PINpad 1000SE

Reference and Programmers Guide

VeriFone Part Number 22903, Revision E

PINpad 1000SE Reference and Programmers Guide

Comments? Please e-mail all comments on this document to your local VeriFone Support Team.

WARNING

Do not dispose of the Li-ion smart battery in a fire. Li-ion batteries must be recycled or disposed of properly. Do not dispose of Li-ion batteries in municipal waste sites.

VeriFone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA

www.verifone.com

VeriFone Part Number 22903, Revision E

CONTENTS

CHAPTER 5 Management Packets

CHAPTER 6 Master/Session Message Packets

This guide is your primary source of information for setting up and installing PINpad 1000SE units.

Audience

This document is designed for merchant service representatives and programmers who need to develop and support PINpad 1000SE applications and install, set up, service, and support PINpad 1000SE.

Organization

This guide is organized with the following chapters:

Chapter 1, Introduction. Provides an overview of the PINpad 1000SE device.

Chapter 2, Setup. Explains set up and installation of the PINpad 1000SE unit. This chapter tells how to select a location for installing and operating the device.

Chapter 3, Using the Interface. Explains the operational features of the PINpad 1000SE unit and describes how to use the PINpad 1000SE keys.

Chapter 4, Programming Considerations. Outlines common developer considerations for communicating with the PINpad via the controller.

Chapter 5, Management Packets. Explains management message packets and formats that work in both Master/Session and Master/Session DUKPT modes. This section also includes a detailed explanation of interactive diagnostic functions.

Chapter 6, Master/Session Message Packets. Provides a detailed explanation of Master/Session message packets and formats.

Chapter 7, MAC Packets. Describes the master-session MAC generation of message preauthorization packets.

Chapter 8, DUKPT Message Packets. Provides a detailed explanation of DUKPT message packets and formats.

Chapter 9, Customizable Command Specification. Discusses PINpad 1000SE support of special prompt display, data entry programmability, and user definable characters.

Chapter 10, Communication Examples. Provides annotated examples of communication flow between the controller and the PINpad 1000SE.

Chapter 11, Troubleshooting and Service. Provides troubleshooting guidelines, should you encounter a problem in unit installation and configuration. This chapter also discusses cleaning and maintenance, as well as power requirements and dimensions for PINpad 1000SE units. It also provides information on contacting your local VeriFone representative or service provider, and information on how to order accessories or documentation from VeriFone.

This guide also contains appendices for Features and Specifications, Key Insertion, ASCII Table, Prompts and Error Messages, Built-In Prompt Tables, Prompt Table for Z2/Z3 Authentication, and Manual Diagnostic Procedures, as well as a Glossary.

Related Documentation

To learn more about the PINpad 1000SE unit, refer to the following set of documents:

- *PINpad 1000SE Certifications and Regulations*, VeriFone Part Number (VPN) - 22900
- *PINpad 1000SE Quick Installation Guide*, VPN - 22901
- *PINpad 1000SE Installation Guide*, VPN - 22902
- *PINpad 1000SE Stand Adapter Quick Installation Guide*, VPN - 22906

Guide Conventions

Various conventions are used to help you quickly identify special formatting. The following table describes these conventions and provides examples of their use.

Convention	Meaning	Example
Blue	Text in blue indicates terms that are cross referenced.	See Guide Conventions.
Italics	Italic typeface indicates book titles or emphasis.	You *must* not use this unit underwater.
`ScreenText - PRE`	ScreenText format is used while specifying onscreen text, such as text that you would enter at a command prompt, or to provide an URL.	`http://www.verifone.com`
	The pencil icon is used to highlight important information.	RS232-type devices do not work with the PINpad port.
	The caution symbol indicates hardware or software failure, or loss of data.	The unit is not waterproof and is intended for indoor use only.
	The lighting symbol is used as a warning when bodily injury might occur.	Due to risk of shock do not use the unit near water.

Introduction

This chapter provides a brief description of the PINpad 1000SE peripheral data entry device. The unit accepts personal identification numbers (PINs) and encrypts those numbers for security purposes. PINs are used during transactions to verify that a customer is authorized to use the offered card.

PINpad 1000SE Device Basics

The PINpad 1000SE unit delivers and expands upon the functionality of VeriFone's established PINpad 1000 and PINpad 101 families. This sleek and stylish PED-compliant handheld device incorporates a broad array of sophisticated security features to guard against fraud and abuse, including full support for 3DES encryption and a choice of Master/Session or Derived Key Per Transaction (DUKPT) key-management methods. The PINpad 1000SE also supports Message Authentication Code (MAC) to protect debit transaction data from accidental or fraudulent tampering during the transfer to its host.

Easily connecting with most existing POS terminals or ECRs, the PINpad 1000SE offers a fast, simple, and secure way to obtain PIN input for the expanding range of debit, electronic benefits transfer (EBT), and other PIN-based transactions.

Figure 1 The PINpad 1000SE peripheral data entry device

The PINpad 1000SE device connects to a controller, or master device, such as a TRANZ or OMNI transaction terminal, or other microcomputer-based system. The controller directs all PINpad device operations, including communication with the host computer.

Features and Benefits

VeriFone's PINpad 1000SE units provide the right combination of features and functions at the right price.

Sophisticated Security

- Certified as PED-compliant for secure solutions and meets ISO and ANSI standards for PIN encryption, key management, and Message Authentication Code (MAC)
- Supports the full range of 3DES security options, including 3DES Master/ Session keys and 3DES DUKPT
- Provides higher level of fraud protection against potential attempts to "crack" single DES keys and access secure data
- Provides mode for clear-text entry, to support fleet applications and others that do not require PIN entry

Ergonomics and Ease Of Use

- Includes large, hard-rubber keys for better tactile feedback to minimize errors and improved ease of use for consumers of all ages
- Occupies less counter space with a smaller design that fits comfortably in the palm of a hand for confidential data entry
- Includes programmable function keys that can be configured as "hot" keys for special tasks
- Includes an easy-to-read 8-character liquid-crystal display that automatically scrolls to display up to 16 characters, with support for multiple languages

Broad Supportability and Compatibility

- Ruggedly reliable to withstand the hard knocks of the point of sale environment
- Fully backward-compatible with VeriFone's PINpad 1000 and PINpad 101 legacy families
- Compatible with existing PINpad 1000 stands, and wall- or counter-mounting hardware
- Works with payment terminals, personal computers, and electronic cash registers (ECRs)

Setup

This chapter describes the unit setup procedure. You will learn how to:

- Select a location and protect the unit from adverse Environmental Factors. See Select Unit Location.
- Unpack the shipping carton. See Unpack Shipping Carton.
- Establish cable connections. See Connect PINpad.
- Secure the optional mount. See Mount Device (optional).
- Install the privacy shield. See Install Privacy Shield (optional).

Select Unit Location

Use the following guidelines described while selecting a location for your PINpad 1000SE unit.

Ease of Use

- Select a location convenient for both merchant and cardholder.
- Select a flat support surface, such as a counter top or table.
- Select a location near a power outlet and a telephone/modem line connection. For safety, do not string the power cable in a walkway or place across a walkway on the floor.

Environmental Factors

- Do not use the unit where there is high heat, dust, humidity, moisture, or caustic chemicals or oils.
- Keep the unit away from direct sunlight and anything that radiates heat, such as a stove or a motor.
- Do not use the unit outdoors.

The PINpad 1000SE device is not waterproof or dustproof, and is intended for indoor use only. Any damage to the unit from exposure to rain or dust may void any warranty.

Electrical Considerations

- Avoid using this product during electrical storms.
- Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, electric motors, neon signs, high-frequency or magnetic security devices, or computer equipment).
- Do not use the unit near water or in moist conditions.

Due to risk of shock or unit damage, do not use the unit near water, including a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.

Power and ESD Protection

The PINpad 1000SE device has been designed to meet or exceed reasonable standards for protection against power line transient noise and environmental electrostatic discharges (ESD). However, environments which exceed these standards can and do exist.

Noisy power, power disruptions (such as blackouts or brownouts), and environmental ESD may have detrimental effects on the operation of the PINpad 1000SE device. While not usually resulting in permanent damage to the unit, these environmental factors can result in corruption of PINpad 1000SE memory requiring reloading of keys, Custom Idle Prompt, etc.

To avoid such failures in the PINpad 1000SE unit when operating in electrically hostile environments, consider the use of surge suppressors, toroid noise filters, or uninterruptible power supplies (UPS). If in doubt, consult with VeriFone Technical Support for assistance.

Unpack Shipping Carton

Open the shipping carton and carefully inspect its contents for possible tampering or shipping damage. The PINpad 1000SE is a secure product and any tampering may cause the unit to cease to function properly.

1. Remove the PINpad 1000SE unit from the shipping carton.
2. Remove any protective plastic wrap and place the unit on a table or countertop.
3. Remove the clear protective film from the display.
4. Replace all the packing materials, close the lid, and save the carton for repacking or moving the PINpad 1000SE device in the future.

Do not use a unit that has been tampered with or otherwise damaged.

The PINpad 1000SE unit comes equipped with tamper-evident labels. If a label or component appears damaged, immediately notify the shipping company and your VeriFone representative or service provider immediately.

Connect PINpad

The PINpad 1000SE panel has a modular, four-wire interface port for power and communication connection to the controller.

CAUTION

Before connecting the PINpad 1000SE to a controller, remove the power cord from the back of the controller. Reconnect the power cord only *after* you are finished connecting the PINpad 1000SE.

Connecting to the Controller

Figure 2 illustrates how to connect the PINpad device to an OMNI 37xx Series terminal. For other terminal or controller connections, refer to the product's documentation.

1. Connect the modular plug on the PINpad cable to the modular jack on the rear of the PINpad 1000SE device.
2. Connect the other end of the cable to the PINpad port on the rear of the terminal.
3. Turn on or plug in power to the terminal.
4. When the PINpad 1000SE unit has power, the PINpad attempts to startup.

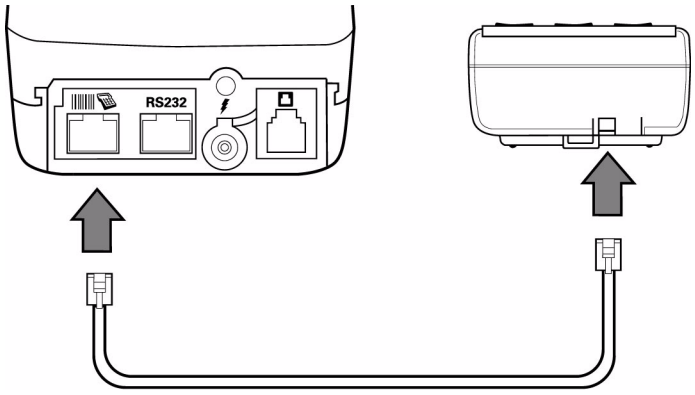


Figure 2 PINpad 1000SE Cable Connections

Connecting to a PC/AT (optional)

If the PINpad 1000SE is to be connected to an IBM PC/AT ® or compatible for general use, or the PC/AT will be running MKIXOR software for key insertion, a special cable product is available which provides power to the PINpad 1000SE device.

