EMV Payments: Changes for Card Issuers

- Anna J. Scurry
- VP, Debit Card Issuing & Processing Products
- First Data
© 2013 First Data Corporation. All Rights Reserved.

This document contains unpublished, confidential and proprietary information of First Data Corporation. You may not disclose, copy or use any part of these materials for any purpose without the express written consent of First Data Corporation. All trademarks, service marks & trade names used in this material are the property of their respective owners.

Disclaimer

This Presentation is provided as a courtesy and is to be used for general information purposes only and as an overview of announced changes, high level system impacts and business impacts. First Data shall not be responsible for any inaccurate or incomplete information. The matters contained herein are subject to change. Individual circumstances may vary and procedures may be amended or supplemented as appropriate. It should not be used as a substitute for reference to the actual card brand/network release technical documents, rules and other official documents. This is not intended to be a complete listing of all applicable procedures. No information contained herein alters any existing contractual obligations between First Data and its clients.
Changes for Card Issuers

Overview of EMV Implementation Options

Considerations for Issuers
- Card interface choices
- Card verification methods
- Transaction authorization
- Offline/online PIN
- Fraud detection & eCommerce

Issuer Decision Points

Cardholder Education & Support

Summary
Plan Ahead

- Begin planning early to prepare for EMV and to accommodate 3-year card reissue cycle
- Work within existing reissue cycles to avoid mass reissue, which could increase fraud
- Note the outstanding industry questions that still remain around debit EMV, which may impact timing for adoption
- Understand EMV and your EMV options to help ensure a thoughtful approach and smooth transition
- Consider that EMV chips extend the life of the card, potentially extending reissue cycles to five years once magnetic stripe is retired
What do Issuers need to know to get ready?

Major tasks for an EMV launch are:

- Dialog and coordination with Associations on EMV program option recommendations, selection and certification requirements

- Design and procurement of chip card – current order & delivery lead times are 15-17 weeks

- Issuer system option discussions
  - Card issuance options
  - Card-level decisioning options

- EMV profile set up – translating program options into chip data
What do Issuers need to know to get ready?

Major tasks for an EMV launch are:

- Association testing and certification requirements
- Operational readiness, e.g. customer service staffing & messaging
- Testing and client roll-out strategy – how much and how fast
- Key Management - set up and exchange of new keys

An EMV chip card launch & processing requires the use of specific functionality and dialog with all enabling partners.
Considerations for Issuers
While chip cards are not a mandate, issuers need to start planning a chip-issuing strategy that considers:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuing Processor Readiness:</td>
<td><strong>U.S. Market</strong> already enables credit and some debit issuer EMV processing today and will continue to enable all credit and debit U.S. issuer EMV processing throughout 2013.</td>
</tr>
<tr>
<td>Dual Interface:</td>
<td><strong>Contact vs. Contactless</strong></td>
</tr>
<tr>
<td>Payment Applications:</td>
<td><strong>Single vs. Dual Application</strong></td>
</tr>
<tr>
<td>Cardholder Verification Methods (CVM):</td>
<td><strong>Offline PIN, Online PIN, Signature, None</strong></td>
</tr>
<tr>
<td>Transaction Authorization:</td>
<td><strong>Online vs. Offline Transactions</strong></td>
</tr>
</tbody>
</table>
## Considerations for Single vs. Dual Application

### Dual Applications for Debit

<table>
<thead>
<tr>
<th>Credit:</th>
<th>Only requires single application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debit:</td>
<td>Logistics for supporting this are still under discussion. US Market is actively working with our industry partners to determine the best solution for interoperability, and an update is anticipated early in 2013.</td>
</tr>
<tr>
<td></td>
<td>US Market interprets Durbin regulations to mean that regardless of the transaction type, at least two unaffiliated debit networks are required, and one way to accomplish this is with dual applications on the chip.</td>
</tr>
</tbody>
</table>

### Single Application

- Credit requires only a single application (e.g. Visa only or MasterCard only)

### Dual Application Options

- Some US Market PIN Debit Networks are adopting or have already developed solutions (e.g. STAR CertiFlash® technology which offers financial institutions a market-ready option for a second debit application). However, the industry direction still under discussion could have broader implications that impact these solutions.
## Considerations for Contact and Contactless

### Dual Interface Contact and Contactless
- Offers cardholders the convenience of paying the way they want – contact or contactless
- Future-proofs your card as more merchants adopt faster contactless acceptance
- U.S. Market - currently produce and support both contact and contactless EMV chip cards.

