CONTENTS

Encrypting PIN Pad

Chapter 10.5

Encrypting PIN Pad

DESCRIPTION

This chapter describes the Encrypting PIN Pad (EPP) used in Automated Teller Machines (ATMs). The EPP gives protection to the cardholder's Personal Identification Number (PIN) and of the keys used to verify and encrypt these PINs. The EPP can also be used to encrypt and decrypt any data sent to it by the application.

The main function of the EPP is to encrypt, immediately, numeric data entered at the keyboard of the ATM so that this data circulating within the ATM is securely encoded. This is done by locating the encrypting component in the keyboard.

Any attempt to disassemble the EPP will result in loss of all data within the security module.

There are three classes of EPP:

- 5807 - High Secure, EPP-E
- 5808 - Standard Secure, EPP-B
- 5809 - Standard Secure, EPP-E

The component parts of the EPP are as follows:

- EPP Keyboard Assembly
- Security Module
- SDC Interface Board.

EPP KEYBOARD ASSEMBLY

The EPP keyboard assembly is the body of the EPP, which includes the keyboard keys, switches and keyboard pcb. The keyboard pcb acts as an interface for power and data from the SDC interface to the security module and heater. The heater is populated on all keyboard variants.

SECURITY MODULE

There are two versions of the security module, High Security (class number 5807) and Standard Security (class numbers 5808 and 5809).

Every security module carries a unique serial number. To comply with security standards NCR must provide the serial numbers of new or replaced EPP assemblies to the owning institution. When a module is installed in an ATM, a sticker, showing the serial number, is placed next to the tracer plate. Once the ATM is installed module tracking becomes the responsibility of the owner of the terminal.

High Security Module

The high security module comprises an encryption pcb which is secured in a RED plastic housing.

Standard Security Module

The standard security module comprises an encryption pcb that is secured in a BLACK plastic housing.

Encryption pcb

The encryption pcb, for both high and standard security, performs all sensitive computations, stores the encryption codes and scans the PIN entry keyboard.

SDC INTERFACE BOARD

The SDC interface board provides the connection to the ATM serial communications bus, power input to the security module and an interface to the FDK and Front Operator Panel keyboards.

SECURITY

Security Levels

The EPP is available in one of two security levels, namely:

- Standard Security Level
- High Security Level.

Each level provides various anti-tamper sensors. Activating any sensor will render the security module inoperable and the whole EPP must be replaced. Removing the security module from the keyboard will activate a sensor and therefore should NOT be attempted.

AUDIT LED

Signal (LED_V) on the SDC interface board connector J4 goes high when the EPP is in secure key entry mode.

An optional LED can be fitted to indicate that the EPP is in secure key entry mode.

LEGACY VARIANTS

The EPP is available in two legacy variants, namely:

- BAPE/HI-BAPE - 5808
- EKC/EKCSM - 5807,5809

In legacy mode the EPP, Standard Security or High Security, is loaded with software that allows it to emulate a HI-BAPE, EKC or EKCSM.

Both BAPE/HI-BAPE and EKC/EKCSM emulation still adheres to the physical security constraints of the EPP module.

LEVEL 0 DIAGNOSTICS

Level 0 diagnostics is carried out on the EPP module following power up or device reset (refer to Chapter 4.2.6).

Diagnostic LEDs

There are four LEDs on the SDC interface board used for diagnostic reporting. After power up or system reset, the level 0 code performs diagnostic tests on the control board.

SERVICE

The EPP module is not a re-workable item. Any attempt to disassemble the module will result in the loss of all signals.

There are no serviceable parts and any failure will require replacement of the complete EPP assembly. In addition, if the security module is removed from the assembly, an alarm is triggered in the security module that will erase all cryptographic keys within it.

EPP ASSEMBLY REPLACEMENT

When unpacking a spare EPP assembly check for any signs of tampering. If tampering is suspected then do not install the assembly. A new tamper free assembly will be required and an investigation initiated to ascertain how tampering was achieved.

If the assembly is tamper free:

1. Check and record the serial number of the new assembly in the NCR work order system.
2. Locate the new serial number label.
3. Install the assembly.
4. Fit the new serial number label to the ATM next to the tracer plate.

Defective Assembly Disposal

When fitting a replacement EPP keyboard assembly ensure that the disposal of the defective assembly conforms to any agreed procedure between NCR and the customer.

If no specific agreed disposal procedure has been made with the customer then carry out the minimum action listed below:

1. Open the defective keyboard assembly and locate the security module.
2. Remove the security module and cut both of the wires from the battery to the module.
3. Dispose of the security module and keyboard assembly in accordance with your country's parts disposal policy.
4. Retain the SDC/F pcb if required for future re-use.

STRAPPING

None.