CAUTION

Using an incorrectly rated power supply may damage the unit or cause it not to work as specified. Before connecting, ensure that the power supply being used to power the unit matches the requirements specified at the back of the unit (see Accessories and Documentation for detailed power supply specifications). Obtain the appropriately rated power supply before continuing.

1. Connect the end of the cord with the DB25/DB9 connector to the PC/AT.
2. Connect the modular plug on the other end of the cable to the modular jack on the rear of the PINpad 1000SE device.
3. Plug the power supply cord into the socket at the base of the PC/AT connector.
4. Plug the PINpad/cable power supply into an AC wall outlet or surge protector.
5. Turn on or plug in the power to the PC/AT.
6. When the PINpad 1000SE unit has power, the PINpad attempts to startup.

WARNING

Do not plug the power pack into an outdoor outlet or operate the unit outdoors.

NOTE

To protect against possible damage caused by lightning strikes and electrical surges, consider installing a power surge protector.

Figure 3 illustrates how to connect the PINpad 1000SE to a PC or AT.

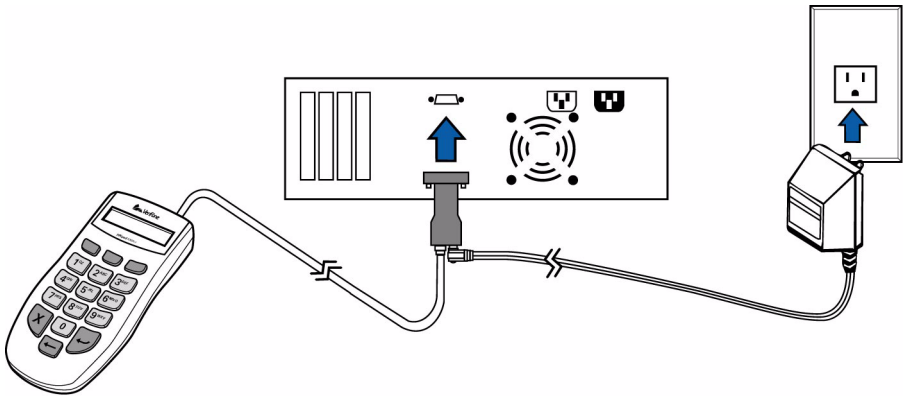


Figure 3 PINpad Device to PC/AT Cable Connection

Mount Device (optional)

The optional stand adapter holds the PINpad 1000SE unit securely to a countertop or a wall. The unit can be removed from the stand adapter anytime for hand-held operation.

Mounting the Adapter

Figure 4 shows how to install a stand adapter onto a pre-existing flat mounting plate.

1. Select a location for the stand adapter on a smooth wall or countertop. Be sure the cable can easily reach the controller from this position without stretching.

2 Position the keyholes on the molded cradle over the slotted screws on mounting plate. Slide the adapter downward until the screws are in the narrow ends of the keyholes. If necessary, loosen the screws slightly until the cradle slides easily.

3 Tighten the slotted screws to secure the cradle to the angled bracket.

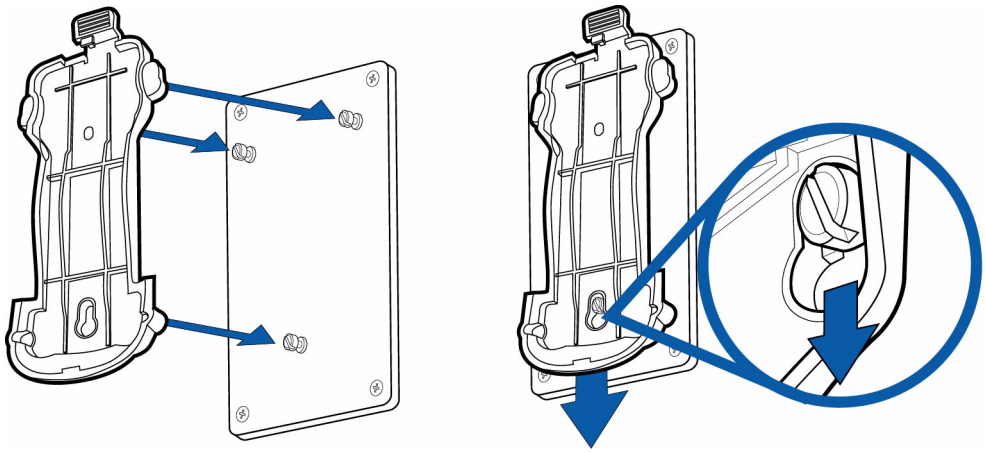


Figure 4 Stand Adapter Installation

The stand adapter may also be screwed directly to a wall or countertop. Use screw anchors when fastening the adapter to a cement or brick wall. When fastening the plate to drywall, the screws must go into the studs behind the wall. Screw anchors alone will not safely hold the adapter to drywall. If you do not want to make holes in a countertop, use double-faced tape to secure the stand adapter.

Using the Stand Adapter

Figure 5 shows how to insert a PINpad 1000SE unit into a stand adapter. Slide the end of the PINpad 1000SE unit into the bottom of the stand adapter, then press the screen end of the PINpad 1000SE unit firmly into the top of the stand adapter until you hear and feel the release lever click.

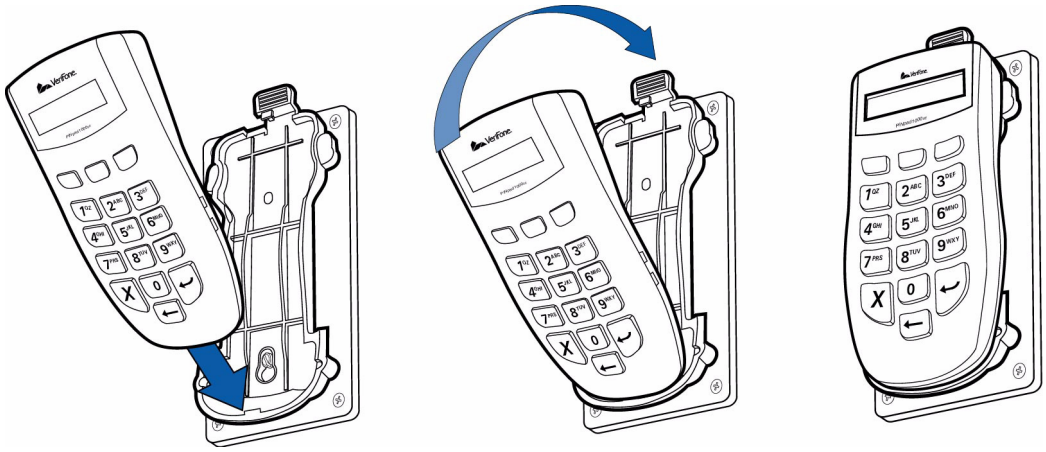


Figure 5 Inserting the PINpad 1000SE device into the Stand Adapter

Removal is simply the reverse: press the release lever at the top of the stand adapter and pull the PINpad 1000SE unit up and out of the stand adapter.

Install Privacy Shield (optional)

Figure 6 shows an example of an installed privacy shield.

Figure 6 Installed Privacy Shield

Using the Interface

The PINpad 1000SE interface includes:

- Eight-character display. See Display.
- 3 programmable function keys. See Programmable Function (PF) Keys.
- 10-key telco-style keypad. See Keypad.
- 3 color-coded function keys. See Function Keys.

Figure 7 illustrates the basic features:

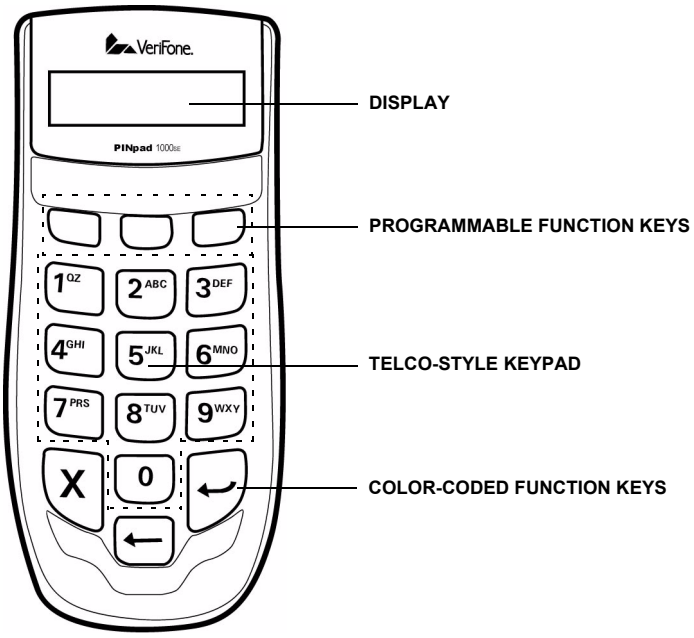


Figure 7 PINpad 1000SE Features

Display

The eight-character liquid crystal display shows up to 16 characters through automatic scrolling. The PINpad 1000SE device displays fully-formed numerals, letters and special characters * and #. Information displayed includes characters entered from the keypad, instructions, prompts and error messages.

Programmable Function (PF) Keys

The row of PF keys directly above the keypad from left-to-right are referred to as PF1, PF2, and PF3. These keys can be assigned application-specific functions. Because such functions are often unique and can vary greatly between applications, they are not discussed in this manual.

Keypad

The PINpad 1000SE unit has 10 keys that includes numerals 0 through 9, and can be used to enter letters A through Z. The ten keypad keys can be used for PIN and data entry and manual diagnostics.

Function Keys

The context of the controller and PINpad combine to determine the specific action performed when you press one of the following function keys. The following descriptions provide general characteristics of these function keys.

Cancel Key

Pressing the cancel key usually has the same effect as pressing the Esc (escape) key on a PC. That is, it terminates the current function or operation.

Backspace Key

The backspace key is commonly used to delete a number, letter, or symbol on the display screen. Press backspace one time to delete the last character typed on a line. To delete additional characters, moving from right to left, press backspace once for each character or hold down backspace to delete all characters on a line.

Enter Key

The enter key is generally used the same as the enter key on a PC, that is, to end a procedure, confirm a value or entry, answer “Yes” to a query, or select a displayed option.

CHAPTER 4

Programming Considerations

Since the PINpad is a peripheral device, its normal operations and diagnostics are determined by the application code that resides in the connected controller. The controller must be programmed with the necessary message packets (or "commands") that the PINpad can interpret.

When planning the application program, consider the following decisions:

- What type of key management is required: DUKPT, Master Session, or both?
- What prompts and commands are used for customer PIN entry?
- What type of prompts are used? Standard or custom prompts?
- What languages must be supported?
- Is the card information entered from the PINpad keypad, the controller cardreader, the controller keypad, or some combination of these?
- What is the controlling device communication baud rate?

