks must pass EMV data, in its original form, to the Issuer or OBO (on-behalf-of) party, regardless of the transaction path that is selected. Although each message format may carry the EMV data in different fields, or present the fields in a different order, all network specifications must adhere to EMVCo standards regarding the minimum data fields that must be included in the transaction request message.

EMF Committee's Business Objectives for US Stakeholders

- Each US merchant, merchant acquirer or processor must be able to make routing choices as prescribed by Durbin, while utilizing BIN table routing or other routing criteria that is already in place today for magnetic stripe cards
- Transaction routing is not to be determined by the consumer at the terminal
- There must be no impact to current Service Level Agreements (SLAs), e.g. time spent in checkout lanes must not increase
- Foreign cardholders must be able to successfully perform transactions using their chip cards at US ATMs and POS devices
- Each US Issuer must be able to change network affiliations without reissuing cards
- Each Issuer will be able to implement EMV processing within its host system's authorization logic
- Cardholder Verification Methods supported by US-issued chip cards must be appropriate to the terminal at which the transaction is performed
- In addition, the chosen solution must:
    - Comply with existing EMVCo specifications
    - Work for both ATM and POS
    - Support offline PIN at POS terminals

In the following sections, we will review three ICC Application strategies that will meet the business objectives set forth by the EMF committee, the benefits and challenges of each strategy, and issues that must be addressed regardless of the strategy that is selected.

US STAKEHOLDER DECISIONS REGARDING ICC APPLICATIONS AND DATA AUTHENTICATION

Stakeholders must select one of the ICC Application strategies (Option 1, Option 2, or Option 3) described in the following section. In addition, all US chip card Issuers that will be verifying and generating EMV cryptograms should select one of the two EMV data authentication strategies presented.

ICC Application Strategy Alternatives for US EMV Stakeholders

Option 1: Each US Issuer uses existing ICC Applications of its choice

Option 2: US Stakeholders agree to use an existing (common) ICC Application

Option 3: A new US-Specific Debit ICC Application is implemented

When any of the three options are selected, the following are true:

- Application Selection between the chip card and the chip-enabled terminal would be performed as per EMVCo specifications.
- Transactions would be routed using current routing logic (BIN, interchange rules, etc); however, to ensure that the EMV data in the transaction reaches the Issuer or OBO (on-behalf-of) party, and to avoid potential liability, acquirers must route EMV transactions only to networks that are EMV-compliant.
- The Issuer, or the OBO party, would be responsible for verifying EMV data. This can be done by modifying its authorization software, or adding new software that can perform this function.

Option 1: Each US Issuer Uses One or More Existing ICC Applications of its Choice

With this option, the stakeholders do not need to agree to support a specific ICC Application. Each Issuer would select one or more existing ICC applications for its cards. Each application and profile would meet the Issuer's specific needs for authentication, cardholder verification, risk management, etc. If the Issuer is a debit network that is not affiliated with a payment association today, the Issuer can license an existing ICC debit application from a payment association. In some cases, the card may not need to be branded for that payment association. There are also "white label" ICC applications available in the market that meet an Issuer's business objectives.

This option utilizes EMV the same way it is used in many countries throughout the world. US-issued chip cards will contain proven, globally-supported ICC application(s) that best meet the Issuer's business requirements. These US-issued chip cards can therefore be used at any chip-enabled terminal in the world; ensuring true interoperability. US terminals will support applications that are certified by the payment associations with which the acquirer is affiliated today, and that are relevant to the individual terminal's function, i.e. ATM or POS.

Benefits

Primary benefits of selecting Option 1 or Option 2:

- Eliminates the time and expense associated with the development, deployment, and maintenance of a new US Debit ICC Application.
- Eliminates the requirement for terminals and terminal vendors to support a new US Debit ICC Application.

CHALLENGES

This solution does not eliminate the situation in which the Issuer, or the OBO party, may not be able to determine which application was selected by the chip card and the terminal, and therefore does not know what algorithm to use to verify the EMV cryptogram in the transaction request. The Issuer or OBO party may need to send multiple requests to their hardware security module (HSM), one for each application the card supports. This would likely require modification to the Issuer's software, and could have a performance impact.

If a "white label" application is used, the Issuer may need to modify the application or a profile to suit its particular requirements. Terminal vendors would need to ensure that their software kernels support this application.

This option does not completely address the issue of key management. Multiple parties may require keys to verify and generate EMV data. The more parties that share a key, the less secure that key becomes.

Option 2: All US Stakeholders Agree to Use an Existing (Common) ICC Application

With this option, the US stakeholders would agree to include a specific existing ICC application in their chip cards and chip-enabled terminals, for example, MasterCard's Maestro ICC application. The selected application, which this paper will refer to as the "Common US Debit ICC Application", would be used instead of developing a new US Debit ICC Application.

