Connected Payments
EMV Whitepaper

June 2015

Address correspondence to:

Manager, Information Solutions Group

NCR Corporation

Discovery Centre, 3 Fulton Road

Dundee, DD2 4SW

Scotland

Internet Address:

http://www.info.ncr.com/Feedback

It is the policy of NCR Corporation (NCR) to improve products as new technology, components, software, and firmware become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions, and operations described herein may not be marketed by NCR in all parts of the world. In some instances, photographs are of equipment prototypes. Therefore, before using this document, consult with your NCR representative or NCR office for information that is applicable and current.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book.

Revision History

Date	Changed By	Comment	Version
6/10/2015	MJM	Initial Document	

Table of Contents

Revision History iii

Table of Contents 4

What is EMV? 6

Global Adoption of EMV 7

Why issuers are choosing EMV 8

How EMV affects merchants 8

EMV Technical Basics 10

EMV Acronyms 10

Application ID Example AID 11

Common Application IDs (AID's) 11

Anatomy of a chip card 11

EMV Transaction Flow 12

MSR Transaction Flow 13

Connected Payments and EMV 13

EMV and P2PE Improve Security 13

EMV and P2PE Explained 14

P2PE Whitelist 15

Equinox P2P for New and Existing Deployments 16

New Deployments 16

Existing Deployments (RKI Injection) 17

Ingenico Terminals 19

Ingenico P2P for New and Existing Deployments 19

New Deployments 19

Existing Deployments 19

Verifone MX Terminals 20

P2P RSA Public/Private Key (Verifone MX Terminals Only) 20

MX900 devices and Certificates 21

MX P2P for New and Existing Deployments 22

New Deployments 22
Existing Deployments 22
Merchant definition of AID preference and prioritization 24
Offline EMV vs Offline Stand In 24
Connected Payments Configurable EMV Settings 25
Card Processing Profile 25
OpenEPS Transaction Sequence Changes 26
Alerting 27
Reporting 28
EMV PIN pad Support and Version Information 29
Testing and Certification 30
Certification Types 30
Card Brand Certification Programs 30
Recertification 31
Contact Information 32

What is EMV?

EMV is a specification standard implemented and embraced by major credit card providers to ensure the security and global interoperability of chip-based payment cards. EMV-enabled cards perform Chip-based transactions using Smart Card technology to secure transactions. EMV transactions require the use of PIN pad devices that support the use of EMV.

EMV® is a trademark dating back to 1999, after **E**uropay, **M**asterCard, and **V**isa, founded EMVCo, with the purpose of developing specifications for secure payment transactions. EMVCo is currently owned by American Express, JCB, MasterCard and Visa, and has six member organizations American Express, Discover, JCB, MasterCard, UnionPay, and Visa.

EMV chip card transactions improve security against fraud compared to magnetic stripe card transactions that rely on the holder's signature and visual inspection of the card to check for features such as hologram. The use of a PIN and cryptographic algorithms such as DES, Triple-DES, RSA and SHA provide authentication of the card to the processing PIN pad device and the card issuer's host system.

EMV transactions may require the use of a PIN, like Debit transactions, for security. Determination as to whether a PIN is required for a transaction depends on the chip settings, acquirer rules, and other criteria.

To enable communication with the embedded chip, the card is inserted into an EMV-enabled PIN pad device for the duration of the transaction; this allows an online request and response from the acquirer to interact with the card’s onboard chip.

Due to the improved messaging and the request-and-response nature of EMV, EMV-enabled cards give the card issuer more say and control over the transaction at the place and time of the transaction. The card no longer just represents an end account number governing transaction routing.

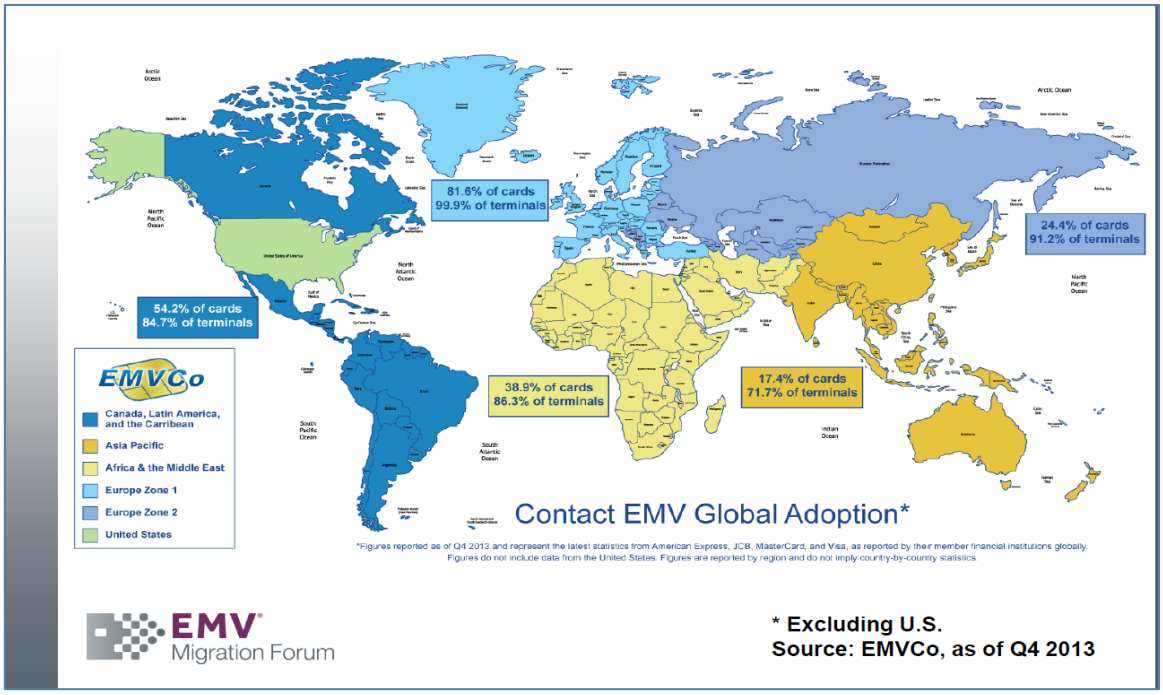
Contactless EMV will be is supported through the use of Near Field Communication (NFC); both card and card reader must support this technology. **NOTE: This feature is slated for NCR deployment in Q1 of 2016**

While EMV transactions reduce fraud by cryptographically confirming the card and transaction authenticity, EMV is not an encryption standard, and as such, the use of integrated Connected Payments end-to-end transaction encryption is still required to secure card and card holder data used in the transaction.

In cases where an EMV-secured transaction is not available, the card may often be read via the magnetic stripe; since this method is not authenticated via the EMV chip, these types of transactions (called EMV Fallback) entail all the current risks of a magnetic read.

Global Adoption of EMV

Because EMVCo provides a global foundation for chip-based payment services, adherence to its specifications ensures global interoperability and offers enhanced security and greater functionality



Global EMV Adoption*: 2.37 Billion Cards and 36.9 Million EMV PIN pad devices

Why issuers are choosing EMV

EMV represents a method of transaction processing that reduces fraud compared to magnetic stripe card transactions. Currently, card issuers are liable for all counterfeit fraud-related losses. However, as EMV cards are issued, liability for counterfeit fraud will shift to merchant **if the merchant is not EMV enabled**.

The card brands assign fraud liability based on the least secure party to the transaction.