Data Entry Events

The sequence of events can vary:

- The card data can be entered before or after the retailer enters the transaction amount.
- The PIN can be entered before or after the retailer enters the transaction amount.
- The transaction can be canceled at nearly any time.
- The controller can solicit single key entries or entire sequences, and what it does can affect consumer use of the CLEAR key, which acts as a backspace key.

The entry sources can also vary:

- The retailer can slide the consumer card through the slot on the controller.
- The retailer can enter the card data on the controller keypad.

PIN Requirements

PIN entry may or may not be required. The PIN requirement may be indicated by:

- Account number falling within the range on the account table
- Retailer entering a keystroke sequence at the controller, causing the PIN request

Display Possibilities

The PINpad offers flexible display capabilities:

- While idle, the display can show the default prompts, or your own custom messages.
- The messages displayed can rotate.

The controller can direct the PINpad 1000SE device to:

- Display a single message
- Display rotating messages in 3 second intervals
- Request a single key entry from the customer
- Request a key entry sequence from the customer and echo the entry on the display
- Request the PIN entry from the customer, encrypt the PIN, create the PIN block and echo the customer display as asterisks

DUKPT and Master/Session Key Management

The PINpad 1000SE device supports both the DUKPT (Derived Unique Key Per Transaction) and Master/Session methods of key management. Though the message packet format requirements for DUKPT and Master/Session are similar, some command types have different formats. In addition, there are several packet types specific to DUKPT that are not supported when the PINpad 1000SE is set as a Master/Session PINpad (and vice versa).

To simplify the programming of the PINpad 1000SE unit, the message packet format requirements have been divided into several sections in this manual. The following few sections detail the packet-level messages, divided for discussion into the following groups:

- Management Packets
- Master/Session Message Packets
- MAC Packets
- DUKPT Message Packets
- Customizable Command Specification

Many of the definitions, structures, and behaviors are the same across these general groups of packets, and these general attributes are discussed in the following sections.

- Preauthorization packets
- Key loading device to PINpad packets

Control Character Definitions

In addition to accepting specific messages to manipulate operations, the PINpad message packets include the following abbreviations and special characters:

Abbrev.	Hex Value	Description
STX	02h	Start of Text
ETX	03h	End of Text
SI	0Fh	Shift In
SO	0Eh	Shift Out
EOT	04h	End of Transmission
ACK	06h	Acknowledge
NAK	15h	Negative Acknowledge
FS	1Ch	Field Separator
LRC		Longitudinal Redundancy Check
SUB	1Ah	Message Parameter

Packet Structures

The PINpad accepts two types of message packets:

- `<STX> data <ETX>{LRC}`
- `<SI> data <SO>{LRC}`

Any other type of packet will be ignored by the PINpad.

NOTE

Full compliance with the packet protocol is described herein, including all ACK/NAK/EOT dialogue required in order to guarantee proper performance.

Receiving a NAK

If during a communication session either the PINpad or controller receives a NAK, it retransmits its last message and increments a NAK counter for the communication session. If more than three NAKs occur while attempting to transmit the same item, the transmitting unit sends an EOT, terminating communication.

Receiving an ACK

When the PINpad receives an ACK, it means the packet was received without error. If the PINpad is receiving an ACK and does not expect it, the ACK is ignored. Likewise, when the PINpad receives a command from the controller without error, it transmits an ACK.

Receiving an EOT

If during a communication session the PINpad receives an EOT, it means to terminate the communication session and returns to the idle state. If the PINpad is receiving and EOT and does not expect it, the EOT is ignored.

Timeout

During a communication session, the PINpad device or the controller times out if it does not receive the expected response within 15 seconds. The unit sends an EOT to terminate the communication session.

Numerical Listing of Messages

The following section provides a detailed numerical listing of the message packets used to control the PINpad device. Each message includes:

- **purpose** – a brief definition of the message
- **category** – the functional type of message (e.g., whether its a diagnostic or communication packet)
- **comments** – any additional information, including the maximum and minimum character length of the message packet and any timing considerations for programming the PINpad
- **message packet** – a sample of the message packet, showing both the request and response packets when applicable
- **elements** of the message packet – including the field type, character length and brief description of each packet element
- **examples** of how the message packet can be used
- **protocol** – including the transmission sequence and direction of the communication between the controller and the PINpad unit

Management Packets

Some packets and formats work both in Master/Session mode and Master/Session DUKPT mode; VeriFone refers to these as management packets.

Functional Listing of PINpad Device Messages

The messages sent to and from the PINpad device to manipulate operations or control specific PINpad functions are divided into three functional groups. These groups include packets for interactive diagnostic tests, and standard and custom communication.

Interactive Diagnostic Test

Interactive tests between the PINpad unit and the controller run only upon request. These tests use the VeriFone-defined message Packets 01-15, and can be run during the same session that you load master keys, use the MKI module or on request from the PINpad controller.

Message	Description
M01	M01 Set PINpad Mode
M02	M02 Check PINpad Mode
M03	M03 Load Permanent Unit Serial Number
M04	M04 Read Permanent Unit Serial Number
01	01 Run Diagnostic Function Routine
05	05 Transfer Serial Number
06	06 Request Serial Number
07	07 DES Reliability Test
09	09 UART Loopback Test
10	10 Request Unencrypted PIN
11	11 PINpad Device Connection Test
12	12 Select Prompt Language
13	13 Set Baud Rate
15	15 Refresh PINpad Key Management Mode
17	17 Set Key Management Mode
18	18 Check Key Management Options Register Mode

Standard Communication

The standard messages sent between the PINpad device and the controller follow the VISA message packet format and allow the PINpad unit to be programmed with standard VISA prompts and control the PINpad display. There is sufficient variation in Packets 70 and 71 to merit specific discussions in both the Master/Session Message Packets and DUKPT Message Packets chapters.

Message	Description
72	72 Cancel Session Request

Custom Communication

These message packets were created to provide the PINpad device with special prompts and data entry requirements for custom applications. The request and response messages pass between the controller and the PINpad, allowing the controller to customize prompts and control PINpad operations. There is sufficient variation in Packets Z60 and Z62 to merit specific discussions in both the Master/Session Message Packets and DUKPT Message Packets chapters.

Message	Description
Q2	Q2 Indicate Host Done
Q5	Q5 Alternate PROCESSING Prompt
Z1	Z1 Return to Idle State
Z2	Z2 Display a String
	MACed Z2 Display a String
Z3	Z3 Display Rotating Messages
	MACed Z3 Display Rotating Messages
Z7	Z7 Turn on/off CANCEL REQUESTED
Z8	Z8 Reset/Set Idle Prompt
Z10	Z10 Load Prompt Table
Z40	Z40 Request Key Code
Z41	Z41 Return Key Code
Z42	Z42 Request Key Value
Z43	Z43 Return Key Value
Z50	Z50 Request String Input
Z51	Z51 Return String Input

M01 Set PINpad Mode

Sets or clears a number of control-switches in the PINpad Mode Register.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

Once PINpad 1000SE mode is set, it CANNOT be changed to another mode. This means that Packet M01 is ignored when the PINpad is in PINpad 1000SE mode. After setting the PINpad mode, use M02 Check PINpad Mode to make sure the PINpad is in the correct mode.

VeriFone recommends that the reserved field be set to zero.

Any request PINpad mode setting outside the specified option is ignored.

Setting the PINpad mode should be carried out in an environment, where the power level can be guaranteed. There is no Power Failure Protection in Packet M01 processing.

For PINpad Mode Register values, see the following table:

Table 1 PINpad Mode Register Values

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
PP1000 mode: Default	- - - - - - - - - -		Reserved		- - - - - - - - - -	0	0	1
PP1000SE mode	- - - - - - - - - -		Reserved		- - - - - - - - - -	0	1	0

Packet Format

```
<SI> M01 [PM] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M01	packet	3	Set PINpad Mode
[PM]	packet parameter	2	The two ASCII-Hex digits are concatenated, big-endian, to produce a single control byte. See the PINpad Mode Register Values table, above, for values.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 8 characters, minimum 8 characters			

Examples

```
<SI>M0101<SO>{LRC}
```

Sets the PINpad to PP1000 mode.

```
<SI>M0102<SO>{LRC}
```

Sets the PINpad to PINpad 1000SE mode, which meets PED requirement.

Protocol

Controller	Transmission Direction	PINpad
M01 packet	------>	
		ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	M01 packet echo
ACK = LRC OK and key management echo OK NAK = LRC incorrect (EOT after 3 NAKs) EOT = LRC OK and key management echo NOT OK	------>	
	<------	EOT to terminate process (PINpad saves new mode)

PINpad Mode Management Rules

1. 1. PP1000 is the Factory Default (PP1000 Tech Spec 06127 functionality plus 3DES)
   - Defaults:
   - Working zero key support ON (may be turned OFF with packet 17 - KMM Bit 4)
   - Z66 MAC - Working key optional
   - Allow multiple keyloading sessions. Do not erase keys if PINpad is in new keyloading session.
   - When switching between MS and DUKPT modes – Do Not erase keys.

2 PP1000SE mode (PP1000 Tech Spec 06127 functionality plus 3DES with the following changes)

- Once PP1000se Mode is set, it CANNOT be changed
- Defaults:
  - Working zero key support OFF (CANNOT be turned on with packet 17 - KMM Bit 4)
  - Packet 17 – KMM Bit 5 cannot be set – Zero GISKE session key support
  - Packet 17 – KMM Bit 6 cannot be set – Initialize RAM
  - Z66 MAC - Working key NOT optional
  - When switching between MS and DUKPT modes – Erase Keys
  - Do not allow multiple clear keyloading sessions.

If KLK NOT loaded	All Master and DUKPT keys are erased at the start of a keyloading session, when loading Master or DUKPT keys.
KLK loaded	All Master and DUKPT keys are erased at the start of a keyloading session, when loading Master or DUKPT keys. Except, if all keys loaded are Master keys, encrypted with the KLK, no keys will be erased.
When the KLK is loaded in the clear, all Master and DUKPT keys are erased.	

- Supports all of the PP1000 packets except the following (Removed to meet PED Spec):

PED is only applicable to PP1000SE)

- 10 - Request Unencrypted PIN
- The following packets are supported with limitations (see prompt rule summary in chapter 9) in version 4E3002E and later releases of the firmware.
- Z40 - Accept a Key, Request Key Code
- Z41 - Return Key Code
- Z42 - Accept a Key, Request Key Code
- Z43 - Return Key Code
- Z50 - Request String Input
- Z51 - Return String Input

- Master Session PIN encryptions are limited to 4 within 120 seconds. If a 5th PIN encryption is attempted within the 120 seconds, the PINpad will prompt with a message 'PLS WAIT' until the 120 second timer has expired and then continue with the encryption.

3. If the PINpad mode is changed all keys are erased:
   - KLK erased
   - All Master Keys erased
   - All DUKPT Keys erased
   - See defaults in 2a above
   - 1 DES mode for MS and all DUKPT engines
   - DUAL Mode (MASTER+DUKPT)
4. Power On Display
   - At power on,
   - In PP1000 mode, the unit will display: PP1000 TDES 4E300xx MM/YY
   - In PP1000se mode, the unit will display: PP1000SE TDES PED CERTIFIED 4E300xx MM/YY
5. Display Mode, FW Version and FW Date
   - Pressing the cancel key (RED) immediately followed by the ‘1’ key will display the following until the cancel key (RED) is pressed or a packet is received.
   - In PP1000 mode, the unit will display: PP1000 TDES 4E300xx MM/YY
   - In PP1000se mode, the unit will display: PP1000SE TDES PED CERTIFIED 4E300xx MM/YY.

M02 Check PINpad Mode

Causes the PINpad unit to check the PINpad mode.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

For PINpad Mode Register values, see the following table:

Table 2 PINpad Mode Register Values

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
PP1000 mode: Default	- - - - - - - - - -		Reserved		- - - - - - - - - -	0	0	1
PP1000SE mode	- - - - - - - - - -		Reserved		- - - - - - - - - -	0	1	0

Request Format

