Secure ECR

TECHNICAL SPECIFICATION

29 March 2011

PT Datindo Infonet Prima

Secure ECR

TECHNICAL SPECIFICATION

29 March 2011

PT Datindo Infonet Prima

CHANGE HISTORY

NO	DATE	REMARKS
1.	24 March 2011	Initial Release
2.	25 March 2011	Change data in Authorization Request Change Master Key (should have odd parity)
3.	29 March 2011	Change Message Format

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Background

The ECR feature is very useful for merchant who want to integrate the EDC to their POS. Some benefit such as single amount entry (no need to enter amount on two devices, only at POS), the result such as approval code, invoice number and card number are send back to POS. But there is sensitive data like card number, etc. How to secure those data? The Secure ECR is designed to secure the communication channel between EDC and POS. After implement the Secure ECR no more plain data in traffic.

1.2. Scope of Document

This document contains technical specification of Secure ECR until stated date.

1.3. Abbreaviations

ECR	Electronic Cash Register
EDC	Electronic Data Capture / Terminal
POS	Point Of Sale

2. SECURE ECR

2.1. Encryption

The Secure ECR use 3DES for encryption. The key length is 32 bytes (double length).

2.2. Process Flow

This section describe how the ECR Library interact with the EDC. This process should be transparant for developer.

2.2.1. Authentication

The Authentication process designed to get the session key to secure the communication channel between ECR Library and EDC. Please find the process flow as below:

- Library request Session Key by sending encrypted zeroes data using Master Key to EDC
- EDC decrypt it using Master Key to validate the session key request
- If valid, EDC generate random number as Session Key, encrypt it using Master Key and send to Library
- Library decrypt it using Master Key, now both have the same Session Key

2.2.2. ECR Transaction

The ECR Transaction should be performed after Authentication process success as the data in between should be enrypted using Session Key. Please find the process flow as below:

- Library encrypt ECR request data using Session Key and send to EDC
- EDC decrypt it using Session Key and process the ECR Transaction as usual
- After get response, the EDC encrypt ECR Response using Session Key and send to Library
- Library decrypt it and send the ECR Response back to application

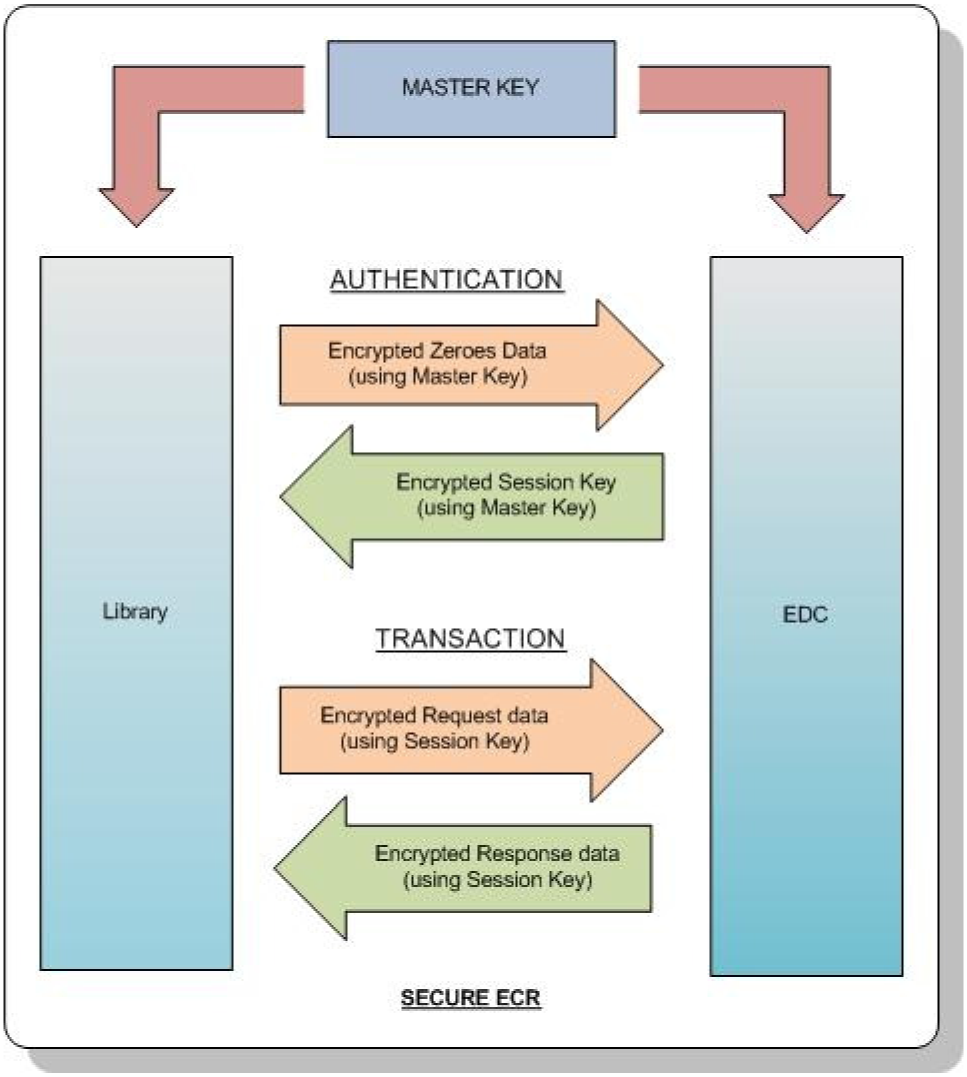
MASTER KEY
AUTHENTICATION
Encrypted Zeroes Data (using Master Key)
Encrypted Session Key (using Master Key)
Library
EDC
TRANSACTION
Encrypted Request data (using Session Key)
Encrypted Response data (using Session Key)
SECURE ECR