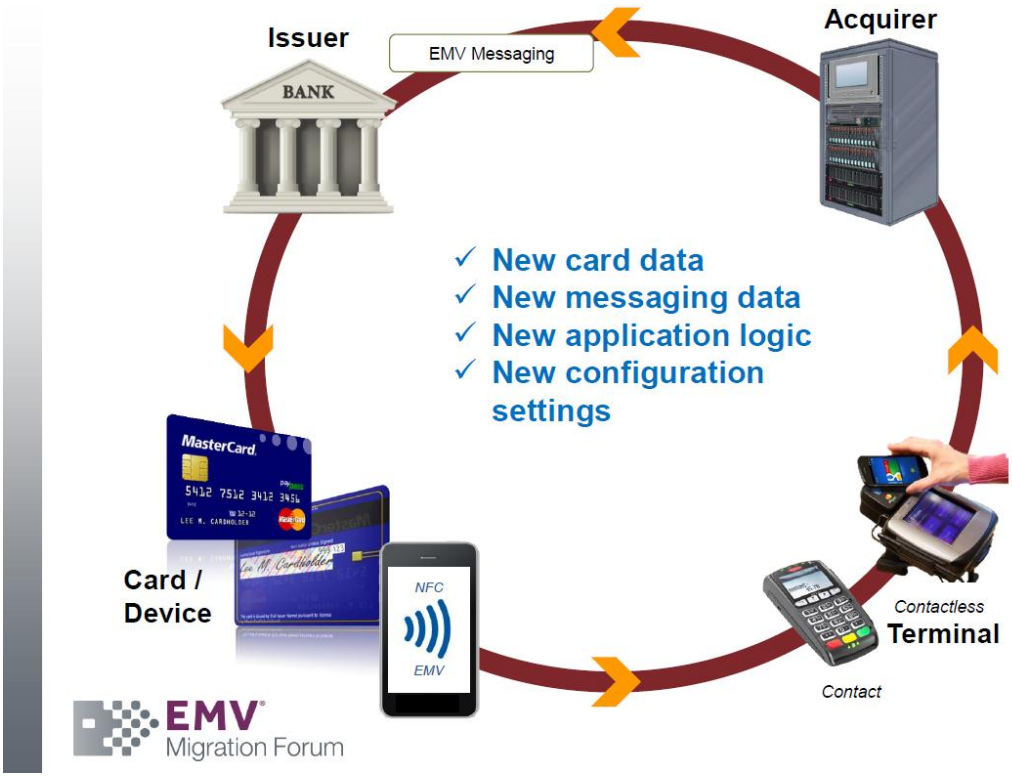
- For example:
  - A card issuer provides a card that does NOT contain a chip. That card is compromised in an EMV enabled store, liability shifts to the card issuer due to the distribution of a mag stripe only card.
  - A consumer with an EMV enabled card shops in a non-EMV enabled location and is forced to use the mag stripe. A fraudulent charge is made against the consumer's card; liability shifts to the non-EMV enabled merchant.

EMV transactions with PIN entry are also protected against fraudulent use of a lost or stolen card.

Issuers can support a single standardized EMV specification which enables Global interoperability of chip cards and payment devices; as a worldwide standard used by all countries, US cards can be accepted in any country that supports the EMV standard and with expanded adoption in the US, cards from abroad can be used in the US. Adoption in Europe has progressed such that European EMV cards are starting to be issued without MSR available; with EMV adoption, these cards will be able to be accepted in the US.

How EMV affects merchants

Card brands have dictated a liability shift in October, 2015: Any merchant not capable of accepting chip transactions will be liable for fraudulent purchases. As such, merchants are incentivized to support EMV-enabled transactions as thieves will likely target non-EMV enabled merchants once EMV adoption is commonplace.



EMV migration impacts all stakeholders involved in payment transaction processing

Often, support for EMV will include the need to purchase PIN pad devices capable of supporting chip-based transactions, as well as investing in the training of employees to smoothly handle the new EMV transaction flow, as the typical flow changes significantly. The most important change is that the card must be inserted into and remain in the PIN pad device for the entire transaction. In new EMV markets this often leads to a higher rate of cards left behind. Due to this inherent liability, merchants will have to employ secure, PCI compliant methods of dealing with card left behind situations. Please consult with your PCI auditor for best practice recommendations.

New EMV customers may not be aware of the nature of EMV, and may be surprised by the need for a PIN on a credit transaction; some customers may be unaware that their credit card possesses a PIN.

EMV Technical Basics

EMV Acronyms

- AID – Application Identifier
  - A value defined by [ISO 7816-5] and used to identify the application on the PIN pad device
  - An AID is comprised of a Registered Application Provider Identifier (RID) and a Proprietary Application Identifier Extension (PIX)
- RID – Registered Application Provider Identifier
  - RID's are registered with the ISO authority
- PIX – Proprietary Application Identifier Extension
  - PIX are assigned by the application provider (ex. Visa)
- CVM – Cardholder Verification Method
  - Ex. Offline PIN, Online PIN, Signature
- TVR – Terminal Verification Result
- TC – Transaction Certificate
  - A digital signature comprised of Issuer selected data objects. The TC is generated by the Chip Card at the end of an approved transaction, enabling the Issuer to verify that critical chip data was not changed prior to card validation
- ARQC – Authorization Request Cryptogram
  - A type of Cryptogram that is generated by a Chip Card when it determines that a transaction should be sent Online
- ARPC – Authorization Response Cryptogram
  - A type of Cryptogram generated by the Issuer, used to enable the Chip Card to validate the authorization response
- AAC – Application Authentication Cryptogram
  - A type of Cryptogram indicating that the Chip Card has declined the transaction
- TAC – Terminal Action Code
  - Rules in the PIN pad device which the device uses to determine whether a transaction should be approved offline, sent online for an authorization, or declined offline if online processing is not available.

Application ID Example (AID)

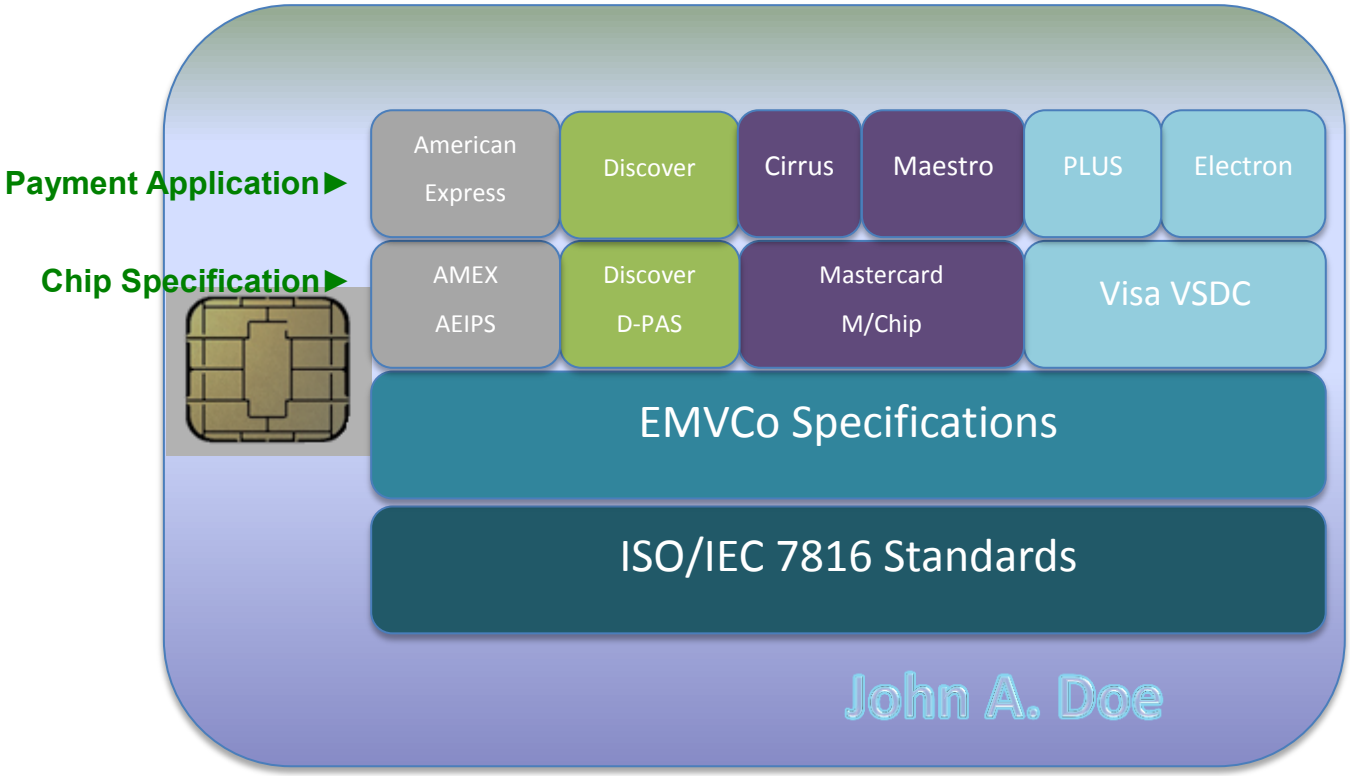
Example:

