

Secure ECR

TECHNICAL SPECIFICATION

25 March 2011



PT Datindo Infonet Prima

Secure ECR

TECHNICAL SPECIFICATION

25 March 2011



PT Datindo Infonet Prima

COPYRIGHT © (2011) BY PT DATINDO INFONET PRIMA

All rights reserved. This material is confidential and proprietary to PT Datindo Infonet Prima and no part of this material should be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor should the material be disclosed to third parties without the express written authorization of PT Datindo Infonet Prima.

[illegible]

TABLE OF CONTENTS

1.	INTRODUCTION	1
1.1.	Background	1
1.2.	Scope of Document.....	1
1.3.	Abbreviations	1
2.	SECURE ECR	1
2.1.	Encryption.....	1
2.2.	Process Flow	1
2.3.	Message Format	3
	LAMPIRAN A. MASTER KEY	4

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. Abbreviations

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

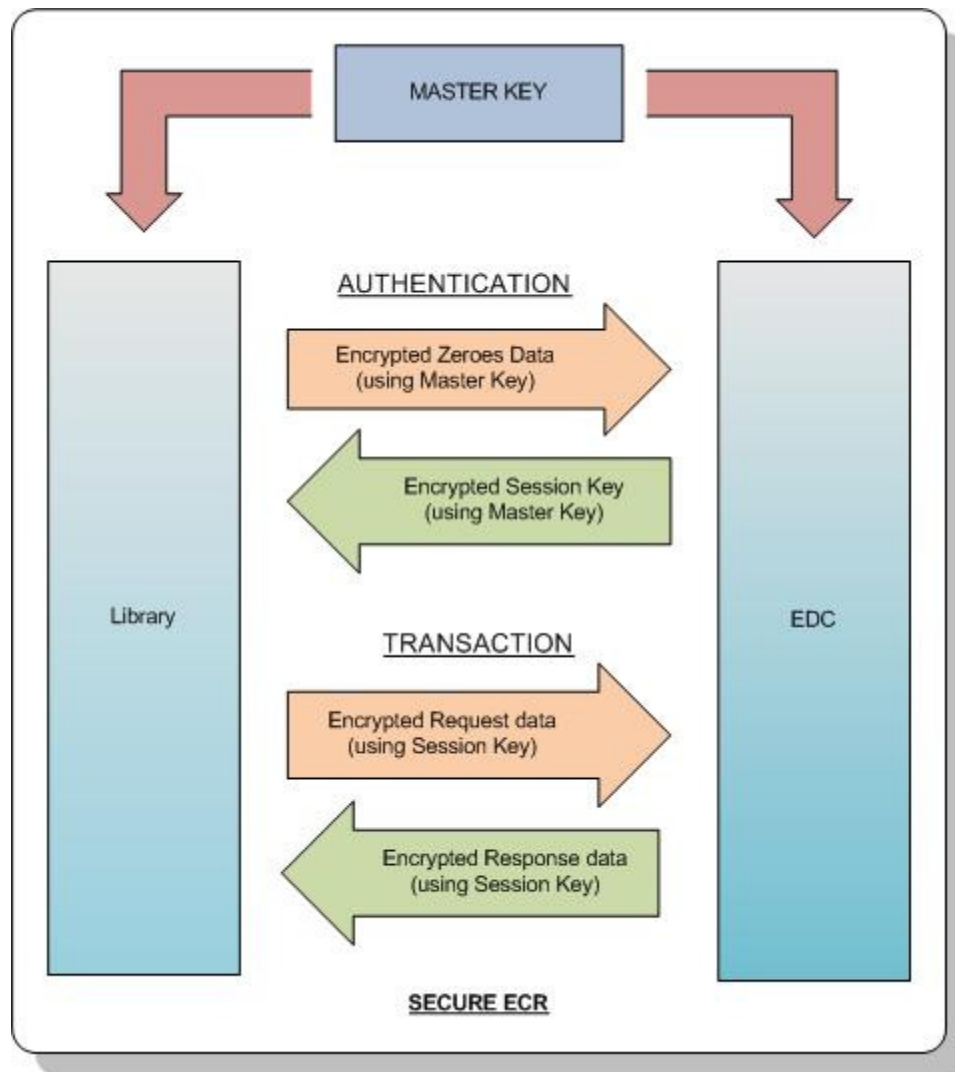


Figure 1. Process Flow

2.3. Message Format

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

2.3.1. Authentication

Request

NO	FIELD	BYTES	COMMENTS
1	Identifier of Secure ECR	4	'SECR'
2	Message Type	2	'00'
3	Length of Message Data	4	'0032'
4	Message Data	32	<p>Encrypted zeroes data using Master Key. Example.</p> <p>Please replace the first two digits and last two digits of zeroes data with random value to ensure the result (encrypted data) is dynamic. Example:</p> <pre> 23 00 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 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 </pre>

Response

NO	FIELD	BYTES	COMMENTS
1	Identifier of Secure ECR	4	'SECR'
2	Message Type	2	'00'
3	Length of Message Data	4	'0032'
4	Message Data	32	Encrypted Session Key (random number) using Master Key

2.3.2. ECR Transaction

Request

NO	FIELD	BYTES	COMMENTS
1	Identifier of Secure ECR	4	'SECR'
2	Message Type	2	'01'
3	Length of Message Data	4	
4	Message Data	...9999	Encrypted ECR Request using Session Key

Response

NO	FIELD	BYTES	COMMENTS
1	Identifier of Secure ECR	4	'SECR'
2	Message Type	2	'01'
3	Length of Message Data	4	
4	Message Data	...9999	Encrypted ECR Response using Session Key

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