```
<SI> M02 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M02	packet	3	Check PINpad Mode
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Response Format

```
<SI> M02 [PM] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M02	packet	3	Check PINpad Mode
[PM]	packet parameter	2	The two ASCII-Hex digits are concatenated, big-endian, to produce a single control byte. See the PINpad Mode Register Values, above, for values.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 8 characters, minimum 8 characters			

Protocol

Controller	Transmission Direction	PINpad
M02 request packet	------>	
		ACK = LRC OK
		NAK = LRC incorrect
	<------	(EOT after 3 NAKs)
	<------	M02 response packet
ACK = LRC OK		
NAK = LRC incorrect		
(EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

M03 Load Permanent Unit Serial Number

Loads the permanent unit serial number (PUSN).

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

The default PUSN is all zeros '0' (0x30).

NOTE

This packet is only available in version 4E3002x and later releases of the firmware.

Once the serial number is loaded it cannot be erased or changed. Subsequent M03 requests are ignored and return an error code.

CAUTION

There is no Power Failure Protection in Packet M03 processing.

Load PUSN only in an environment where the power level can be guaranteed.

Both the request and response formats are shown below.

Request Format

```
<SI> M03 [PUSN] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M03	packet	3	Load PUSN
[PUSN]	packet	11	Permanent Unit Serial Number Format: xxx-xxx-xxx **Note:** PUSN has input range from '0' ~ '9', 'A' ~ 'Z' and '-'. Location and number of '-'are not restricted or limited.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 17 characters, minimum 17 characters

Response Format

```
<SI> M03 [r] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M03	packet	3	Load PUSN
[r]	packet parameter	1	Response Code; • 0=no error • 1=PUSN format error, input is outside the range of '0' ~ '1', 'A' ~ 'B', or '-'. • 2=PUSN is already loaded, and the M03 request is ignored.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 7 characters, minimum 7 characters			

Protocol

Controller	Transmission Direction	PINpad
M03 request packet	------>	
		ACK = LRC OK
		NAK = LRC incorrect
	<------	(EOT after 3 NAKs)
	<------	M03 response packet
ACK = LRC OK		
NAK = LRC incorrect		
(EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

M04 Read Permanent Unit Serial Number

Checks the permanent unit serial number (PUSN).

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

Both the request and response formats are shown below.

This packet is only available in version 4E3002x and later releases of the firmware.

Request Format

```
<SI> M04 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M04	packet	3	Check PUSN
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Response Format

```
<SI> M04 [PUSN] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
M04	packet	3	Check PUSN
[PUSN]	packet parameter	11	Permanent Unit Serial Number Format: xxx-xxx-xxx
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 17 characters, minimum 17 characters			

Protocol

Controller	Transmission Direction	PINpad
M04 request packet	------>	
		ACK = LRC OK
		NAK = LRC incorrect
	<------	(EOT after 3 NAKs)
	<------	M04 response packet
ACK = LRC OK		
NAK = LRC incorrect		
(EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

01 Run Diagnostic Function Routine

Causes the PINpad unit to run self-diagnostic functions and send information to the master device.

Category Interactive Diagnostic Test

Comments The response packets to Packet 01 are packet 09 UART Loopback Test and Response Packet 14.

This test is initiated by the controller. The PINpad displays the response to this diagnostic test.

The table of two-byte ASCII code for diagnostic testing is as follows:

Diagnostic #	Description	PP1000 and PP1000SE modes
00	Change Proc Msg	Yes
01	RAM Test/One time	Yes
02	RAM Test/Continuous	Yes
03	PROM Checksum Test	Yes
04	Keyboard Test	Keyboard Test
05	Display Test	Display Test
06	Serial Number Check	Yes
07	UART Loopback Test	Yes
08	Current BAUD Rate	Yes
----	----	----
----	----	----
----	----	----
12	RAM Test/One Time	Yes
13	RAM Test/Continuous	Yes
14	PROM Checksum Test	Yes
15	PINpad ROM Version #	Yes

Packet Format

```
<SI> 01 [diagnostic#] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
01	packet type	2	Interactive Diagnostic Routine
[diagnostic#]	packet parameter	2	Two-byte ASCII code for the diagnostic test to run; Range: 00-09 (See the preceding table)
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'

Type	Field	Length	Description
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 7 characters, minimum 7 characters			

Examples

```
<SI> 0101 <SO>{LRC}
```

This packet sends the PINpad the request to run diagnostic test 1, the one-time RAM test.

```
<SI> 0106 <SO>{LRC}
```

This packet sends the PINpad device a request to run diagnostic test 6, which displays the serial number.

Protocol

This protocol is used with diagnostic numbers 01 through 06, as well as 08.

Diagnostic Numbers 01-06 and 08

The following is the protocol for options 01-06 and 08.

Controller	Transmission Direction	PINpad
01 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		PINpad executes test
	<------	EOT when test finished

UART Loopback Test (07)

The following is the protocol for option 07, the UART Loopback Test option.

Controller	Transmission Direction	PINpad
	<------	09 request packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
09 response packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	09 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT when test finished

12 RAM Test/One Time

The following is the protocol for option 12.

Controller	Transmission Direction	PINpad
01 packet: `<SI>0101<SO>{LRC}`	------>	
	<------	ACK = LRC OK NAK = LRC incorrect
	<------	14 response packet: `<SI>14RAM TST BEGIN<SO>{LRC}`
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	14 response packet: `<SI>14RAM TST OK<SO>{LRC}` or `<SI>14BAD RAM<SO>{LRC}`
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

13 RAM Test/Continuous

The following is the protocol for option 13.

Controller	Transmission Direction	PINpad
01 packet: `<SI>0102<SO>{LRC}`	------>	
	<------	ACK = LRC OK NAK = LRC incorrect
	<------	14 response packet: `<SI>14RAM TST BEGIN<SO>{LRC}`
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	14 response packet: `<SI>14RAM TST OK<SO>{LRC}` or `<SI>14BAD RAM<SO>{LRC}`
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

14 PROM Checksum Test

The following is the protocol for option 12.

Controller	Transmission Direction	PINpad
01 packet: `<SI>0103<SO>{LRC}`	------>	
	<------	ACK = LRC OK NAK = LRC incorrect
	<------	14 response packet: `<SI>14xx<SO>{LRC}`
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

NOTE

In the preceding table, xx is the one-byte PROM internal checksum. There are two checksums inside the PINpad 1000SE. One is the PROM checksum, used for manufacturing purposes, which is 2 bytes long and located at 3FFE/3FFF. The other one is the PROM internal checksum.

05 Transfer Serial Number

Transfers the internal serial number from the controller or master device to the PINpad.

NOTE

This message overwrites any number already stored as the serial number.

Category Interactive Diagnostic Test

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments Use the Serial Number Check, Message 06, to check the internally-stored serial number before using Message 05 to assign one.

Packet Format

```
<SI> 05 [serial number]     packet parameter     16     Serial Number
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
05	packet type	2	Transfer Serial Number
[serial number]	packet parameter	16	Serial Number
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 21 characters, minimum 21 characters			

Example

```
<SI> 00000123-456-789 <SO>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
05 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
	<------	05 packet echo

Controller	Transmission Direction	PINpad
ACK = LRC OK	------>	
NAK = LRC incorrect, PINpad stores serial number		
(EOT after 3 NAKs)		
		PINpad stores serial number
	<------	EOT

06 Request Serial Number

Directs the PINpad device to transmit its internal serial number to the controller or master device.

Category Interactive Diagnostic Test

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments The controller uses this packet to request that the PINpad send its serial number. If the PINpad does not have its serial number stored, it transmits a hex ASCII string that translates to 16 bytes of zeros (0). See 05 Transfer Serial Number to assign the internal serial number.

Both the request and response formats are shown below.

Request Format

```
<SI> 06 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
06	packet type	2	Request Serial Number
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Response Format

```
<SI> 06 [serial number]     packet parameter     16     Serial Number
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
06	packet type	2	Request Serial Number
[serial number]	packet parameter	16	Serial Number
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 21 characters, minimum 21 characters			

Example

```
<SI> 00000123-456-789 <SO>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
06 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	06 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT

07 DES Reliability Test

Tests PINpad encryption function forward and backward with master key, a cleartext, and a known ciphertext.

Category Interactive Diagnostic Test

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments This packet consists of a master key, a cleartext, and a known ciphertext. Upon receipt of this packet, the PINpad encrypts the cleartext using the master key and compares the encrypted result with the known ciphertext. If the comparison is good, PINpad will decrypt the known ciphertext using the same master key and compare the decrypted result with the cleartext. The DES test is considered reliable only after both comparisons are valid. The PINpad displays the result of the test.

Packet Format

```
<SI> 07 [kkkkkkkkkkkkkkk] [ddddddddddddddd] [ccccccccccccccc] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
07	packet type	2	DES Reliability Test
[kkkkkkkkkkkkkkk]	packet parameter	16	master key
[ddddddddddddddd]	packet parameter	16	cleartext
[ccccccccccccccc]	packet parameter	16	known ciphertext of [ddddddddddddddd] encrypted by [kkkkkkkkkkkkkkk]
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 53 characters, minimum 53 characters

Examples

```
<SI>071234567890ABCDEF1111222233334444555566667777888<SO>{LRC}
```

This request packet tells the PINpad device to run the DES reliability test with the provided master key, cleartext, and known ciphertext.

Protocol

Controller	Transmission Direction	PINpad
07 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
	<------	EOT

09 UART Loopback Test

Verifies that the receiver and transmitter circuitries and the UART codes are functioning correctly.