ADJUSTMENTS

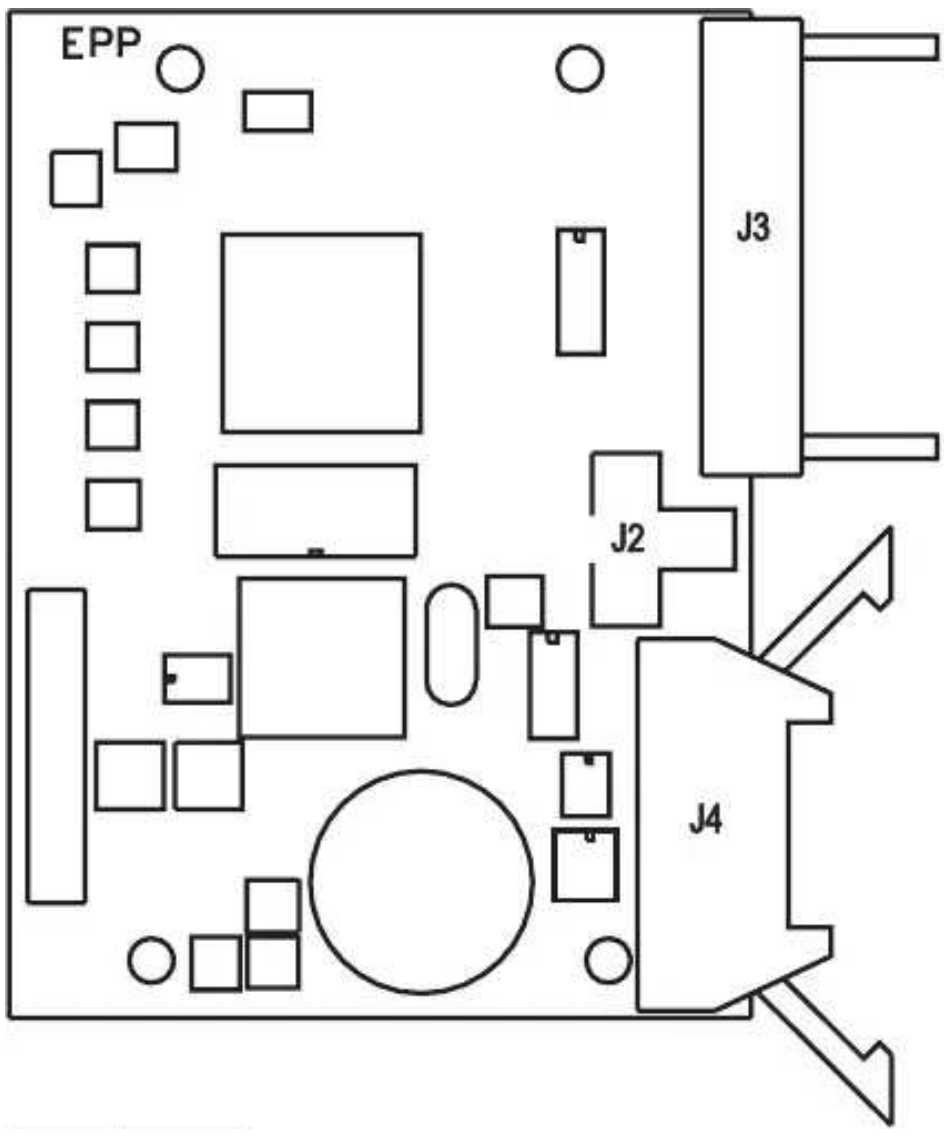
None

TEST TOOLS

None.

CONNECTORS

SDC INTERFACE BOARD



Heater Connector (J2)

The heater Connector (J2) is a 2-way connector with the following pinouts:

+24V	1	2	GND

SDC Connector (J3)

The SDC connector (J3) is a 10-way connector with the following pinout:

N/C	1	2	N/C
DATA_P	3	4	DATA_N
RESET_P	5	6	RESET_N
N/C	7	8	N/C
SDC_GND	9	10	N/C

Combined Power, FDK & FOP Connector (J4)

The combined power, FDK & FOP connector (J4) is a 26-way connector with the following pinout:

+5V	1	2	GND
SCAN_IN0b	3	4	N/C
AUDIT_LEDb	5	6	LEDV
N/C	7	8	N/C
FDK_LEFTb	9	10	FDK_RIGHTb
SCAN_IN0b	11	12	SCAN_FOP_IN1b
SCAN_FOP_IN2b	13	14	N/C
N/C	15	16	N/C
N/C	17	18	N/C
SCAN_OUT0b	19	20	SCAN_OUT1b
SCAN_OUT2b	21	22	SCAN_OUT3b
SCAN_OUT4b	23	24	SCAN_OUT5b
SCAN_OUT6b	25	26	SCAN_OUT7b