### Contact
- Merchants may prefer contact for high-ticket purchases, where the speed of individual transactions and the volume of transactions are not a factor

### Contactless
- Merchants may encourage contactless in high-volume, low-ticket situations where speed of transaction is important
### Considerations for Chip & PIN Cardholder Verification Method (CVM) Prioritization

#### Different CVM Priorities for Debit vs. Credit

<table>
<thead>
<tr>
<th>Type</th>
<th>Priority List</th>
<th>Details</th>
</tr>
</thead>
</table>
| Debit CVM  | 1. Online PIN 2. Offline PIN 3. Signature 4. None | - Online PIN: The terminal sends the PIN entered by the cardholder to the issuer processing system for verification  
- Online PIN verification is currently in use for debit |
| Credit CVM | 1. Offline PIN 2. Online PIN 3. Signature 4. None | - Offline PIN: The terminal verifies that the PIN entered by the cardholder matches the PIN on the chip/card  
- Offline PIN is consistent with standards outside the U.S. and is the most frequently used CVM outside the U.S.  
- Online PIN for credit has not seen widespread use since the introduction of EMV |

- **Set offline PIN** as the first priority for credit verification to increase security and decrease potential for fraud
- **Set online PIN** as the first priority for debit verification to reflect what is currently in use for debit
Considerations for Transaction Authorization

Enabling Online Transactions

- Enable online transactions for all cards
- Enable offline transactions to support international travelers
- Limit offline transaction parameters based on risk tolerance

Limiting Offline Transactions

- **Online Authorizations**: The terminal sends the transaction to the issuer’s processor for verification and approval.
- U.S. infrastructure supports online authorization

Online Authorization

- **Offline Authorization**: The transaction is approved or declined based on parameters within the chip on the card (offline approval allowed, dollar amount, number of transactions)
- Typically used when terminals do not have online connectivity (e.g., at a ticket kiosk) or where connectivity is unreliable or costly (mainly outside the U.S.)
Considerations for PIN Management

Limited Options for Cardholder to Select a PIN

- Use existing PIN for card reissue
- Allow cardholder PIN selection only prior to card production, otherwise send a system-generated PIN
- Do not allow PIN changes after cards have been produced
- If a PIN is not selected prior to card production, the system-generated PIN should not be changed

Online and Offline PIN sync

- Significant constraints for syncing online/offline PINs in the current marketplace will make changing a PIN confusing for cardholders
- The ability to sync PIN changes at POS and ATMs most likely will not be widely available until greater market adoption is achieved
Considerations for EMV Fraud Detection Strategy

Decisioning EMV authorizations through Fraud Detection systems like Falcon, may require changes to your existing strategies and possibly trigger the creation of new strategies.

- How will transaction elements I use today appear differently?
- What other transaction elements should I consider?
- How do I combine all of the transaction elements in a strategy to best identify when the potential for fraud exists?
Considerations for Impact on eCommerce Fraud

Global experience demonstrates adoption of chip technology can reduce fraud at POS but can drive higher card not present (CNP) fraud*

- UK: CNP fraud 62% of all fraud on UK cards (2010), compared to 30% in 2004
- France: CNP fraud 54% of all card fraud on French cards, up 25% since 2006
- Canada: From 2008 – 2010, CNP fraud losses increased 37%; overall CNP fraud losses were 31% of all fraud losses in 2008 & rose to 50% in 2010
- Australia: CNP fraud increased nearly 70% from 2008 – 2010

Leverage CNP fraud tools

- Increased verification methods (3D Secure) from Visa (Verified by Visa) and MasterCard (MasterCard Secure Code)