Category Interactive Diagnostic Test

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments Either the controller or PINpad device may initiate this test. The PINpad unit displays the test results. The response packet of 01 Run Diagnostic Function Routine contains packet 09 UART Loopback Test as well.

Request Format

```
<SI> 09 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
09	packet type	2	UART Loopback Test ?
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Response Format

```
<SI> 09 <SUB>PROCESSING <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
09	packet type	2	UART Loopback Test
<sub>	packet parameter	1	ASCII Substitute Character; Value: 1Ah
PROCESSING	packet parameter	10	Display ASCII Text: PROCESSING
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 16 characters, minimum 16 characters			

Examples

```
<SI> 09 <SO>{LRC}
```

This request packet tells the PINpad device to run the UART loopback test.

```
<SI> 09 <SUB>PROCESSING <SO>{LRC}
```

This response packet is used for comparison by the controller/PINpad unit.

Protocol

Controller	Transmission Direction	PINpad
09 request packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	09 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
09 response	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	EOT

10 Request Unencrypted PIN

Causes the PINpad unit to request PIN number entry by the customer.

Support Mode

PINpad 1000	PINpad 1000SE
✔	

Comments

Upon receipt of this packet from the master device, the PINpad requests a PIN number from the customer and returns the unencrypted PIN number to the master device.

NOTE

This packet is disabled in DUKPT-only mode.

Both the request and response formats are shown below.

Request Format

```
<SI> 10 [aaaaa.aa] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
10	packet type	2	Request Unencrypted PIN
[aaaaaaa]	packet type	3-7	Amount of purchase with implicit decimal point
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 12 characters, minimum 8 characters			

Response Format

```
<STX> 10 [bb] [ff] [ppppppppppp] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
10	packet type	4	Request Unencrypted PIN
[bb]	packet parameter	2	length of PIN; Range: 4-12
[ff]	packet parameter	2	01 flag
[ppppppppppp]	packet parameter	4-12	PIN number
<ETX>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'

Type	Field	Length	Description
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 23 characters, minimum 15 characters			

Examples

```
<SI> 10 1.00 <SO>{LRC}
```

This request packet sends the PINpad a request for customer PIN entry and sends a transaction amount of $1.00.

```
<STX> 71.0 04 01 1234 <ETX>{LRC}
```

This return packet and specifies that the PIN has 04 characters, an 01 flag, and a PIN of 1234.

Protocol

Controller	Transmission Direction	PINpad
10 request packet	------>	
		ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
		PINpad displays message requesting PIN entry
	<------	User enters PIN
	<------	10 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT test complete

11 PINpad Device Connection Test

Checks the communications/connection between the controller and the PINpad device.

Category Interactive Diagnostic Tests

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments If the connection is okay, the controller receives an ACK (acknowledgment) from the PINpad within a second. If the controller does not receive the ACK within a second, it assumes the PINpad unit is not attached.

Packet Format

```
<SI> 11 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
11	packet type	2	PINpad Connection Test
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Example

```
<SI> 11 <SO>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
11 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect

12 Select Prompt Language

Selects the language used for the prompts.

Category Interactive Diagnostic Test

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments The controller uses this packet to select the prompt language. There are two different languages from which to choose. Languages are selected from one of the listed single digit codes.

NOTE

Current firmware only supports English and Spanish prompts.

Packet Format `<SI> 12 [language code] <SO>{LRC}`

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
12	packet type	2	Select Language code
[language code]	packet parameter	1	Language control Selection; • 1 = English • 2 = Spanish **Note:** Any value besides 1 or 2 will result in no change, and the PINpad device will send out an <EOT>.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 6 characters, minimum 6 characters

Example `<SI> 122 <SO>{LRC}`

This example selects the Spanish language prompts (code = 2)

Protocol

Controller	Transmission Direction	PINpad
12 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect PINpad displays in selected prompt language.

13 Set Baud Rate

The master device uses this packet to set the baud rate for RS232 communication with the PINpad device.

Category

Interactive diagnostic tests

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

After the new baud rate has been selected, the unit displays the new baud rate in the format "xxxx BPS" for 3 seconds, then returns to the idle prompt.

There are five different baud rate selections: 1200, 2400, 4800, 9600, and 19200 bps. The default of a new PINpad device is 1200 bps.

The baud rate setting is stored in backup RAM.

The PINpad device retains any change to this default through subsequent power cycles.

NOTE

After power cycling memory test or battery power is lost, the baud rate setting is reset to the factory default.

The current baud rate can be determined by using 01 Run Diagnostic Function Routine with diagnostic test # - '00.'

Packet Format

<SI> 13 [bc] <SO>{LRC}

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
13	packet type	2	Set baud rate
[bc]	packet parameter	1	Baud rate codes: • 1=1200 baud (default) • 2=2400 baud • 3=4800 baud • 4=9600 baud • 5=19200 baud
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 6 characters, minimum 6 characters

NOTE

If code of [bc] is out of range or missing, the PINpad directly echoes EOT and defaults to 1200 baud.

Examples

`<SI> 134 <SO>{LRC}` (9600 baud)

`<SI> 131 <SO>{LRS}` (1200 baud)

`<SI> 138 <SO>{LRS}` (1200 baud)

`<SI> 13 <SO>{LRC}` (1200 baud)

PINpad Protocol

Controller	Transmission Direction	PINpad
13 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect

15 Refresh PINpad Key Management Mode

The master device uses this packet to set the key management mode of the PINpad device. After the new key management mode has been selected, the PINpad device displays the new key management mode for 3 seconds, then returns to the idle prompt.

Category

Interactive diagnostic tests

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

PINpad Mode Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
15	packet type	2	Key Management Mode
[keycode]	packet parameter	4-5	Key Management Codes: • 'MKEY' - Master Session • 'DKEY' - DUKPT • 'DUAL' - Master + DUKPT • others - no change
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error check character
Packet Length: maximum 9 characters, minimum 8 characters			

PINpad Mode Comments

The master device uses this packet to change between the following key management modes supported by the PINpad:

- VISA MASTER SESSION+DUKPT mode (default)
- MASTER SESSION only mode
- DUKPT only mode

After the new key management mode has been selected, the PINpad device displays the new key management mode for 3 seconds, then returns to the idle prompt.

NOTE

Once the key management scheme is selected, it will be retained across power cycles. When switching between key management modes, sensitive data will be erased according to the following table (only in PINpad 1000SE mode -- no keys are erased in PP1000 mode).

From	To: DUAL	To: MKEY	To: DKEY
DUAL	No Change	Erase All DUKPT Engines keys	Erase M/S keys and KLK
MKEY	No Change	No Change	Erase All keys and KLK
DKEY	No Change	Erase All keys and KLK	No Change

PINpad Mode Request Format

```
<SI> 15 [keycode] <SO>{LRC}
```

PINpad Mode Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
15	packet type	2	
[keycode]	packet parameter	4-5	Available Key Management Codes: • 'MKEY' - Master Session • 'DKEY' - DUKPT • 'DUAL' - Master + DUKPT • others - no change
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error check character
Packet Length: maximum 10 characters, minimum 9 characters			

NOTE

If code of [keycode] is out of range or missing, the packet command will be ignored and aborted by an <EOT>.

PINpad Mode Response Format

```
<SI> 15 [keycode] <SO>{LRC}
```

PINpad Mode Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
15	packet type	2	Set Key Management Mode

Type	Field	Length	Description
[keycode]	packet parameter	4	Current Key Management Codes: • 'MKEY' - Master Session • 'DKEY' - DUKPT • 'DUAL' - Master + DUKPT • others - no change
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error check character
Packet Length: maximum 9 characters, minimum 10 characters			

Examples

```
<SI> 15 MKEY <SO>{LRC}
```

Sets PINpad to Master Session mode

```
<SI> 15 DKEY <SO>{LRS}
```

Sets PINpad to DUKPT mode

```
<SI> 15 DUAL <SO>{LRS}
```

Sets PINpad to dual (Master + DUKPT) mode

Protocol

Controller	Transmission Direction	PINpad
15 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	15 packet
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT to terminate process

NOTE

If the controller receives the response without any error, then it sends an ACK to the PINpad. Then PINpad then sends an <EOT> to terminate the session.

17 Set Key Management Mode

Provides additional PINpad Key Management configuration by setting or clearing control-switches in the Key Management Options Register.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet allows additional PINpad Key Management configuration through setting control-switches in the Key Management Options Register. The PINpad 1000SE supports the following additional functions compared to the PINpad 1000/ PINpad 1000+:

- 3DES DUKPT Support
- GISKE Master-Session Key Support
- Secure Messaging
- Zero Key Support
- Empty GISKE Key Support
- MAC-ed Prompt Support

NOTE

The new MAC alternatives apply only when GISKE is active, and are selected by key attribute and not by key management switch.

For compatibility, the default Key Management mode in PINpad is set to MS-DUKPT/ Single DES interleaving mode. Once a new key management scheme is selected, it will be retained during the power cycle.

NOTE

Setting a new mode causes the PINpad to erase all existing keys or non-volatile security values stored for secure messaging.

For Key Management Mode Register values, see the following table:

Table 3 Key Management Mode Register Values

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
1DES master session – **Default**	-	-	-	-	-	0	0	0
Mixed Mode (1DES & 3DES GISKE)	-	-	-	-	-	0	0	1
3DES GISKE master session	-	-	-	-	-	0	1	0
DUKPT Engine 0								
1DES DUKPT – **Default**	-	-	-	-	0	-	-	-
3DES DUKPT	-	-	-	-	1	-	-	-

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
PP1000 mode:	-	-	-		-	-	-	-
• Zero Key support off				0				
• Zero Key support on – **Default**				1				
PP1000SE mode:	-	-	-		-	-	-	-
• Zero Key support off – **Default** and always off.				0				
• Zero Key support on – N/A				1				
Empty GISKE session key support off – **Default** and always off for PP1000SE	-	-	0	-	-	-	-	-
Empty GISKE session key support on	-	-	1	-	-	-	-	-
do nothing	-	0	-	-	-	-	-	-
Clear all MS master keys & KLK.	-	1	-	-	-	-	-	-
Reserved	Rsvd	-	-	-	-	-	-	-

One ASCII-Hex digit is used produce half of a control byte which the PINpad uses as the DUKPT Engine 1/3 Mode Flag (DEMF):

Table 4 DUKPT Engine 1/3 Mode Flag (DEMF)

	Bit 3	Bit 2	Bit 1 (DUKPT Engine "2")	Bit 0 (DUKPT Engine "1")
1DES DUKPT - **Default**				0
3DES DUKPT				1
1DES DUKPT - **Default**			0	
3DES DUKPT			1	
Reserved		Reserved		
Reserved	Reserved			

Examples:

- DEMF = 0x30 equates to 1DES for Engine “1” and 1DES for Engine “2”
- DEMF = 0x32 equates to 3DES for Engine “1” and 1DES for Engine “2”
- DEMF = 0x32 equates to 1DES for Engine “1” and 3DES for Engine “2”
- DEMF = 0x33 equates to 3DES for Engine “1” and 3DES for Engine “2”