The payment associations have already developed profiles for their global ICC Applications that conform to current US business practices. If the Issuer is a debit network that is not affiliated with a payment association today, the Issuer can license an existing ICC debit application and US-specific profile from a payment association. In some cases, the card may not need to be branded for that payment association. There are also "white label" ICC applications available in the market that may meet the stakeholders' business objectives.

The Common US Debit ICC Application must have priority within each US-issued card that contains the application, and within each US EMV-enabled terminal. Issuers would configure their chip cards so that the Common US Debit ICC Application could be automatically selected by the terminal when the card and the terminal both support this application, and the cardholder would not be prompted to select or confirm the application. Acquirers would configure their terminals so that the Common US Debit ICC Application has priority over other debit applications supported by the terminal.

When the Issuer or OBO party receives a transaction request, they would assume that if the transaction was initiated by their US-issued chip card at a US chip-enabled terminal, then the Common US Debit Application was used. The Issuer or OBO party would attempt to verify the EMV data using the algorithm associated with the Common US Debit ICC Application. The application designated as the Common US Debit ICC Application will very likely be one that Issuers were already planning to put on their chip cards.

CHALLENGES

If the transaction is initiated by a US chip card at a US chip-enabled terminal, the Issuer or OBO party would assume that the Common US Debit ICC Application was selected, and would then attempt to verify the EMV data according to the algorithm supported by that application. If the EMV data cannot be verified using this algorithm, the Issuer/OBO could either decline the transaction, or continue attempting to verify the EMV data using algorithms associated with any other applications on the card. Stakeholders may need to agree on the proper course of action for this scenario.

Multiple card profiles may be needed to support different parameters and values required by US Issuers.

It may be difficult for all stakeholders to agree on a single ICC Application to use as the Common US ICC Debit Application.

This option does not completely address the issue of key management. Multiple parties may require the keys to verify and generate EMV data. The more parties that share a key, the less secure that key becomes.

Option 3: A US-Specific Debit ICC Application is Implemented

This is the approach currently being pursued by the Debit Working Committee of the EMF. This option would be needed only if a debit network that currently issues magnetic stripe cards is not allowed to license an existing ICC Application from a payment association with which the debit network has no affiliation today. However, since MasterCard (and perhaps other payment associations) will permit this, there is no benefit to this option, but there are many challenges.

CHALLENGES

Developing a new US-Specific Debit ICC Application is a complex, time-consuming, and expensive project, with many steps that will add to the expense – and slow the progress – of the US EMV migration. These steps include, but are not limited to:

- Development, approval, distribution and maintenance of a technical specification
- Development, certification and maintenance of the ICC Application and associated profiles
- Certification by payment associations and stakeholders, and development of a certification test plan (and possibly selecting a certification test lab)
- Request for a unique Application ID (AID) assigned by ISO
- Adoption (and related changes) by any entity that is updating software kernels for US terminals or providing chip cards to US Issuers, thus affecting terminal vendors, merchants and acquirers, card providers, Issuers, debit networks, processors, payment associations, software providers, and others.

It would likely take a year or more before the new US Debit ICC Application would be available to the stakeholders, and, once developed, the application would require ongoing enhancement and maintenance throughout its lifespan. EMV stakeholders must bear in mind the possible delays and the added expense of developing the application.

Developing a new US-Specific Debit ICC Application is a complex, time-consuming, and expensive project which requires:

- Project management
- Application development (and possible changes to chip production)
- Certification by payment associations and stakeholders, and development of a certification test plan (and possibly a certification test lab)
- Request for a unique Application ID assigned by ISO
- Adoption (and related changes) by any entity that is updating software kernels for US terminals or providing chip cards to US Issuers, thus affecting terminal vendors, merchants and acquirers, card providers, Issuers, debit networks, processors, payment associations, software providers, and others.

This process can be streamlined to some degree by using an existing ICC application and an existing profile, and making only minor modifications to that profile to fit the business needs of the stakeholders. However, depending on who currently owns the source application, networks that are not affiliated with that entity may have challenges obtaining permission to use it.

Documentation and maintenance of the modifications will still be required, and formal certifications will be necessary, although the certification process can be streamlined if an existing profile is used. Multiple profiles may be needed to satisfy the requirements of all US stakeholders.

This option does not completely address the issue of key management. Multiple parties may require the keys to verify and generate EMV data. The more parties that share a key, the less secure that key becomes.

Fundamental Authentication Principles

Both of the authentication strategies include the following common characteristics.