* "Fraud: The Facts", 2011, Financial Fraud Action UK

U.S. Market recommends online fraud protection solutions and increased verification methods for card not present
Issuer Decision Points
### Chip & Interfaces

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
</table>
| Plastic Vendor     | Different plastic vendors support different chip types because each chip requires a specific method for creating a secure channel during the initial stages of the chip data prep process.  
Note: Output Vendor’s unsupported chips may require script development  
-Even a chip, by the same chip manufacturer, utilized by a different vendor (e.g. Gemalto vs. CPI), will require additional work. |
| Interface          | Contactless interface alone does not support participation in the liability shift.  
Current contactless (U.S. domestic) interface specification is not truly an EMV spec; as it utilizes mag stripe data on the chip; these cards, as issued to-date, will not qualify for liability shift participation. |
| Chip Type          | KONA 141S and JCOP – support dual interface  
KONA 151S – supports contact only  
Different chips may be subject to delays based on due diligence of chip/vendor (may include additional certification, project work, scripting needs, etc.) |
| Operating System   | MultOS is an option, however very long project delays could ensue if MultOS is required.  
Global Platform supports both Visa and MC, and the chip First Data is utilizing for Amex supports Global Platform 2.1.1. |
# Chip Data Authentication

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
</table>
| Data Authentication Method (aka Offline Data Authentication) | • **Offline Chip Data Authentication** – validates the integrity of the chip itself. Will you be supporting Offline Data Authentication? If so, what method?  
  • **DDA - Dynamic Data Authentication** – utilizes chip data and dynamic transaction data for authentication  
    - More secure  
    - Significantly minimizes counterfeit fraud  
    - For use by contact interface only  
    - Includes RSA cryptographic support on the chip  
  • **Fast DDA (fDDA)** – utilizes a pre-defined list of data elements for authentication, rather than using the Default Data Object List (DDOL) that is on the card and used for standard DDA signatures  
    - fDDA is quicker due to less data used in the signature created by the card and subsequently verified by the terminal  
    - Mandated by Visa for use in contactless and dual interface, IF Offline Data Authentication is used |
# Chip Data Authentication

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Authentication Method (aka Offline Data Authentication)</td>
<td></td>
</tr>
</tbody>
</table>
| • **CDA - Combined Data Authentication** – utilizes a methodology of multiple iterations of DDA authentication (i.e. a second authentication step utilizing the transaction cryptogram)  
  - Mandated by MasterCard for use in contactless and dual interface, IF Offline Data Authentication is used  
| • **SDA – Static Data Authentication** – utilizes only static elements from the chip for authentication  
  - Less secure than other options  
  - More prone to fall victim to counterfeit fraud  
  - No RSA cryptographic support on chip  
  - Least costly  
  - This option is not supported for all Associations (e.g. MasterCard and American Express) |
## Chip Data Authentication

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
</table>
| Data Authentication Method (aka Offline Data Authentication) | • “Always online” – no chip data authentication used  
  - In cases where the issuer opts to always go online for transaction authorization and Cardholder Verification, issuer could choose to use a chip that doesn’t support any chip data authentication  
  - transaction will still send, and the host will still validate, the ARQC.  

* Note regarding backwards compatibility of chip authentication:  
Chips with a higher security capability are backward compatible with lower security methods. For instance a chip capable of performing DDA can “drop down” and perform SDA instead assuming the chip is encoded appropriately at perso. Kona 141/151 and JCOP support DDA and the 141 and JCOP are CDA capable as they are dual interface capable chips. Selecting either of the CDA capable chips ensures the issuer will be able to support whatever offline data authentication method they desire. |
| Application | CAP and DPA – enables card-not-present EMV-compliant transactions; could be supported in fairly short term. |
## Authorization Processing