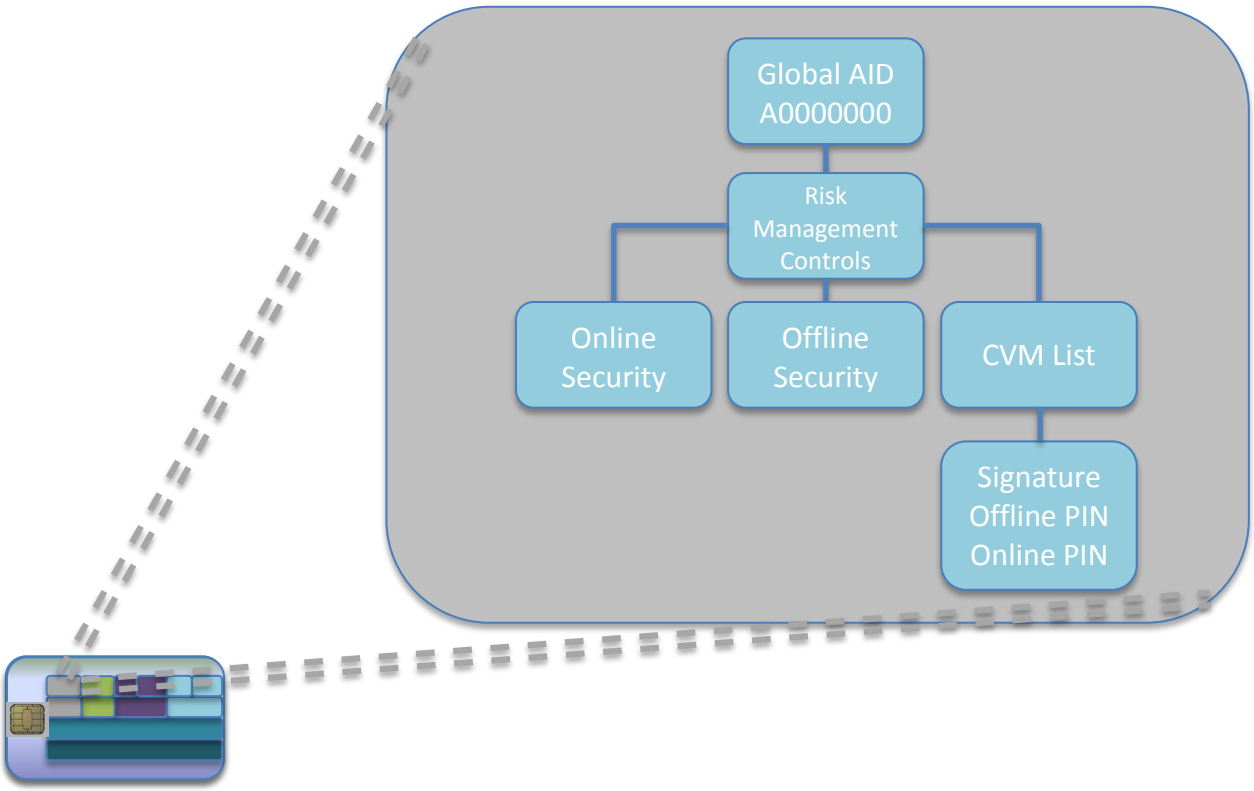
Card Product	Registered App Provider ID (RID)	Proprietary App Identifier Extension (PIX)	Application ID (AID)
Discover	A000000324	1010	A0000000031010

Common Application IDs (AID's)

Card product	Application ID (AID)
Visa Global	A0000000031010
Mastercard Global	A0000000041010
American Express	A00000002501
Discover	A0000003241010
Visa US Common Debit	A0000000980840
Mastercard US Common Debit	A0000000042203

Anatomy of a chip card





EMV Transaction Flow

The new EMV flow has significant differences from the current MSR card swipe flow. The biggest difference is the need to leave the card inserted in the PIN pad device for the length of the transaction.

- **1. Card is inserted into EMV PIN pad device's EMV chip reader**
- 2. First Half of EMV Transaction Protocol
  - A. Application Selection
  - B. Read Application Data
  - C. Offline Data Authentication
  - D. Processing Restrictions
  - E. Cardholder Verification
  - F. Terminal Risk Management
  - G. Terminal Action Analysis
  - H. Card Action Analysis
- 3. Online Authorization Request from Card to PIN pad device
- 4. Authorization Request from OpenEPS to Connected Payments
- 5. Authorization Request from Connected Payments to Acquirer
- 6. Authorization Response from Connected Payments to OpenEPS

- 7. Authorization Response from OpenEPS to PIN pad device
- 8. Completion and script processing. If Issuer approved but card denied the transaction, a reversal (void) for that transaction is generated
- 9. Transaction Information delivered to POS
- **10. Card is removed from EMV chip reader**

MSR Transaction Flow

The MSR Transaction flow below is provided for comparison to the new EMV flow to illustrate the differences between magnetic card swipe and EMV.

- 1. Card is swiped at the PIN pad device
- 2. PIN validated ONLINE (for Debit)
- 3. Authorization Request from OpenEPS to ServerEPS
- 4. Authorization Request from ServerEPS to Acquirer
- 5. Authorization Response from ServerEPS to OpenEPS
- 6. Information delivered to POS
- 7. Transaction Completed

Connected Payments and EMV

EMV and P2PE Improve Security

We at NCR are focused on keeping our customers secure. As a result of our commitment to our customer's security, EMV implementation will **require a hardware P2PE solution.** The hardware P2PE solution has been part of the Connected Payments suite for over 3 years and is distributed widely through our customer base. The NCR P2PE solution has been recognized as an approved method by the PCI council and is in the process of becoming a listed, certified P2PE solution. The following sections will outline the methodology and steps for updating your devices to P2PE via RKI (Remote Key Injection) as well as provide important versioning information.