- Issuers select one or more ICC Applications which meet the Issuer's specific needs
- Application selection (between the terminal and chip card) is based on EMVCo specs
- Issuers/OBOs are responsible for verification and generation of EMV data
- Routing occurs based on current BIN/interchange routing logic, but acquirers must route EMV transactions to an EMV-compliant party

Issuer EMV Data Authentication Strategy Options

After the stakeholders agree on one of the ICC Application policies discussed previously, US Issuers that are verifying or generating EMV data must select one of the following EMV data authentication strategies. A strategy is needed because the Application ID is not carried in most online transaction request messages; therefore, it's not immediately obvious which ICC Application was used when generating the EMV cryptogram in the message. Ideally, one of these options would be universally accepted by all Issuers, but unfortunately that is unlikely.

With either authentication strategy, each Issuer would select one or more existing ICC applications for its cards (this includes the new US-specific Debit ICC Application, if one is developed). Each application and profile would meet the Issuer's specific needs for authentication, cardholder verification, risk management, etc.

Application Selection between the chip card and the chip-enabled terminal would be performed as per EMVCo specifications. The Issuer, or the OBO party, would be responsible for verifying and generating EMV data. This can be done by modifying its authorization software, or adding new software that can perform this function.

Transactions would be routed using current routing logic (BIN, interchange rules, etc); however, the acquirer must ensure that the EMV transaction is routed to an EMV-compliant party.

Why Select an Authentication Strategy?

If all US Issuers do not uniquely identify each ICC Application on the card, their authorization system may not be able to **immediately determine which application was selected** by the chip card and the terminal. The system is therefore unable to immediately select the correct algorithm to verify the EMV data in the transaction request. Modification of the Issuer's software may be required to enable multiple requests to the HSM, and performance may be impacted.

Option 1: Each US Issuer Uses Unique Values to Identify Each ICC Application on a Card

When selecting this option, each Issuer must ensure that one of the following is true:

- The Application PAN (EMV Tag 5A) and therefore the corresponding Track 2 Equivalent Data (EMV Tag 57) are unique for each ICC Application on each chip card.
- If the Application PAN is not unique for each ICC Application on a chip card, then the Application PAN Sequence Number (EMV Tag 5F34) must be unique for each ICC Application on the chip card.

Standard processing will ensure that if the chip is read successfully by the chip-enabled terminal, the Track 2 data in the transaction request will contain the Application PAN for the selected ICC application, and the Application PAN Sequence Number will be included in the EMV-specific data that is passed to the Issuer.

Using the Application PAN and the Application PAN Sequence Number, the Issuer or OBO party will be able to determine the correct algorithm and key to use to verify and generate EMV data.

The correct information would be sent to the Issuer or OBO party's HSM, thereby reducing the potential number of calls to the HSM.

Option 2: Each US Issuer Uses Common Values to Identify Each ICC Application on a Card

If this option is selected, each Issuer must ensure that:

- The PAN (EMV Tag 5A) and the Application PAN Sequence Number (EMV Tag 5F34) are the same for each ICC application on a card.
- The Derivation Key Index and Cryptogram Version Number, which are part of the Issuer Application Data (EMV Tag 9F10), must be the same for each ICC application on a card.
- The same Issuer Master Key (IMK) must be used to generate the Unique Derived Key (UDK) for each ICC application on a card.

The keys and algorithms used for every ICC application on that card would therefore be the same, so the unique cryptogram generated for each of the applications on the card would therefore be generated in the same manner.

The Issuer or OBO party would be able to verify and generate EMV data for any ICC application on the card, because the keys and algorithms would be the same for all ICC Applications on the card.

BEST PRACTICES THAT HELP MEET STAKEHOLDERS' BUSINESS NEEDS

To achieve true interoperability, comply with EMVCo and payment association specifications, comply with various US regulations (including Durbin), and still allow the flexibility of choice required by acquirers and processors, the US stakeholders must work toward the following goals.

- **To accept non-US chip cards, US terminals must be modified to support ICC Applications** for the global payment associations with which the terminal owner is affiliated, regardless of the ICC Application strategy selected by the stakeholders.
- **When a US-issued chip card is used at a US EMV-compliant terminal, all possible paths for the transaction must eventually support EMV**. However, until all associated entities in the US are EMV-compliant, all networks, acquirers, and processors must enhance their existing routing logic so that every transaction that contains EMV data will only be routed to an EMV-compliant party. After all acquirers, Issuers (or OBO parties), networks, and processors can handle EMV data, this routing logic will no longer be required.
- **Ideally, any entity publishing a specification for online transactions should modify that specification to include the AID.** If the AID was carried in all online transaction request messages, Issuers could quickly determine which ICC Application was selected between the chip card and the EMV-enabled terminal and thus know which algorithm and key to use to enable cryptogram verification. There would be no need for an EMV data authentication strategy, and no need for an Issuer to make multiple calls to the HSM when attempting to verify the cryptogram. Until all specifications, worldwide, include the AID in transaction request messages, Issuers will need a way to determine which ICC Application was selected between the chip card and the EMV-enabled terminal.
- **Ideally, US Issuers would all agree to use the same EMV data authentication strategy.** However, since this is unlikely, each Issuer or OBO party must be prepared to handle EMV data generated by chip cards — whether produced using one of the Issuer EMV data authentication strategies presented previously, or by another strategy not explored here.