Packet Format

```
<SI> 17 [KMM] [DEMF] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
17	packet type	2	Set Key Management Mode

Type	Field	Length	Description
[KMM]	packet parameter	2	The two ASCII-Hex digits are concatenated, big-endian, to produce a single control byte. See the Key Management Mode Register Values, above, for [KMM] values.
[DEMF]	packet parameter	1	DUKPT Engine 1/3 Mode Flag (DEMF) See the DUKPT Engine 1/3 Mode Flag (DEMF), above, for [DEMF] values.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 8 characters, minimum 8 characters			

Examples

The following examples show only the command packet from the Master Device, and its translated meaning:

```
<SI>17000<SO>{LRC}
```

1DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>17010<SO>{LRC}
```

Mixed MS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>17020<SO>{LRC}
```

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>17080<SO>{LRC}
```

1DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

```
<SI>17090<SO>{LRC}
```

Mixed MS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

```
<SI>170A0<SO>{LRC}
```

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

```
<SI>17100<SO>{LRC}
```

1DESmS Mode - Zero Key Support On - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>17310<SO>{LRC}
```

Mixed MS Mode - Zero Key Support On - Empty GISKE Session Key Support On & 1DES DUKPT Mode

`<SI>17220<SO>{LRC}`

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support On & 1DES DUKPT Mode

`<SI>17180<SO>{LRC}`

1DESmS Mode - Zero Key Support On - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

`<SI>17390<SO>{LRC}`

Mixed MS Mode - Zero Key Support On - Empty GISKE Session Key Support On & 3DES DUKPT Mode

`<SI>172A0<SO>{LRC}`

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support On & 3DES DUKPT Mode

NOTE

These examples are just some of the valid PINpad KMM options. The combinations of KMM setting are limited, which means that the mixtures of MS Mode, Zero Key Support, Empty GISKE Session Key Support, SM Mode, and DUKPT Mode are not applicable in some cases. If there is a conflict in KMM setting, use the priority rules from Table 5.

Table 5 Key Management Mode Priority Rules

Priority	KMM setting	Notes
1	MS mode vs. Zero Key Support	Zero Key Support is not applicable in 3DES MS mode, due to the Key Usage Rule (single length key usage is not allowed in the 3DES MS mode)
2	MS mode vs. Empty GISKE Session Key Support	Empty GISKE Session Key Support is not applicable in 1DES MS mode, due to the Key Usage Rule (triple length key usage is not allowed in the 1DES MS mode)

Rules of Key Management Switching

The rules of Key Management Switching are listed as follows:

Rules	to 1DES (VISA)	to Mixed Mode	to 3DES
from 1DES (VISA) (!)	NC	NC	2/3K
from Mixed mode (!!)	1K	NC	2/3K
from 3DES (!!!)	E	E	NC

NOTE

In the preceding table, exclamation points (!) denote levels of security:

- (!) shows the least secure mode
- (!!) shows the transition period
- (!!!) shows the most secure mode

The other abbreviations are:

- NC – no change
- E – all key are erased
- 1K – valid 1DES keys (single length key) are retained and other keys are erased
- 2/3K – valid 3DES keys (double / triple length key) are retained and other keys are erased.

Key Mode	1DES & 3DES Key Usage Rules
1DES only (!)	• Load/Use 1D master/session keys permitted • Load KLK permitted • Load 3D master keys permitted • Use of 3D master keys forbidden • Load 3D session keys forbidden • Use of 3D session keys forbidden • Key Attributes are verified (exception: Key Usage = 'AN'-Any is allowed) • GISKE Key Block are verified
Mixed mode (!!)	• Load/Use 1D/3D master/session keys permitted • Load KLK permitted • 1D master keys used for 1D session keys • 3D master keys used for 1D and 3D DES keys • Key Attributes are verified (no exception is allowed) • GISKE Key Block are verified
3DES only (!!!)	• Load/Use 3D master/session keys permitted • Load KLK permitted • Load 1D master keys forbidden • Use of 1D master keys forbidden • Load 1D session keys forbidden • Use of 1D session keys forbidden • Key Attributes are verified (no exception is allowed) • GISKE Key Block are verified

NOTE

1. In the preceding table, exclamation points (!) denote levels of security:
   - (!) shows the least secure mode
   - (!!) shows the transition period
   - (!!!) shows the most secure mode
2. Key Management Register is set using 17 Set Key Management Mode.
3. In the preceding table, 'Key Attributes are verified' indicates that upon using a Key stored in the PINpad, the PINpad must validate the content of all key attributes. The attributes of the key are validated against GISKE Spec that is acceptable for that command.
4. In the above table, 'GISKE Key Block are verified' indicates that upon receiving a Key Block, the PINpad must validate both the validity of the Key Block Binding Method of the Key Block and the validity of the content of the header. The header of the key is validated against a list of headers that are acceptable for that command.

NOTE

All DUKPT related keys, counters, and registers are erased, when PINpad Key Management switches between 1DES DUKPT and 3DES DUKPT. Other MS related information remains untouched.

Protocol

Controller	Transmission Direction	PINpad
17 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)

Controller	Transmission Direction	PINpad
	<------	17 packet **Note:** For Packet 17 KMM Bits 2-0, Secure Messaging Mode cannot be selected if PINpad. If any attempt is made to switch to Secure Message, only ACK is returned and no further response is sent. **Note:** Due to PINpad Mode Management Rules (see PINpad Mode Management Rules for more details), if the setting does not compile with the rule, only ACK is returned and no further response is sent.
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs) EOT if LRC correct but key management NOT OK	------>	
	<------	EOT to terminate process **Note:** PINpad saves new key management and will use the PINpad key management accordingly.

NOTE

1. The default setting of PINpad KMM is "old single DES mode," with all zeros in KMM register.
2. When Empty GISKE Session Key Support is "ON", the current master key is used for PIN encryption, only if the current master key has it's key attribute set to "PIN Encryption" or "ANY". Empty GISKE (3DES) session key means all fields are zeros in the GISKE Key Block.
3. More information on the multiple DUKPT Engine functionality is described in Multiple DUKPT Engines.
4. Key Mode Management Rules are used under the PINpad Mode Management Rules. See PINpad Mode Management Rules for details.

18 Check Key Management Options Register Mode

Checks the setting in the PINpad Key Management Options Register.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

Request Format

```
<SI> 18 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
18	packet type	2	Check Key Management Options Register Mode
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 5 characters, minimum 5 characters

Response Format

```
<SI> 18 [KMM] [DEMF] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
18	packet type	2	Set Key Management Mode
[KMM]	packet parameter	2	The two ASCII-Hex digits are concatenated, big-endian, to produce a single control byte. See the Key Management Mode Register Values, under 17 Set Key Management Mode, for [KMM] values.
[DEMF]	packet parameter	1	DUKPT Engine 1/3 Mode Flag See the DUKPT Engine 1/3 Mode Flag (DEMF), under 17 Set Key Management Mode, for [DEMF] values.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 8 characters, minimum 8 characters

Examples

The following examples show the response packet from the PINpad, and its translated meaning.

In the first set of examples, the PINpad contains the MS key(s) or the KLK key.

<SI>18000<SO>{LRC}

1DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

<SI>18010<SO>{LRC}

Mixed MS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

<SI>18020<SO>{LRC}

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

<SI>18080<SO>{LRC}

1DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

<SI>18090<SO>{LRC}

Mixed MS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

<SI>180A0<SO>{LRC}

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

<SI>18100<SO>{LRC}

1DESmS Mode - Zero Key Support On - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

<SI>18310<SO>{LRC}

Mixed MS Mode - Zero Key Support On - Empty GISKE Session Key Support On & 1DES DUKPT Mode

<SI>18220<SO>{LRC}

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support On & 1DES DUKPT Mode

<SI>18180<SO>{LRC}

1DESmS Mode - Zero Key Support On - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

<SI>18390<SO>{LRC}

Mixed MS Mode - Zero Key Support On - Empty GISKE Session Key Support On & 3DES DUKPT Mode

<SI>182A0<SO>{LRC}

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support On & 3DES DUKPT Mode

In the next set of examples, all MS master key registers and KLK key register are clear:

```
<SI>18400<SO>{LRC}
```

1DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>18410<SO>{LRC}
```

Mixed MS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>18420<SO>{LRC}
```

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support Off & 1DES DUKPT Mode

```
<SI>18580<SO>{LRC}
```

1DESmS Mode - Zero Key Support On - Empty GISKE Session Key Support Off & 3DES DUKPT Mode

```
<SI>18790<SO>{LRC}
```

Mixed MS Mode - Zero Key Support On - Empty GISKE Session Key Support On & 3DES DUKPT Mode

```
<SI>186A0<SO>{LRC}
```

3DESmS Mode - Zero Key Support Off - Empty GISKE Session Key Support On & 3DES DUKPT Mode

Protocol

Controller	Transmission Direction	PINpad
18 request packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	18 response packet
ACK = LRC OK NAK = LRC incorrect	------>	
	<------	EOT to terminate process

72 Cancel Session Request

Returns the PINpad device to its idle state.

Category

Standard Communication Packet

Comments

Packet 72 is the only packet which can be used to cancel/abort following PIN/data entry mode:

Entry	Packet Types
PIN entry	Z60, Z62, 60, 62, 70
Data entry	Z40, Z42, Z50

After the PINpad device receives a 72, an EOT is sent back to terminate the session. If a Packet 72 is received and the PINpad unit is not in PIN or data entry mode, an ACK response is the normal condition.

Packet Format

```
<STX> 72 <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
72	packet type	2	Cancel Session Request
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Example

```
<STX> 72 <ETX>{LRC}
```

The PINpad goes to the idle state.

Protocol

Controller	Transmission Direction	PINpad
72 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect

Q2 Indicate Host Done

Informs the PINpad device the host has responded and the transaction is at an end.

Category Custom Communication Packet

Comments When the PINpad unit receives the Q2 message packet, it displays THANK YOU for 3 seconds, followed by the idle prompt.

Packet Format

```
<STX> Q2 <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Q2	packet type	2	Indicate Host Done
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Example

```
<STX> Q2 <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
Q2 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect Three-second THANK YOU message display, followed by idle prompt.

Q5 Alternate PROCESSING Prompt

Selects the companion message that the PINpad device displays in rotation with the "PROCESSING" message.

Category Custom Communication Packet

Comments The companion message is either PIN PAD or PIN PAL; the default is PIN PAD. The alternating processing messages appear after PIN entry, following either Packet Z60, Accept and Encrypt PIN, or Packet Z70, Request PIN Entry. If the PINpad unit is currently displaying the processing messages when it receives this message packet, it changes to the requested sequence.