EMV and P2PE Explained

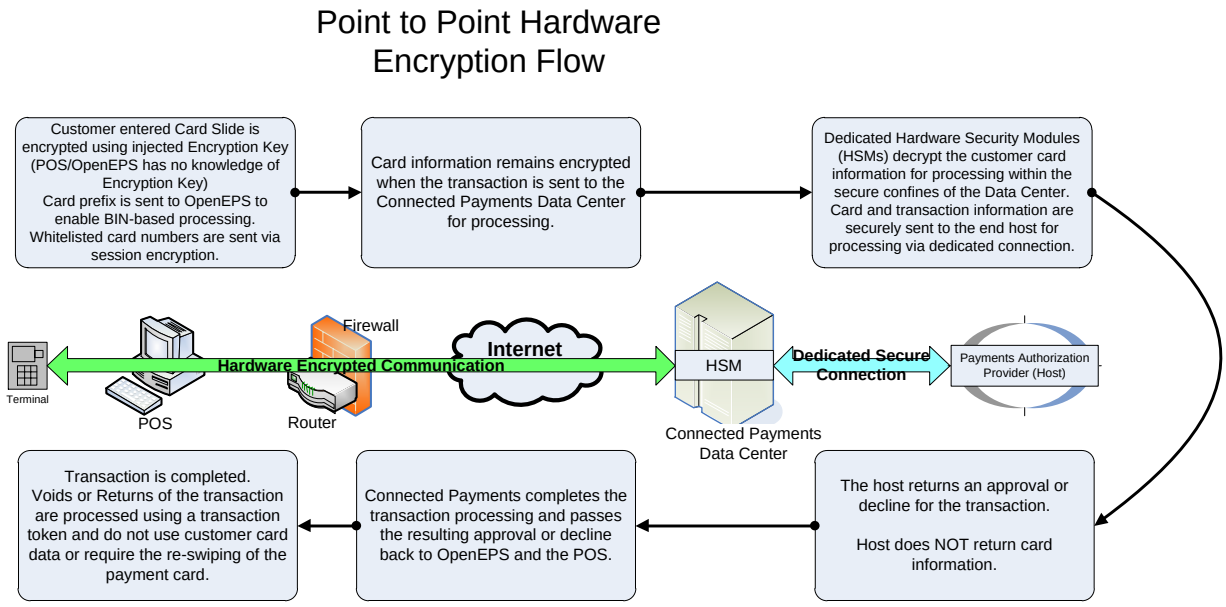
EMV and Point to Point Encryption (P2PE) both improve the security of a transaction, but do so in different ways.

EMV utilizes cryptography to digitally sign both requests and response messages, ensuring the card and transaction are legitimate; man in middle attacks are prevented from occurring though the use of transaction data as part of cryptogram generation.

EMV uses cryptography for authentication and prevention of fraud, but does not encrypt the contents of the transaction message. Point to Point Encryption supplied by Connected Payments ensures that the entire message is protected, and that sensitive card and card holder data from chip, mag stripe, or manually entered cards is not sent in the clear.

Using P2P encryption, card data is encrypted in the TRSM (Tamper-resistant security module) in the device and not decrypted until it reaches our data centers. OpenEPS does not have the ability to decrypt this data. This method is also known as End to End Encryption (E2EE) or simply Hardware Encryption.

P2PE encryption requires the injection of the NCR P2PE key into the terminal; this is often accomplished when the terminal is initially ordered, but potentially may be accomplished via Remote Key Injection for some terminals.



The following terminals support P2PE and ESE.

Terminal	Minimum Firmware Version	Minimum OpenEPS Version	Remote Key Injection	
			Independent	Through Connected Payments
Equinox L5300 3.0	7.P.409	828.1	Ethernet to Internet	No
Equinox L5300 2.0	7.P.409	828.1	Ethernet to Internet	No
Equinox L5200 3.0	7.P.409	828.1	Ethernet to Internet	No
Equinox L4150 2.0	5.P.138	828.1	Ethernet to Internet	No
Equinox L4150	5.P.138	828.1	Ethernet to Internet	No
Equinox L4250	5.P.138	828.1	Ethernet to Internet	No
Equinox L4100	5.P.138	828.1	Ethernet to Internet	No
Verifone 915 3.0	3.0.1 Build18	828.1.2X.465	No	packing list load
Veirfone 925 3.0	3.0.1 Build18	828.1.2X.465	No	packing list load
Verifone MX8XX	234E	828.1.2X.465	No	packing list load
Ing iSC350	2.0.9	828.1	No	packing list load
Ing iSC250	2.0.9	828.1	No	packing list load

Remote Key Injection (RKI) is either processed independently or through the Connected Payments network connection.

- No: This option for RKI is not supported
- Independent, Ethernet to Internet: The terminal must be detached from its normal cabling and plugged into an Ethernet cable with direct access to internet, and the manufacture must be contacted to perform the load.
- Through Connected Payments, packing list load: The terminal remains connected as per normal operation to Connected Payments, and a special signed packing list is loaded automatically.

P2PE Whitelist

P2PE using devices possess a whitelist. The whitelist contains card number ranges that are software encrypted using an AES session key and passed to OpenEPS to unencrypt, so that the full card number will be available to OpenEPS.

- For VeriFone devices, the whitelist is a file called the BET.DAT which can be a standalone tgz load or included in the FA load. Ranges listed in the BET.DAT will not be encrypted using the CHD.
- For Equinox terminals, the whitelist name can be vary, allowing *.TCMS, with typical default filenames being WL_ALL_PC2.TCMS (PCI terminal version 2) or WL_ALL_PC3.TCMS (PCI terminal version 3).

Customers determine their own whitelist ranges, based on need. Specifically, if any in-house gift cards, or the like require the POS system to acquire the full card number, then those card types should be included in the whitelist.

Once a customer determines what range or ranges are required to be whitelisted, the customer provides that list to NCR through Support (CustomerSupport@retalix.com); that list will be taken, formatted properly, and then securely signed before NCR assigns the list for automatic loading to the target Pin Pads.

Example BET.DAT Whitelist File:

This is an example of a BET.DAT file:


```
# This file contains the BIN ranges that will NOT be encrypted
700000-730000;
750000-780000;
500000-520000;
204400-204600;
```

Equinox P2P for New and Existing Deployments

New Deployments

When ordering new Equinox devices the following will need to be requested:

1. Request the injection of their host's debit key.
2. Request the injection of the NCR P2P key.

New terminals should have the above keys loaded, so that they are ready to be deployed once they reach the merchant location.

The terminals must be deployed in coordination with updates performed from the RGP side! As such, you will need to contact RGP and schedule a deployment date.

- Contact RGP and schedule a deployment date.

- This is the date that the terminals will need to be deployed into the merchant environment as well as the date that RGP will adjust the merchant settings to enable P2PE.
- Enabling P2PE may include a terminal load initiated by RGP as well as potentially a new OpenEPS DLL deployment. Good connectivity during this period will ensure rapid deployment.
- When contacting RGP, Support may request additional information about the merchant location, such as the Version of the POS software in use.

Existing Deployments (RKI Injection)

To perform Remote Key Injection for Equinox terminals, merchants will need to contact Equinox, provide Equinox the serial numbers of the PIN pads to be injected, and connect those pin pads to the internet.

