Terminal Enhanced Encryption

Point to Point & Software Encryption

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.

Revision History

Date	Changed By	Comment	Version
6/6/2014	MJM	▪ Created doc based on the MX Terminal Enhanced Encryption (P2P, ESF) (2014 04-03) doc.	1
9/9/2014	MJM	▪ Updated Format to NCR	
		▪	
		▪	
		▪	

Table of Contents

Contacting RGP

When purchasing terminals for use with P2PE or converting preexisting terminals to P2PE, you may need to contact Retalix Global Payments. Use telephone number and/or email address provided in the Contact Information section at the back of this document to reach RGP.

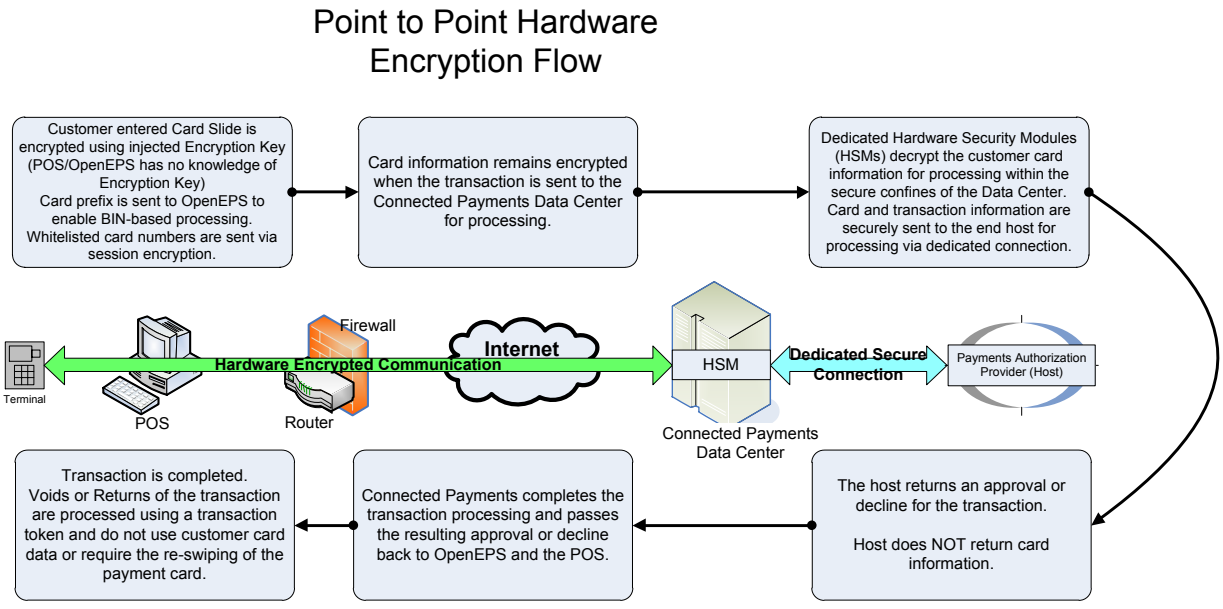
Terminal Encryption

P2PE vs. ESE Explained

P2PE (Point to Point Encryption)

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 knowwn as End to End Encryption (E2EE) or simply Hardware Encryption.

P2PE encryption requires the injection of the Retalix 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. Refer to the Supported Terminals chart below, and the individual terminal sections for encryption key injection instructions.



ESE (Enhanced Software Encryption)

In ESE, card holder data is encrypted using a session key, and not decrypted at OpenEPS. Since the encryption key is part of the loaded software, the terminal does not require the key to be specially injected; however, because software encryption is not handled by dedicated hardware components it is not considered as secure as Hardware P2PE.

Supported 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 avaialbe 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 (ConnectedSupport@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 Terminals

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 Retalix 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.

5. Once a terminal has been successfully injected, it can be moved back to the payments late 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 Retalix 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

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 Retalix 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

ESE Specifics

ESE Required DLL

Requires non-P2P dll (support began in 828.1.1X.465)

Enhanced Software Encryption

1. Load FA package supporting Enhanced Software Encryption (CARD_RESPONSE_FORMAT=1, E2EE_ENCRYPT=0)
   - Minimum Firmware versions are listed in the Supported Terminals chart.