- **Optimally, all US Issuers would be able to handle EMV data.** This includes verifying an ARQC, generating an ARPC, generating Issuer scripts, and using EMV data when making an authorization decision. The logic to perform these tasks would reside either in the Issuer's authorization software, or in an add-on product that is integrated with the Issuer's authorization software.

  If an Issuer is not able to handle EMV data (either in the short term or long term), any entity acting on behalf of the Issuer must be able to perform these tasks. If multiple OBO parties must perform these tasks for an Issuer, all of those OBO parties must possess the necessary keys or certificates. The Issuer and the OBO parties must establish appropriate key and certificate exchange procedures, and accept the risks associated with providing keys and certificates to multiple entities.

CONCLUSION AND CALL TO ACTION

Any EMV implementation plan includes issues that must be addressed, and stakeholders must consider all possible alternatives before making a decision. Creating or modifying ICC applications or profiles, and obtaining new AIDs for regional networks will introduce greater complexity into an already complex endeavor.

What Stakeholders Can Do

- Get educated! Invest in EMV training for your organization.
- Consult industry experts with experience in EMV migration.
- Review lessons learned from other regions where EMV is in place.

Certified and tested ICC applications and standard card profiles appropriate for the US are already available through payment associations. Using existing components will save stakeholders time and money as the industry implements EMV in the US.

Remember that regardless of the ICC application strategy selected, unless every Issuer is able to handle EMV processing, or has only one OBO party to handle all EMV transactions with all the keys required to do so, there will still be issues to address in the US related to managing the distribution and security of EMV-related keys.

As with all aspects of EMV, education is the key to understanding the issues and alternatives. When facing an EMV migration, stakeholders should not hesitate to call upon industry experts who have already been through this process. It is also important to review lessons learned in other regions that have already implemented EMV, so that the US can avoid costly mistakes, and ensure a successful migration to EMV.

Recommended Reading

If you need more information, refer to:

EMV FAQ from the Smart Card Alliance

What are Chip Applications and How are They Used?

What's Involved in Implementing a New US Debit ICC Application?

Is a New US Debit ICC Application the Answer?

ABOUT THE AUTHORS

Deborah Spidle, Director of EMV Solutions for Paragon Application Systems, has over 20 years experience in the IT industry, focusing on banking and financial applications. Most recently, Deborah has been responsible for helping a major national switch, a large bank, and multiple credit unions migrate to EMV.

During her career, Deborah has worn many hats including: development, business analysis, design engineering, program management, software implementation/installation management, project management, development management, technical writing, software installation, user testing, and client training. Deborah's managerial responsibilities have included the management of personnel across multiple disciplines (engineering, development, testing) as well as management of large, multi-functional project teams. Past clients have included financial institutions in the US, Canada, Brazil, Australia, and England.

Deborah recently earned the Certified Smart Card Industry Professional/Payments Certification (CSCIP/P) from the Smart Card Alliance, a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. She had previously earned the general CSCIP certification, and is among the first to achieve the new, Payments-specific certification.

Mansour Aaron Karimzadeh, Managing Director of SCIL USA, applies nearly 25 years of experience to his leadership role at SCIL. His background includes payment and transaction processing systems in the financial industry, an in-depth understanding of how to create new businesses and drive demand for emerging products and technologies. He has been instrumental in implementing many large card and payment processing projects worldwide specializing in smart cards and EMV systems - including projects in the UK, Canada, USA, Latin America, Middle East and Australia. He served as a Board member of Global Platform and Chair of its Marketing Center.

He previously managed a smart card consultancy and software company that was acquired by ACI Worldwide. At ACI he served as VP of Operations and Director of Smart Cards Unit. Mansour has been involved in the smart card based healthcare card in the USA.

Contributors:

Dana Blegen, Master Engineer, Paragon Application Systems
Nick Green, ISD Consultants, UK (www.isdconsultants.com)
Wendy Sibley, Senior Technical Writer, Paragon Application Systems