1. Gather the serial numbers of the PIN pads to be injected.
    - Terminal serial numbers are often located on the outside of the terminal. Alternately serial numbers are reported to Connected Payments and are available for review via the Reports > PIN Pad Serial Number Report.
2. Contact Equinox and request Remote Key Injection; provide Equinox with the serial numbers of the terminals to be injected.
3. Contact RGP and request to be moved to P2PE; you may receive additional instructions on how to proceed, and additional information may be required. RGP will assign a new P2PE OpenEPS DLL to be automatically downloaded to the merchant location (828.1.2X.465 or later). You will be provided a conversion date when P2PE will go live; key injection must be completed by the go-live date, so make sure the date provided fits your injection schedule.
4. Equinox will provide information on when to connect the terminals to an internet facing connection. Terminals will need to be connected via Ethernet and will need to be able to establish an outbound connection to Equinox. This may require the terminals be disconnected from their location at the payments lane.
    - If the terminals are behind a firewall that prevents outbound connections, an outbound path will need to be opened; contact Equinox to determine what IP address or URL will be need to be opened up.
    - Steps for RKI Download
        1. Plug a standard Ethernet cable attached to an internet-facing network into the 100 Base T slot on the terminal.
        2. On the terminal, go to Setup.
        3. Go to ECR Port

4. Select TCP/IP Client; there is a small >> button, select that.
5. Enter the IP address and Port for the Equinox RKI network, provided by Equinox.
6. Select Apply Now. This will take you back to the setup menu screen.
7. Select Network.
8. On the 5300 there is only an option for Ethernet with the same >> button; select that button.
9. Select either DHCP or a static address; the address selected must be available and not in use by another device.
10. Select Apply now. This will take you back to the setup menu screen.
11. Select Exit.
12. Select Utility.
13. Select Download.
14. Select Download keys.
15. If the PIN Pad received a valid address using DHCP or a valid static address was entered, the pin pad will attempt to connect to the RKI system. If this step is working properly, download should take less than 1 minute.
16. Go back to the Main menu.
17. Select Setup.
18. Select ECR Port.
19. Select Serial line or USB, as applicable for how the terminal will be (or has been) attached to the POS system. Select Apply Now.
20. Exit all the way out of the menu until the PIN Pad goes to lane closed.
21. The terminal will reboot and is now ready for use.

5. Once a terminal has been successfully injected, it can be moved back to the payments lane for use.

Ingenico Terminals

Ingenico P2P for New and Existing Deployments

New Deployments

When ordering new Ingenico devices the following will need to be requested:

1. Request the injection of their host's debit key.
2. Request the injection of the NCR P2P key.

New terminals should have the above keys loaded, so that they are ready to be deployed once they reach the merchant location.

The terminals must be deployed in coordination with updates performed from the RGP side! As such, you will need to contact RGP and schedule a deployment date.

1. Contact RGP and schedule a deployment date.
    - This is the date that the terminals will need to be deployed into the merchant environment as well as the date that RGP will adjust the merchant settings to enable P2PE.
    - Enabling P2PE may include a terminal load initiated by RGP as well as potentially a new OpenEPS DLL deployment. Good connectivity during this period will ensure rapid deployment.
    - When contacting RGP, Support may request additional information about the merchant location, such as the Version of the POS software in use.

Existing Deployments

Customer sends in a list of serial #'s and they keys requested, P2P or Debit, Ingenico creates a signed file, we assign that like any standard screen file set, do our packing list load stuff and the pin pad does the rest.

1. Gather the serial numbers of the PIN pads to be injected.
    - Terminal serial numbers are often located on the outside of the terminal. Alternately serial numbers are reported to Connected Payments and are available for review via the Reports > PIN Pad Serial Number Report.
2. Contact Ingenico and provide them with a listing of the collected terminal serial numbers, and request either the NCR P2P key, or Debit key: Ingenico will create a signed file for the terminals that includes the requested key and provide that file to RGP.

3. Contact RGP and request to be moved to P2PE; you may receive additional instructions on how to proceed, and additional information may be required. RGP will assign a new P2PE OpenEPS DLL to be automatically downloaded to the merchant location (828.1.2X.465 or later). You will be provided a conversion date when P2PE will go live; the date provided will be the date when the new P2PE terminal code file will be downloaded to the merchant location.
4. RGP will receive the terminal code file from Ingenico and schedule it for download to the terminals.
5. The signed file will be automatically loaded to the terminals as part of the standard code loading process; terminals must be properly connected to the POS system and capable of processing transactions to Connected Payments in order to receive the update.

Verifone MX Terminals

P2P RSA Public/Private Key (Verifone MX Terminals Only)

1. Device must have public and private key pair injected by VeriFone.

- How to view RSA Public/Private Key Pairs on an MX Device:

Device	System Mode Menu	Screen Capture
MX800	Security>Key Status>RKL Key Status	
MX900	Security>Key Status>VRK	

2. Form Agent Load supporting Verifone Remote Key injection (VRK) with P2P off (CARD_RESPONSE_FORMAT=1, E2EE_ENCRYPT=0)
   - minimum version is 301-BUILD9 or 301-BUILD18 for MX900
   - minimum version is 233e for MX800
3. Load Card Holder Data (CHD) Key
4. Turn on P2P encryption by loading E2EE_ON.tgz (E2EE_ENCRYPT=1)

If the CHD key has not been loaded then the device will display "E2EE init failed" and require the CHD key to be manually loaded via direct download

MX900 devices and Certificates

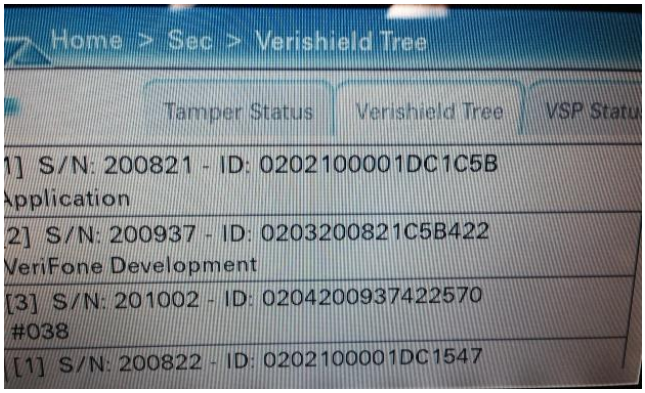
Devices may come preloaded with a NCR, Lab or Custom certificate. If this is the case, all future loads must be signed with the same certificate. The only exception is a Screen File load (MX915default.tgz) which may be unsigned if loaded via xdld (the process that OpenEPS uses to load the device automatically).

If the device does not have a certificate then whatever the device is first loaded with will determine the certificate. All future loads must be signed with that certificate. The only exception is a SF load which may be unsigned if loaded via xdld (the process that OpenEPS uses to load the device automatically).

As a rule, all packages must be signed so the customer may load the device via OpenEPS or direct download.

View Loaded Certificate

To view the certificate loaded on the device, navigate to Home>Sec>Verishield Tree and scroll down to view the application certificate.