Packet Format `<STX> Q5[flag] <ETX>{LRC}`

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Q5	packet type	2	Alternate Processing Display
[flag]	packet parameter	1	Display Message Type Value: • 0 = PIN PAD • 1 = PIN PAL
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example

```
<STX> Q51 <ETX>{LRC}
```

The PINpad alternately displays the "PIN PAL" and "PROCESSING" messages.

Protocol

Controller	Transmission Direction	PINpad
Q51 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect

Z1 Return to Idle State

Returns the PINpad device to the idle state.

Category Custom Communication Packet

Packet Format `<STX> Z1 <ETX>{LRC}`

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z1	packet type	2	Return to Idle State
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Example `<STX> Z1 <ETX>{LRC}`

The PINpad unit goes to the idle state.

Protocol

Controller	Transmission Direction	PINpad
Z1 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect

Z2 Display a String

Directs the PINpad device to display a single string message.

Category Custom Communication Packet

Comments The PINpad unit displays the message until the user presses [CLEAR] or it receives another message from the controller that changes the message contents or returns to the idle prompt.

The exceptions are Packets Z40, Z42, Z50, Z60, and 60. The display of the message must remain intact upon receipt of any one of these five packets. Without a <SUB> but with a null message, the last message is displayed.

Packet Format

```
<STX> Z2 <SUB> [message] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z2	packet type	2	Display a String
<SUB>	message parameter	1	Optional; Clears display Value: `1Ah'
[message]	packet parameter	0-16	Message/Prompt to Display format is ASCII (not counted string)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 22 characters, minimum 5 characters			

Examples

```
<STX> Z2 THX <ETX>{LRC}
```

Directs the PINpad to add the message THX to the end of the currently displayed message. If the total display exceeds 16 characters, only the first 16 characters are shown.

```
<STX> Z2 <SUB> PLZ SLIDE CARD <ETX>{LRC}
```

Directs the PINpad device to clear the current display (substitute), then display the message PLZ SLIDE CARD.

Protocol

Controller	Transmission Direction	PINpad
Z2 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect Display message

MACed Z2 Display a String

Directs the PINpad device to display a single string message and provides MAC message authentication capabilities.

NOTE

See Non-MACed Z2/Z3 Message Matching Rules for details on MAC message authentication.

See Z40 Request Key Code/Z41 Return Key Code, Z42 Request Key Value/Z43 Return Key Value, and Z50 Request String Input/Z51 Return String Input for more details on validating MACing and how that affects the return of keystrokes from the PINpad to the controller.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

This packet is only available in version 4E3002x and later releases of the firmware.

If in PINpad 1000 mode, the PINpad ignores any MAC data and returns 0 (no error).

Comments

The PINpad unit displays the message until the user presses [CLEAR] or it receives another message from the controller that changes the message contents or returns to the idle prompt.

The exceptions are Packets Z40, Z42, Z50, Z60, and 60. The display of the message must remain intact upon receipt of any one of these five packets. Without a <SUB> but with a null message, the last message is displayed.

The MAC will be calculated using a selected MAC key. This MAC key will be used to calculate an Outer CBC MAC with an IV of 0x0000000000000000. If the prompt data is not on an even 8-byte boundary, the last block will be right-padded with 0x30's. The four left most bytes (8 hex digits) of the resulting cryptogram will be used for the MAC value.

NOTE

The MAC key used to verify this packet must be 112 bits in length to meet the November, 2003 Visa PED requirements and must also be tagged as a MAC verification key.

- Version 4E3003x and later releases of the firmware enforce the 112-bit MAC key rule.
- Appropriate algorithms and key sizes will change slowly over time, as computing capability expands to make brute force attacks more feasible.

Request Format

```
<STX> Z2 <FS> <MKI> <MV> <SUB> <message> <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z2	packet type	2	Display a String
<FS>	packet parameter	1	Field separator; Value: '1Ch'
[MKI]	packet parameter	1	MAC Key Index; Select Key from keys 0-F
[MV]	packet parameter	8	Mac Value; the four left most digits of the MAC calculation
<SUB>	message parameter	1	Optional; Clears display Value: `1Ah'
[message]	packet parameter	0-16	Message/Prompt to Display format is ASCII (not counted string)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 255 characters, minimum 15 characters

The User Definable Character (UDC) function is supported in this packet for [message]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

Example Request

```
<STX> Z2 <FS> <MKI> <MV> <SUB> AB <ETX>{LRC}
```

This sample packet initiates the PINpad to clear the display and then shows 'AB.'

Response Format

```
<STX> Z2 <R> <ETX> {LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z2	packet type	2	Display a String
[R]	packet parameter	1	Z2 Response • 0 = No Error • 1 = MAC Key index error • 2 = MAC key attributes error • 3 = MAC value error • 4 = Packet format error
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example Response

```
<STX> Z2 0 <ETX> {LRC}
```

Further Examples

Examples of Z2 packets with MAC values:

MAC key value used to compute the following MAC values:

```
6AC292FAA1315B4D8234B3A3D7D5933A
```

MAC algorithm used to compute the following MAC values:

```
"10"(ISO 9797-1 MAC Algorithm 1 - 112 bits)
```

Packet format:

```
<STX>Z2<FS>kvvvvvvvv<SUB>prompt<ETX>
```

- k = MAC Key index
- v = The four leftmost bytes of the MAC calculation converted to hex ascii
- The prompt may contain a user definable character (<US>xxxx)

```
<STX>Z2<FS>307211021<SUB>MUDCHR 59<US>8A12<US>4A72 STOP<ETX>
```

Data MACed - `<SUB>MUDCHR<US>8A12<US>4A72STOP000  Padding 000`

```
<STX>Z2<FS>3EF3F9B78<SUB>MENTER VEHICLE #<ETX>
```

Data MACed - `<SUB>MENTERVEHICLE00  Padding 00`

```
<STX>Z2<FS>37B40BA95<SUB>  MENTER ODOMETER <ETX>
```

Data MACed - `<SUB>MENTERODOMETER0  Padding 0`

Protocol

Controller	Transmission Direction	PINpad
Z2 request packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	Z2 response packet clear display, then show [message]
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT

Z3 Display Rotating Messages

Directs the PINpad device to display up to seven messages or prompts in rotation.

Category Custom Communication Packet

Comments Up to seven prompts or messages can be displayed in rotation. The PINpad device displays the message strings at 3-second intervals until it receives another message or the customer presses [CLEAR].

The message must remain intact upon receipt of Packets Z40, Z42, Z50, and Z60.

Packet Format `<STX> Z3 [count] <SUB> [message1] <FS> [message2 ... 7] <ETX>{LRC}`

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z3	packet type	2	Display Rotating Messages
[count]	packet parameter	1	Number of messages; Range: 0-7
<SUB>	message parameter	1	Optional; Substitute Value: `1Ah'
[message1]	packet parameter	0-16	First Message (Not counting string)
<FS>	packet parameter	1	Optional; Field Separator; Only Present When Next Message Follows; Value:`1Ch'
[message2...7]	packet parameter	0-16	Next Message or Prompt to Display; each message separated by <FS>; format is ASCII (not counting string)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 124 characters, minimum 6 characters

Example

```
<STX> Z33<SUB>WELCOME <FS> PLEASE <FS> SLIDE CARD <ETX>{LRC}
```

The PINpad device clears the current display and displays, at three second intervals, the messages WELCOME, PLEASE, and SLIDE CARD.

Protocol

Controller	Transmission Direction	PINpad
Z3 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		Alternately display:
		[message1] [message2..7]

MACed Z3 Display Rotating Messages

Directs the PINpad device to display up to seven messages or prompts in rotation and provides MAC message authentication capabilities.

NOTE

See Non-MACed Z2/Z3 Message Matching Rules for details on MAC message authentication.

See Z40 Request Key Code/Z41 Return Key Code, Z42 Request Key Value/Z43 Return Key Value, and Z50 Request String Input/Z51 Return String Input for more details on validating MACing and how that affects the return of keystrokes from the PINpad to the controller.

Category Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

This packet is only available in version 4E3002x and later releases of the firmware.

If in PINpad 1000 mode, the PINpad ignores any MAC data and returns 0 (no error).

Comments Up to seven prompts or messages can be displayed in rotation. The PINpad device displays the message strings at 3-second intervals until it receives another message or the customer presses [CLEAR].

NOTE

The message must remain intact upon receipt of Packets Z40, Z42, Z50, and Z60.

The MAC will be calculated using a selected MAC key. This MAC key will be used to calculate an Outer CBC MAC with an IV of 0x0000000000000000. If the prompt data is not on an even 8-byte boundary, the last block will be right-padded with 0x30's. The four left most bytes (8 hex digits) of the resulting cryptogram will be used for the MAC value.

NOTE

The MAC key used to verify this packet must be 112 bits in length to meet the November, 2003 Visa PED requirements and must also be tagged as a MAC verification key.

- Version 4E3003x and later releases of the firmware enforce the 112-bit MAC key rule.
- Appropriate algorithms and key sizes will change slowly over time, as computing capability expands to make brute force attacks more feasible.

NOTE

Use message lengths of no more than 16 characters per message. If longer messages are used, the display will only show the last 16 characters entered and any extra characters will be ignored.

Request Format

```
<STX> Z3 <FS> <MKI> <MV> <N> <SUB> <message> <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z3	packet type	2	Display Rotating Messages
<FS>	packet parameter	1	Field separator; Value: '1Ch'
[MKI]	packet parameter	1	MAC Key Index; Select Key from keys 0-F
[MV]	packet parameter	8	Mac Value; the eight left most digits of the MAC calculation
[N]	packet parameter	1	Number of Messages: 0-7
<SUB>	message parameter	1	Optional; Clears display Value: `1Ah'
[message 1]	packet parameter	0-16	First message to display format is ASCII (not counted string)
<FS>	packet parameter	1	Field separator; Value: '1Ch'
[message2...n]	packet parameter	0-16	Next message to display (up to 7 messages); each message separated by <FS>
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 255 characters, minimum 16 characters

NOTE

The User Definable Character (UDC) function is supported in this packet for [message]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

Example Request

```
<STX> Z3 <FS> <MKI> 81762593 3 <SUB> AB <FS> <FS> CD <ETX>{LRC}
```

This packet causes the PINpad to display the message 'AB' first, then a blank display, then 'CD,' and then redisplays the messages, starting over from the 'AB' message. This continues until the CLEAR key is pressed or another packet is received, with the exception of Packets Z40, Z42, Z50, and Z60.