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Processing</td>
<td>• Host auth processing options still apply for on-line authorization processing, with some new decision elements based on chip data.</td>
</tr>
<tr>
<td></td>
<td>• Offline authorization parameters are established via Off-line Risk Parameter settings on the chip. They may be modified via a script.</td>
</tr>
<tr>
<td></td>
<td>• Receipt of DE55 – Optional to receive if processor or association is conducting Cryptography On-Behalf-Of Issuer’s host system; Required if Issuer’s host system will conduct cryptography or builds auth strategy around the content of DE55.</td>
</tr>
</tbody>
</table>
## Authorization Processing

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scripting</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scripting is an optional service;</td>
</tr>
<tr>
<td></td>
<td>– Scripting options can be established via Rules setting at time of start up or via NMs later in program</td>
</tr>
<tr>
<td></td>
<td>– Scripting can only be done in context of a contact transaction</td>
</tr>
<tr>
<td></td>
<td>• Application block – Blocks usage of a single application (e.g. payment, transit) on the card</td>
</tr>
<tr>
<td></td>
<td>• Card block – Blocks usage of entire card</td>
</tr>
<tr>
<td></td>
<td>• PIN change – Valid for Off-Line PIN only; update PIN on the chip</td>
</tr>
<tr>
<td></td>
<td>• PIN unlock – Valid for Off-Line PIN only; Resets PIN try counter on the chip (Note: the PIN try counter on the card is only decremented for offline PIN attempts)</td>
</tr>
<tr>
<td></td>
<td>• Auth Parameter changes – See Offline Risk Parameter</td>
</tr>
</tbody>
</table>
## Card Verification

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Verification Method</td>
<td><strong>Off-Line:</strong> PIN stored within the chip on the card; verification takes place at POS between card and terminal; at this time, Offline PIN CVM requires a contact interface; PIN Management challenges need to be considered; allows greater level of usage coverage (Interoperability)</td>
</tr>
<tr>
<td></td>
<td><strong>On-Line PIN:</strong> PIN verification takes place at host system; required as the CVM for Cash Advance at ATM transaction types.</td>
</tr>
<tr>
<td></td>
<td><strong>Signature:</strong> Chip card protection is reduced to merely that which is afforded via the chip authentication (SDA, DDA, CDA); Cardholder verification is reliant upon validation of signature, cardholders may experience reduced interoperability in regions that require PIN</td>
</tr>
<tr>
<td></td>
<td><strong>No CVM:</strong> Usually the last CVM option; issuers are not required to support “No CVM” option, but it is recommended to promote widest usability (e.g. at QSRs – Quick Service Restaurants)</td>
</tr>
<tr>
<td>On-Line Risk Parameters</td>
<td>Parameters are often enabled in both fraud and risk management systems as well as card management rules.</td>
</tr>
</tbody>
</table>
## Risk Parameters

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off-line Risk Parameters</td>
<td>These settings only apply at a transactional level if off-line authorizations are used.</td>
</tr>
</tbody>
</table>
## Risk Parameters

<table>
<thead>
<tr>
<th>Component</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Off-line Risk Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>LCOTA – <strong>Lower Cumulative Offline Transaction Amount</strong> – Issuer-specified preference for the maximum total transaction amount(s) before an on-line authorization is preferred.</td>
<td></td>
</tr>
<tr>
<td>UCOTA – <strong>Upper Cumulative Offline Transaction Amount</strong> – Issuer-specified preference for the maximum total transaction amount(s) before an authorization is declined by the card I the terminal cannot go online.</td>
<td></td>
</tr>
<tr>
<td><em>LCOTA &amp; UCOTA are used for transactions performed in the issuer currency.</em></td>
<td>This is only used for transactions performed in the Issuer currency.</td>
</tr>
<tr>
<td>For Off-line Risk Parameters, there is the concept of “Online Preferred” – which means setting the lower limit values, LCOL and LCOTA, to zeros and UCOL to a “reasonable” number of transactions allowed offline. These settings will force the transaction to go on-line for authorization if able, and if not able to go on-line, still allow a set number of transactions offline.</td>
<td></td>
</tr>
</tbody>
</table>
Cardholder Education & Support
First Data EMV surveys: Security is the most appealing value to EMV among consumers