MX P2P for New and Existing Deployments

New Deployments

When ordering new devices from VeriFone the following will need to be requested:

1. NCR or Custom Certificate(MX900 only)
2. Latest Form Agent Build supporting P2P and VRK (currently 301-BUILD18 for MX900 and 233e for MX800) with P2P (E2EE) turned on
   a) Include "Common MTX Config variables"
   b) E2EE_ENCRYPT=1
   c) CARD_RESPONSE_FORMAT=1
   d) Production WIC Keys
   e) BET.DAT if required (Whitelist for cards such as Fleet and Valulink) - by default there are no BIN exclusions and all cards will be P2P encrypted
3. NCR CHD Key
4. Debit PIN Key
5. Custom or Default Screen Files (optional - as these can be loaded with OpenEPS)
   a) Form Manager and Source Code available from ftp.servereps.com (please contact support for a username and password)
6. Request P2P dll assignment from RGP (828.1.2X.465 or later)

Existing Deployments

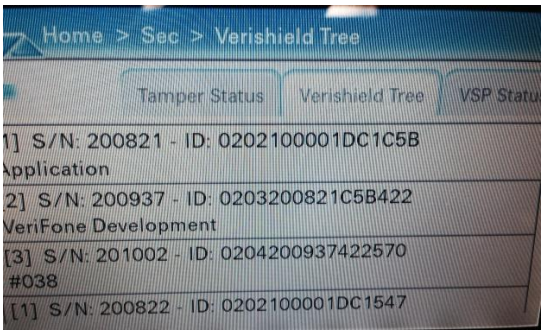
1. Confirm that VRK is supported by checking for the presence of RSA Public/Private Key Pairs

Device	System Mode Menu	Screen Capture
MX800	Security>Key Status>RKL Key Status	

Device	System Mode Menu	Screen Capture
MX900	Security>Key Status>VRK	

2. Determine Certificate currently installed on device (MX900 only):

   a) Navigate to Home>Sec>Verishield Tree and scroll down to view the application certificate.



3. Request Load Form Agent supporting VRK with P2P off (CARD_RESPONSE_FORMAT=1, E2EE_ENCRYPT=0) signed with certificate loaded in device.

   a) Minimum version is 301-BUILD9 or 301-BUILD18 for MX900

   b) Minimum version is 233e for MX800

   c) Include BET.DAT (Whitelist) as needed - by default there will be no Bin Exclusions and all cards will be P2P encrypted

4. Load NCR CHD Key signed with certificate loaded in device
5. Turn on P2P encryption by loading E2EE_ON.tgz (E2EE_ENCRYPT=1) signed with Certificate loaded on device.

   a) If the CHD key has not been loaded then the device will display "E2EE init failed" and require the CHD key to be manually loaded via direct download

6. Request P2P dll assignment from RGP (828.1.2X.465 or later)

NOTE: For information on RKI (Remote Key Injection) processes, please contact your NCR account representative.

Merchant definition of AID preference and prioritization

- Gives merchant configurable control of which AID they would prefer to process or present to the customer to selection when a chip card contains multiple AID's
- Stays within EMV requirements and does not impact certification
- There are certain cards with AID combinations that are required to prompt the customer which AID they would like to choose
- Connected Payments configuration will allow the merchant to limit as much as possible what AID's are displayed to limit complication for the customer and provide the merchant with routing preference
- Details on configuration options will be forthcoming

Offline EMV vs Offline Stand In

The US is an "online always" country.

Every transaction will be attempted as an online authorization

After the authorization is attempted but there is no response received at the lane, the card is notified that there has been no host response

There are two scenarios at this point:

- Offline EMV approval
  - The card may return a Transaction Certificate (TC)
  - This means that the card issuer is approving the transaction
  - Same as getting an online approval
- Offline Stand In
  - The card, in most cases, will return an "AAC" (Application Authentication Cryptogram)
  - This is essentially a decline from the issuer
  - The merchant may choose to stand in at this point, using the same floor limits as previously used for mag stripe
- Merchant accepts same liability as before

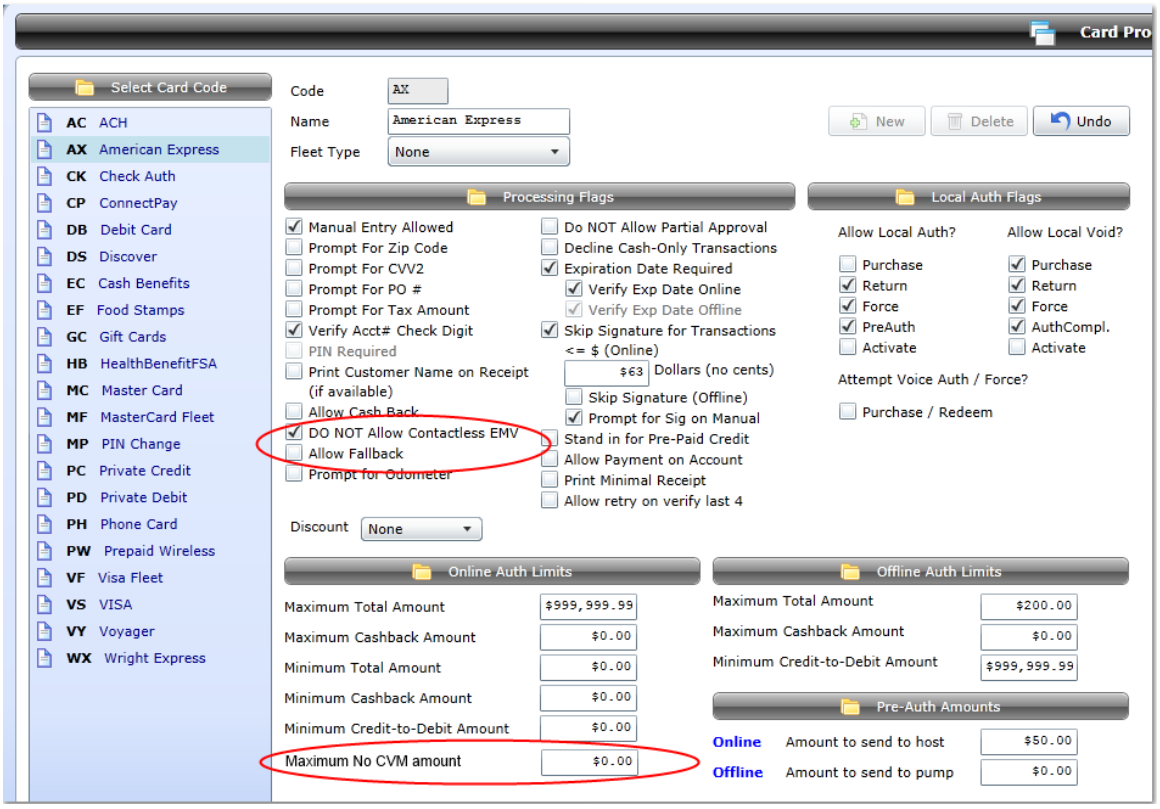
Connected Payments Configurable EMV Settings

Connected Payments offers simple configuration options for several aspects of EMV transactions.

Card Processing Profile

All Connected Payments Card Processing Profile configuration options are available by signing into your Connected Payments account, and accessing the Administration > Store Configuration link.

EMV settings are available in the Card Processing Profile and linked to the Transaction Sequence, so each setting can be configured on a per-card and per-transaction type basis.



Options Include:

- Do NOT Allow Contactless EMV

  With this setting activated, Contactless EMV transactions will not be allowed for this Card Type.

- Allow Fallback

  EMV Fallback is the conversion of a transaction from EMV to swiped. This can occur when and EMV chip is damaged or unreadable. In this case, the user will be prompted to swipe the magnetic stripe on the EMV card to complete the transaction.

- Maximum No CVM Amount

  Used with low dollar amount transactions.

  The value entered here, if any, will determine what value (and under) the transaction can be processed without using a Cardholder Verification Method (CVM); if the transaction meets this criterion, no PIN will be requested and no customer signature will be prompted for.