Figure 1. Process Flow

2.3. Message Format

The length of data should be multiple of 8 bytes, left justify, padding with 0xFF.

2.3.1. Authentication

Request

NO	FIELD	BYTES	COMMENTS
1	STX	1	
2	Length of packet	2	BCD. Value : 0x0024
3	Identifier of Secure ECR	4	'SECR'
4	Message Type	2	'00'
5	Length of Encrypted Data	2	BCD. Value : 0x0016

6	Encrypted Data	16	Encrypted zeroes data using Master Key. Example.
			Please replace the first byte and last byte of zeroes data with random value to ensure the result (encrypted data) is dynamic.
			Example:
			`23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 => data`
			`31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 => key`
			`35 78 71 D0 44 FD 58 7D 35 78 71 D0 44 FD 58 7D => encr`
			
			`16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 => data`
			`31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 => key`
			`9A DE 94 48 7E C6 71 A0 9A DE 94 48 7E C6 71 A0 => encr`

7	ETX	1	
8	LRC	1	

Response

NO	FIELD	BYTES	COMMENTS
1	STX	1	
2	Length of packet	2	BCD. Value : 0x0024
3	Identifier of Secure ECR	4	'SECR'
4	Message Type	2	'00'
5	Length of Encrypted data	2	BCD. Value : 0x0016
6	Encrypted Data	16	Encrypted Session Key (random number) using Master Key
7	ETX	1	
8	LRC	1	

2.3.2. ECR Transaction

Request

NO	FIELD	BYTES	COMMENTS
1	STX	1	
2	Length of packet	2	BCD
3	Identifier of Secure ECR	4	'SECR'
4	Message Type	2	'01'
5	Length of Encrypted Data	2	BCD
6	Encrypted Data	…9999	Encrypted ECR Request using Session Key
7	ETX	1	
8	LRC	1	

Response

NO	FIELD	BYTES	COMMENTS
1	STX	1	
2	Length of packet	2	BCD
3	Identifier of Secure ECR	4	‘SECR’
4	Message Type	2	‘01’
5	Length of Encrypted Data	2	BCD
6	Encrypted Data	…9999	Encrypted ECR Response using Session Key
7	ETX	1	
8	LRC	1	

LAMPIRAN A. MASTER KEY

The Master Key for Secure ECR as below:

```
6D 58 A2 BF F1 0E B3 4F E6 A1 F8 CD B3 C1 D5 BA
```