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 Retalix, 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.

Response Format for Card Data:

ResponseCodeFirst6PAN<FS>Last4PAN<FS>ServiceCode<FS>ExpiryDate<FS>PANLength<FS>Cardholder Name<FS>CardDataSource<FS>**[KSN<FS>E2EEEncryptedData]/[SessionKeyEncryptedData]**

P2P/ESE ResponseCode:

ResponseCode	Meaning
00	where the E2EE encrypted data is sent along *Note: for a Manual card entry expiry date, the response code will always be 00*
01	where the card read request is cancelled for multiple bad swipe attempts (per configuration) OR track2 is invalid OR not read OR in manual card data request, when the request packet is invalid (combination of PAN/expiry date/CVV is requested in a single command)
02	If session key is not established when E2EE encryption is enabled
03	where the session key encrypted data is sent along (driving licenses/E2EE encryption failure)
04	where the session key encrypted data is sent along (BIN exclusion case)
05	Session key encrypted data (when E2EE_ENCRYPT=0).

OpenEPS logging for message type 00 (P2P):

```
11/11/13 10:45:13.499 SERIAL 00000804 Field First6PAN [600639]
11/11/13 10:45:13.499 SERIAL 00000804 Field ServiceCode [000]
11/11/13 10:45:13.499 SERIAL 00000804 Field ExpiryDate [0000]
11/11/13 10:45:13.499 SERIAL 00000804 Field PANLength [15]
11/11/13 10:45:13.499 SERIAL 00000804
TSCATMessage_MX870_GetCardData_Response.ParseMessageData -
Result=True, MessageType=00, FieldCountEx=11, CurrentTAC=B
11/11/13 10:45:26.358 SVREPS ::::::::: SE_SEND(TimeOutSecs 050):
thread[1956] URL[https://testtrn1.servereps.com/]
MSG[MTX[1E][1]2TAa211[1C]Ab3[1C]Ac000501[1C]Ad20131111104526[1C]Ae0205
55[1C]AhVT00005[1C]ArY[1C]Be****[1C]BfS[1C]BnPD[1C]Bo600639[1C]Bp4708[
1C]BqPrivate
Debit[1C]Da300[1C]Dk988[1C]Ga02[1C]Gb1[1C]GfG[1C]GhB/GF>[1C]GkOE1[1C]I
a***************[1C]Ib***************[1C]Ic169-008-
949[1C]Ig3|1|MX2010-
10[1C]Im****************************************|FFFF9876543210E00
0B6[1C]Oa18]
```

OpenEPS logging for message type 05 (ESE):

```
02/06/14 09:09:15.560 SERIAL 00001934 Field First6PAN [441277]
02/06/14 09:09:15.560 SERIAL 00001934 Field ServiceCode [101]
02/06/14 09:09:15.560 SERIAL 00001934 Field ExpiryDate [1612]
```

```
02/06/14 09:09:15.560 SERIAL 00001934 Field PANLength [16]
02/06/14 09:09:15.560 SERIAL 00001934
TSCATMessage_MX870_GetCardData_Response.ParseMessageData -
Result=True, MessageType=05, FieldCountEx=10, CurrentTAC=B


02/06/14 09:09:30.992 SVREPS ::::::::: SE_SEND(TimeOutSecs 040):
thread[8460] URL[https://trn1.servereps.com/]
MSG[MTX[D8][1]2TAa100029[1C]Ab304[1C]Ac000101[1C]Ad20140206090930[1C]A
e041042[1C]Ah00001967[1C]ArN[1C]Be****[1C]BfS[1C]BkD[1C]BnDB[1C]Bo4412
77[1C]Bp8731[1C]BqDebit
Card[1C]Da7368[1C]Dk988[1C]Ga04[1C]Gb211[1C]GfG[1C]GhB/GFjL>[1C]GkOE1[
1C]Ia***************[1C]Ib***************[1C]Ic099-592-
510[1C]Ig2|2|MX2010-
10[1C]Ih**********************************************************
**[1C]Im**********************************************************
**********************************************************************
************************************[1C]Oa18]
```