OpenEPS Transaction Sequence Changes

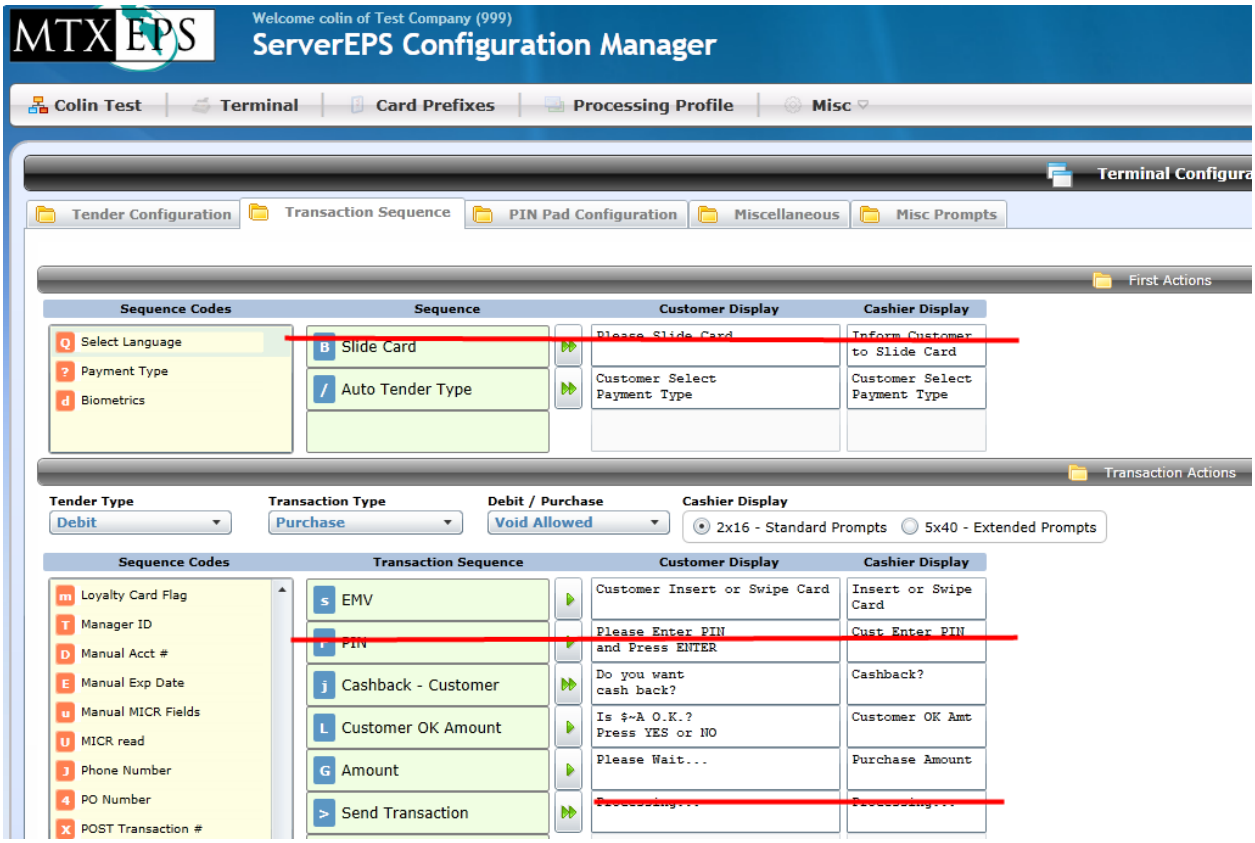
All Connected Payments Transaction Sequence configuration options are available by signing into your Connected Payments account, and accessing the Administration > Store Configuration link.

OpenEPS uses a highly configurable TAC sequence to drive transactions; this sequence is customer configurable, and contains configurable customer and cashier prompt text.

Please note that during an EMV transaction, several portions of the transaction process are driven by the PIN pad device itself and the EMV flow configured in the PIN pad application software. Processes like PIN entry and re-enter PIN prompts are driven by the PIN pad device. As such, many EMV-related text prompts are hard coded and are not subject to configuration.

Hard coded prompts are often defined in multiple languages and the EMV cards themselves contain a “Customer Preferred Language” tag. If the language is supported by the PIN pad device, the prompts adjust to display the preferred language.

Example of new terminal driven configuration:



In the above example, the Slide Card portion of the sequence no longer applies as EMV requires the card to be inserted. Card slide will be enabled only if the EMV chip cannot be utilized and fall back is allowed.

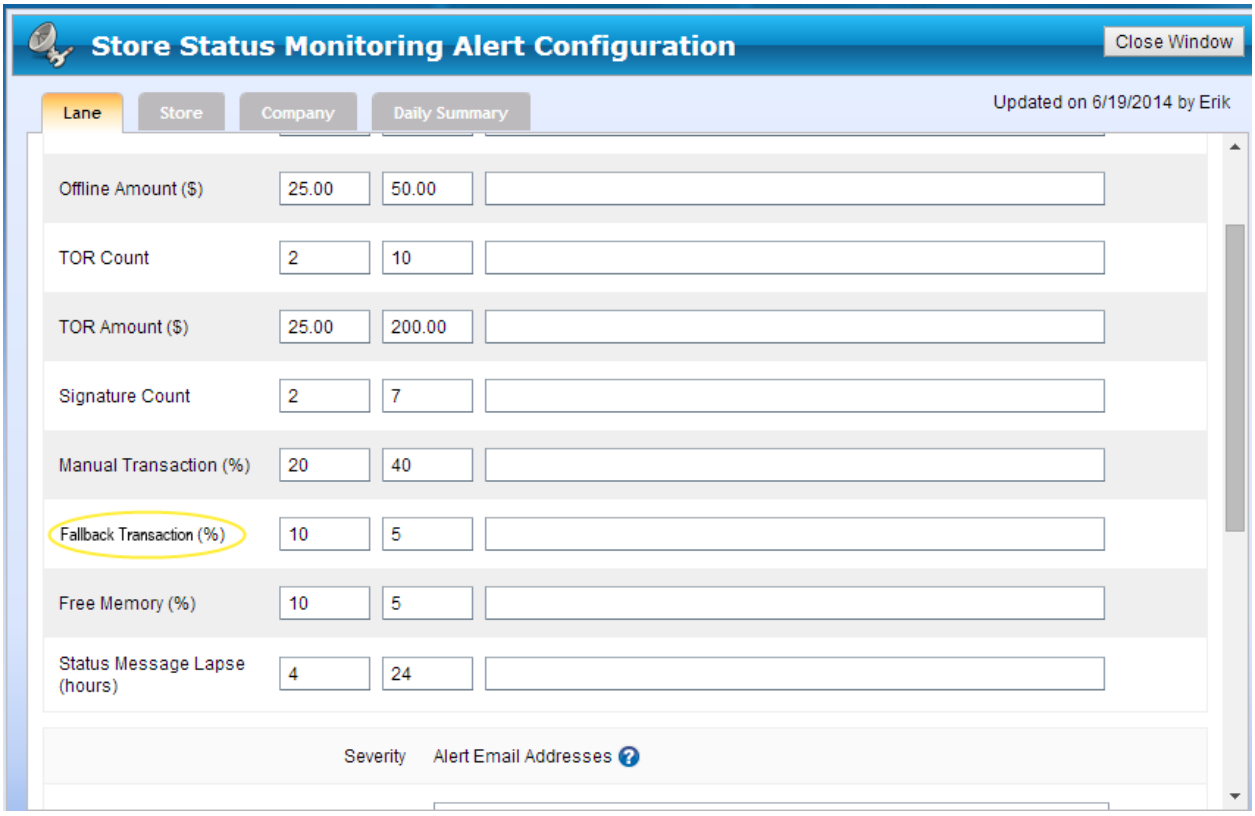
The PIN entry portion of the transaction is similarly hard coded; the prompts are integrated into the EVM process and the text cannot be configured in the Connected Payments system.