- Without education, majority of consumers would not change their credit card usage if an EMV transaction required a PIN
- When informed that a PIN adds security, the percentage of consumers more likely to use their credit card increases to 24%

Consider industry rollout timing at merchants when planning for cardholder communications

Communicate as clearly, consistently and simply as possible following industry standards
Kitchener-Waterloo pilot yielded important lessons about consumer and merchant education (Canada)

- Positive customer experience was a key success factor
- Consumers need to associate a PIN with credit, not just debit
- Consumers must remember to retrieve card from terminal after transaction completed
- How/where to complete offline PIN changes/resets
- Consistent terminal prompts (e.g. to take their card out of the card reader) greatly reduced consumer frustration at the POS
- Multiple touch points starting prior to card issuance: Direct Mail, FAQs, web site and/or EMV microsite, IVR, Email, videos

Consider customer support needs for next 3 – 5 years as full portfolio is migrated to chip payments

- United Nations Federal Credit Union (UNFCU): Implemented 24 x 7 Customer Service to assist with any EMV-related question and type of service may be based on portfolio / demographics
Cardholder messaging ahead of the reissue cycle should communicate:

- Your new card will have a chip that makes it more secure.
- Your current PIN will remain the same
- If you want to select a different PIN for your new card, you must change the PIN on your current card before (date of card production)
- You’ll start to see a new way to use your card at stores – insert or tap your card when making purchases
- Your card should also be accepted when you travel abroad
## PIN is a Key Decision

### How will consumers change their offline PIN?

- **Europe**: Easily updated online at ATMs
- **Canada**: Major national issue resolved by implementing PIN change at Canada Post
- **U.S.**: To be determined…

### Options for consumers to set up, change or reset their offline PIN

- **In branch**: Original PIN set up offers opportunity to meet with customers, answer questions, offer additional services
- **ATM**: Offers 24 x 7 availability but requires upgrade
- **IVR**: Requires consumer to understand complexity involved the first time card is used after change is made and challenges with unique PIN by cardholder
- **No changes**: Do not allow issued PIN to be changed

### May involve coordination with ATM upgrade strategy for EMV

If ATMs do not support EMV PIN changes at same time EMV cards are issued, what other mechanisms are in place to change PIN?
## Summary

<table>
<thead>
<tr>
<th>Topic</th>
<th>Implications &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Launch Date</td>
<td>Plan for a six-to-nine month project for initial launch</td>
</tr>
<tr>
<td>Portfolio Type</td>
<td>Debit? Credit? Both?</td>
</tr>
<tr>
<td>Chip Card Procurement</td>
<td>First Data can perform procurement and will work with vendors to order chips to meet specs. First Data works with specific chip types at this time</td>
</tr>
<tr>
<td>Contact-only or Dual Interface</td>
<td>Contactless-only interface does not support participation in the liability shift</td>
</tr>
<tr>
<td>Offline Data Authentication</td>
<td>Impacts the type of chip needed, as well as data sent to the chip</td>
</tr>
<tr>
<td>Cardholder Verification Methods</td>
<td>Offline PIN; Online PIN; Signature; No CVM</td>
</tr>
<tr>
<td>PIN Management</td>
<td>PIN management changes allowed? Customer Selected PIN?</td>
</tr>
<tr>
<td>On-Line Risk Parameters</td>
<td>Fraud Detection Strategy</td>
</tr>
<tr>
<td></td>
<td>PIN Authentication method</td>
</tr>
<tr>
<td></td>
<td>Card Activation</td>
</tr>
<tr>
<td>Off-line Risk Parameters</td>
<td>Settings only apply at a transactional level if off-line authorizations are used. Values still must be set.</td>
</tr>
<tr>
<td>Authorization Processing</td>
<td>On-Line and Off-Line; Host auth processing options still apply for on-line authorization processing, with some new decision elements based on chip data.</td>
</tr>
</tbody>
</table>
Anna Scurry
First Data
440-779-2131
Anna.Scurry@FirstData.com

- Smart Card Alliance
  - 191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556–6828
  - www.smartcardalliance.org