OpenEPS logging for message type 04 (Bin Exclusion Case):

```
11/11/13 11:47:16.169 SERIAL 00000CA0 Field First6PAN [523345]
11/11/13 11:47:16.179 SERIAL 00000CA0 Field ServiceCode [101]
11/11/13 11:47:16.179 SERIAL 00000CA0 Field ExpiryDate [1502]
11/11/13 11:47:16.179 SERIAL 00000CA0 Field PANLength [16]
11/11/13 11:47:16.179 SERIAL 00000CA0
TSCATMessage_MX870_GetCardData_Response.ParseMessageData -
Result=True, MessageType=04, FieldCountEx=10, CurrentTAC=B
11/11/13 11:47:23.800 SVREPS ::::::::: SE_SEND(TimeOutSecs 040):
thread[2644] URL[https://testtrn1.servereps.com/]
MSG[MTX7[1]2TAa211[1C]Ab3[1C]Ac000201[1C]Ad20131111114723[1C]Ae020568[
1C]AhVT00014[1C]ArY[1C]Be****[1C]BfS[1C]BnMC[1C]Bo523345[1C]Bp0102[1C]
BqMaster
Card[1C]Da200[1C]Dk988[1C]Ga02[1C]Gb1[1C]GfG[1C]GhB/G>[1C]GkOE1[1C]Ic1
69-008-949[1C]Ig1|2|OE2010-
10[1C]Ij**********************************************************
**[1C]Il**********************************************************
**[1C]Oa18]
```

Sample messages (Not logged in OpenEPS):

P2P:

```
Transmit: <STX>Q13<ETX>P
Receive : <ACK>
Receive : <STX>00526861<FS>6006<FS>101<FS>1812<FS>16<FS>ARCHANA SHAH
<FS>M<FS>FFFF9876543210E00006<FS>C65E9902336859619C77A9250D4D828F20FE4
43A2A355117AF41AC630FE243A76FA97280DE357E0EC7A0333328B483E8EE12CEFCA9F
1EA84195364CE6B5B87FE7A3F469BB2E924366932D20DA7490FE04AF8BE67039918673
7378CAA761FD38B5600CA1A8AEFAB13AD8B4E8FD2860BFD4DA1D385B3DA511D<ETX>o
Transmit: <ACK>
```

Bin Exclusion Case:

```
Transmit: <STX>Q13<ETX>P
Receive : <ACK>
Receive : <STX>04454198<FS>1077<FS>101<FS>1112<FS>16<FS>ARCHANA
SHAH<FS>M<FS>9D53153E438E15A83797A886F9817976CB200D0EA855A4B8D728E88A1
29A68715998468B4BFB71A4A97A1EF706CECF37A6479D9E3CD0C6B1503ACFC8DFEAED2
11D70546BA618E
646E08D52BF6F2F4C5E4F5872D28A20F04100B011DE98593A8109BEC591E9153C2D32E
34F4F3ADE8DDFFDBA5BC77B6F1930B4E29CE08DC59E3F<ETX><ETX>
Transmit: <ACK>
```

ESE:

```
Transmit: <STX>Q13<ETX>P
Receive : <ACK>
Receive : <STX>05454198<FS>1077<FS>101<FS>1112<FS>16<FS>ARCHANA
SHAH<FS>M<FS>9D53153E438E15A83797A886F9817976CB200D0EA855A4B8D728E88A1
29A68715998468B4BFB71A4A97A1EF706CECF37A6479D9E3CD0C6B1503ACFC8DFEAED2
11D70546BA618E646E08D52BF6F2F4C5E4F5872D28A20F04100B011DE98593A8109BEC
591E9153C2D32E34F4F3ADE8DDFFDBA5BC77B6F1930B4E29CE08DC59E3F<ETX><ETX>
Transmit: <ACK>
```

For additional information, please refer to FA_MTX_E2EE-V2.5.pdf

MX P2P for New and Existing Deployments

New Deployments

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

1. Retalix 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. Retalix 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	
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 Retalix 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)

Contact Information

Retalix Global Payments

85 Argonaut

Suite 150

Aliso Viejo CA, 92656

Tel: 949-614-1600

E-mail: ConnectedSupport@retalix.com

Web site: http://www.mtxeps.com/

NCR Corporation

NCR Corporation

Discovery Centre, 3 Fulton Road

Dundee, DD2 4SW

Scotland

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