The final transaction “sending” text is overridden by the EMV flow as EMV contains built in request and response process that confirms with the host the final transaction disposition. This procedure can end as an approval, decline, or an alternate EMV flow, such as requesting a card swipe (fall back).

Alerting

All Connected Payments Alerting configuration options are available by signing into your connected Payments account, and are accessible through the Monitoring > Store Status link.

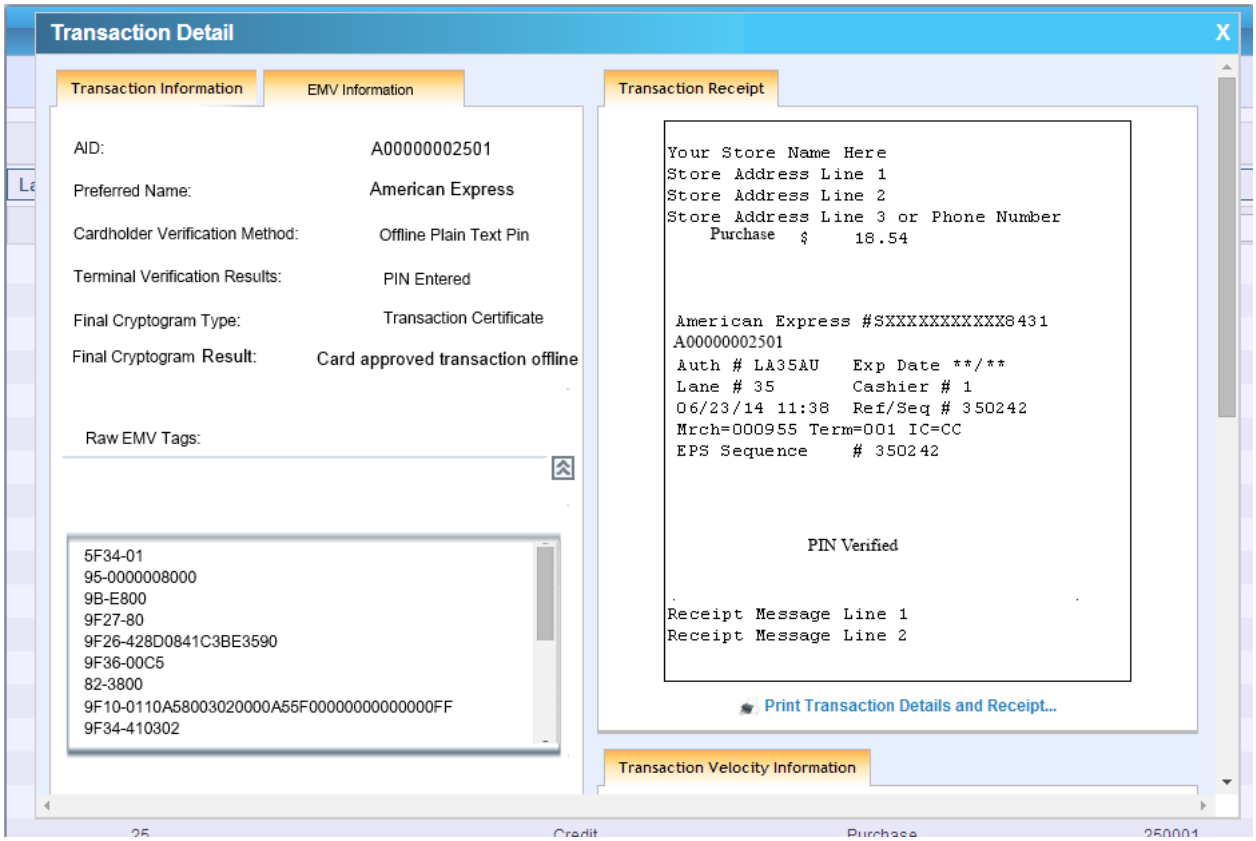
To assist in monitoring the EMV process, a new configurable alert for fallback percentage has been added to the Lane alerts list. Fallback for EMV is generally a magnetic card swipe although any fall back scenario is treated similar to that of manual transactions, as a high risk transaction type. This new alert can assist in tracking how often fallback occurs.



Reporting

All Connected Payments Reports are available by signing into your connected Payments account, and are accessible through the Reports link.

When viewing the listing of processed transactions via the Connected Payments Transaction Search feature, you may select an individual transaction and use the EMV Information Tab to review the EVM details for that particular transaction.



EMV PIN pad Support and Version Information

The following charts detail the minimum versions of PIN application and minimum versions of other PIN pad software components required for processing EMV:

VeriFone	O/S	Form Agent	XPI
Mx9xx	RFS30140200	3.0.3	5200jb6
Mx8xx	RFS00000018	2.4.0	4200hBuild3

OpenEPS Version 828.7

Equinox	Firmware	FPE
L5200/5300	5.05	5.2.0

OpenEPS Version 829.x

Ingenico	Firmware	RBA
iSC250 / iSC350 / iSC480	N/A	14

Please note that versions WILL change as new functionality is introduced to PIN pad application Kernels, Updated AID support, OpenEPS enhancements, OS version changes, etc…

Testing and Certification

Although the NCR team is performing vendor level EMV certification with all supported acquirers, adoption of EMV may require a merchant level certification. Please check with your acquirer customer representative to see if your implementation requires additional certification efforts.

Certification Types

Certification Type	Performed by
Level 1: Certification of the device's electrical, mechanical, and communication protocol	PIN pad Manufacturer
Level 2: Certification of application software (EMV kernel) ▪ Typically performed by the device manufacturer but could fall to a third party software provider	NCR Connected Payments Team
Level 3: End-to-end certification ▪ Typically managed by host/acquirer ▪ Merchants are typically involved to some degree in this portion. ▪ Level of involvement depends greatly on the host/acquirer ▪ Certifications typically take 1-3 months(varies depending on host/acquirer)	NCR Connected Payments Team

Merchants should get in contact with their host/acquirer to determine the nature and extent of required certifications, and should work any expected certification times into their plan to deploy EMV.

Card Brand Certification Programs

Depending on the card provider, the certification process will vary. Below are typical certifications performed as required by the listed card provider.

- American Express (30 tests)
  - American Express ICC Payment Specification (AEIPS)
- Discover (24 tests)
  - D-PAS Acquirer-Terminal End-to-End (E2E)

- MasterCard (114 tests)
  - MasterCard terminal integration process (M-TIP)
- Visa (105 tests)
  - Acquirer Device Validation Toolkit (ADVT)

Recertification

If a merchant makes changes to their EMV environment, they may have to participate in recertification depending on scope and area of the changes.

Examples of changes that could require merchant recertification:

- Change PIN pad device to a device with a different kernel than was originally certified
- Installation of a new PIN pad device family
- Addition of support for a new AID (Most likely smaller recertification around affected application)

Examples of changes that do not require merchant recertification:

- Adding support for new card prefixes
- Changing customer display text (If text is configurable)
- Updating PIN pad device screen files with new marketing
- Any changes to Connected Payments configuration

Contact Information

Retail Global Payments

85 Argonaut

Suite 150

Aliso Viejo CA, 92656

Tel: 949-614-1600

E-mail: **CustomerSupport@retalix.com**

NCR Corporation

NCR Corporation

Discovery Centre, 3 Fulton Road

Dundee, DD2 4SW

Scotland

Web site: http://www.info.ncr.com/