Response Format

```
<STX> Z3 <R> <ETX> {LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z3	packet type	2	Display a String
[R]	packet parameter	1	Z3 Response • 0 = No Error • 1 = MAC Key index error • 2 = MAC key attributes error • 3 = MAC value error • 4 = Packet format error
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 6 characters, minimum 6 characters

Example Response

```
<STX> Z3 0 <ETX> {LRC}
```

Further Examples

Examples of Z3 packets with MAC values:

MAC key value used to compute the following MAC values:

```
6AC292FAA1315B4D8234B3A3D7D5933A
```

MAC algorithm used to compute the following MAC values:

```
"10"(ISO 9797-1 MAC Algorithm 1 - 112 bits)
```

Packet format:

```
<STX>Z3<FS>kvvvvvvvvn<SUB>prompt1<FS>prompt2<ETX>
```

- k = MAC Key index
- v = The four leftmost bytes of the MAC calculation converted to hex ascii
- n = Number of messages
- The prompt may contain a user definable character (<US>xxxx)

```
<STX>Z3<FS>386A200932<SUB>MESSAGE ONE 1<FS>MESSAGE TWO 2<ETX>

<STX>Z3<FS>386A200932<SUB> MESSAGE ONE 1.0<FS>MESSAGE TWO 2.0 <ETX>

<STX>Z3<FS>386A200932<SUB> MESSAGE 1.0 ONE<FS>MESSAGE 2.0 TWO <ETX>
```

Data MACed - `<SUB>MESSAGEONE<FS>MESSAGETWO00  Padding 00`

NOTE

The MAC value is the same for the above Z3 packets.

Protocol

Controller	Transmission Direction	PINpad
Z3 request packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
	<------	Z3 response packet
		clear display, then cycles through [message 1], [message 2]...
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT

Z7 Turn on/off CANCEL REQUESTED

Disables (turn off) or enables (turn on) the CANCEL REQUESTED prompt.

Category Custom Communication Packet

Comments When the controller sends message Packet Z7, the PINpad either displays or does not display the CANCEL REQUESTED message when [CLEAR] is entered or when the controller requests a cancel termination.

Packet Format

```
<STX> Z7 [flag] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z7	packet type	2	Turn on/off CANCEL REQUESTED
[flag]	packet parameter	1	Cancel Request Flag Range: • 0 = Show message • 1 = Do not show message
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example

```
<STX> Z71 <ETX>{LRC}
```

Disable CANCEL REQUESTED message.

Protocol

Controller	Transmission Direction	PINpad
Z7 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect Turns on/off prompt

Z8 Reset/Set Idle Prompt

Sets or resets the PINpad device idle prompt display.

Category Custom Communication Packet

Comments To reset the PINpad device idle prompt, send Packet Z8 with a null string. The PINpad unit will display a cycling arrow at idle.

Packet Format

```
<STX> Z8 [prompt] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z8	packet type	2	Reset/Set Idle Prompt
[prompt]	packet parameter	0-16	Prompt to display when idling
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 21 characters, minimum 5 characters			

Example

```
<STX> Z8 <ETX>{LRC}
```

This message packet does not include the display specification; it directs the PINpad to display the cycling arrow.

Protocol

Controller	Transmission Direction	PINpad
Z8 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect idle prompt displays

Z10 Load Prompt Table

Loads a new prompt table to PINpad RAM.

NOTE

This packet is only available in version 4E3002x and later releases of the firmware.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

In PINpad 1000 mode, Packet Z10 has no real relevance: the RAM table contained in the packet is ignored. The response packet is a "no error" packet (return code '0') but the packet data is NOT loaded into RAM.

Comments

This packet must be MACed using a selected Master key as the MAC key. This MAC key will use the ANSI/ISO MACing algorithms for MACing, available as indicated by the GISKE Key Usage attributes. See *GISKE Key Block Specification* VPN - 22986 for details of MAC algorithms.

NOTE

The MAC key used to verify this packet must be 112 bits in length to meet the November, 2003 Visa PED requirements and must also be tagged as a MAC verification key.

- Version 4E3003x and later releases of the firmware enforce the 112-bit MAC key rule.
- Appropriate algorithms and key sizes will change slowly over time, as computing capability expands to make brute force attacks more feasible.

Data fields need to be MACed including the "prompt message" and the field separator. Valid prompt text characters for MACing over are any characters in the range 'A' - 'Z' (0x41 - 0x5A) and user definable characters (UDCs) (eg: <US>4E72, all five characters need to be MACed). Empty text in any message block is NOT allowed. If the last MAC input is not on an even 8-byte boundary, the last block will be right-padded with 0x30's. The four left most bytes (8 hex digits) of the resulting cryptogram will be used for the MAC value. The PINpad internally allocates one control byte for each prompt text. This control byte is used to indicate the length of the prompt text.

NOTE

This packet will overwrite the existing prompt table in the RAM if no error is detected.

Request Format

```
<STX> Z10 [MKI] [MV] <FS> [prompt message 1] <FS> [prompt message 2] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z10	packet type	3	Load Prompt Table
[MKI]	packet parameter	1	Master Key used to do the MACing
[MV]	packet parameter	8	The four leftmost bytes (8 digits) of the MAC calculation
<FS>	packet parameter	1	Field separator; Value: '1Ch'
[prompt message 1]	packet parameter	1-16	First prompt message text
<FS>	packet parameter	1	Field separator; Value: '1Ch'
[prompt message2...n]	packet parameter	1-16	Next prompt message to display; each message separated by <FS>
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 255 characters, minimum 17 characters (with one byte in the prompt table)			

Response Format

```
<STX> Z10 <R> <ETX> {LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z10	packet type	3	Load Prompt Table Reponse
[R]	packet parameter	1	Z10 Response • 0 = No Error • 1 = MAC Key index error • 2 = MAC key attributes error • 3 = MAC value error • 4 = Packet format error • 5 = Repeat Message error (a message appears twice or more in the Z10 packet)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 7 characters, minimum 7 characters			

Example Response

```
<STX> Z10 0 <ETX> {LRC}
```

Examples

Example of Z10 packet:

MAC key value used to compute the following MAC values:

```
6AC292FAA1315B4D8234B3A3D7D5933A
```

MAC algorithm used to compute the following MAC values:

```
"10"(ISO 9797-1 MAC Algorithm 1 - 112 bits)
```

Packet format:

```
<STX>Z10kvvvvvvvv<FS>prompt1<FS>prompt2<FS>prompt3<ETX>
```

- k = MAC Key index
- v = The four leftmost bytes of the MAC calculation converted to hex ascii
- The prompt may contain a user definable character (<US>xxxx)

```
<STX>Z1035C5CD64A<FS>ENTERTELNUMBER<FS>ENTERSSNNUMBER
<FS>UDCHR<US>8A12<US>4A72STOP<FS>ENTERVEHICLE<ETX>
```

Data MACed -

```
<FS>ENTERTELNUMBER<FS>ENTERSSNNUMBER<FS>UDCHR<US>8A12<US>4A72STOP
<FS>ENTERVEHICLE0     Padding 0
```

Protocol

Controller	Transmission Direction	PINpad
Z10 request packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	Z10 response packet
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	EOT

Z40 Request Key Code

Requests entry of the key code representing a key from the PINpad.

NOTE

This packet does not change the PINpad device display.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments

The controller sends this packet after the PINpad device has displayed one or more messages requesting the customer's key entry (Packets Z2 or Z3). This packet also specifies how long the PINpad device has to wait for the input before a timeout.

- If no key is pressed before the timeout, the PINpad returns to its idle state.
- If a key is pressed before the timeout, the PINpad sends the ASCII key code to the controller.

See Z41 Return Key Code for details on how the PINpad unit responds to the Z40 request. The PINpad unit does not echo the input on its display.

NOTE

Rev. 0I and earlier versions of PP101 required a full three-digits value for [timeout]. Later versions allow one to three digits (i.e. 1, 01, and 001 all signify a one-second timeout value).

Packet Format

```
<STX> Z40 [timeout] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z40	packet type	3	Request Single Key
[timeout]	packet parameter	1-3	Timeout value in seconds; range is 0-255
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 9 characters, minimum 7 characters			

Example

```
<STX> Z40 120 <ETX>{LRC}
```

The packet requests a single key entry from the PINpad and tells the PINpad to wait up to 120 seconds for the entry. The PINpad unit sends the ASCII key code of the entered key to the controller.

Protocol

Controller	Transmission Direction	PINpad
Z40 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect user presses key

Z41 Return Key Code

Returns a key code to the controller in response to Z40 Request Key Code.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments

Upon receipt of Z40 Request Key Code, the PINpad returns the ASCII key code of the entered key to the master device via Packet Z41, or a '?' if the timeout limit expires.

Use Packets Z40 and Z41 messages when you want the PINpad to return the *code* representing the key entered; use Packets Z42 and Z43 when you want the PINpad to return the *key value* entered.

NOTE

PINpad 1000SE Mode

In PINpad 1000SE mode, the usage of Packets Z40 and Z41 is dictated by the message Z2 or Z3 display packet that immediately precedes them.

- If the Z2 or Z3 packet is MACed correctly, or if the message in the Z2 or Z3 packet matches, then Packets Z40 and Z41 have full functionality and all keystrokes are returned.
- If this is not the case, then the PINpad does not return numeric keystrokes '0' - '9' (0x30 - 0x39) in the response Packet Z41.

See Non-MACed Z2/Z3 Message Matching Rules for details on what ‘matching’ means in this context.

PINpad 1000 Mode

In PINpad 1000 mode, Packets Z40 and Z41 can be used with full functionality without MAC or matching message validation. If a Z2 or Z3 packet is received with a MAC, the MAC is ignored and the message is displayed. Even if the MAC value is incorrect, the MAC field is simply ignored and the Z41 returns all keypad strokes including numeric keys.

For key codes, see the following table:

Key Pressed	1	2	3	4	5	6	7	8	9	*	0	#	/[a]	F1	F2	F3
Key Code	1	2	3	5	6	7	9	10	11	13	14	15	16	20	21	22

a. '/' in the above table indicates backspace

Packet Format

```
<STX> Z41 [key code] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z41	packet type	3	Return Key Code
[key code]	packet parameter	1-2	Code for key entered; ASCII of the key pressed; range is indicated in the table above; Value is `?' if timed out
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 8 characters, minimum 7 characters			

Example

```
<STX> Z4 111 <ETX>{LRC}
```

This packet shows the key [9] has been entered.

Protocol

Controller	Transmission Direction	PINpad
Z40 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs) user presses key
	<------	
		Z41 packet
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	

Z42 Request Key Value

Requests the ASCII value of a key to be entered from the PINpad device.

NOTE

This packet does not change the PINpad unit display.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments

The controller sends this packet after the PINpad has displayed one or more messages requesting the customer's key entry (Packets Z2 or Z3). This packet also specifies how long the PINpad has to wait for the input before a timeout. The PINpad sends the ASCII value of the key entered to the controller. Upon receipt of the key input, the PINpad will send the ASCII key value of the entered key to the master device via Packet Z43.

The PINpad does not echo the input on its display, and if no key input occurs within the specified timeout interval, the PINpad returns to its idle state.

See Z43 Return Key Value for details on how the PINpad responds to the Z42 request.

Packet Format

```
<STX> Z42 [timeout] <ETX>
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z42	packet	3	Request Key Value
[timeout]	packet parameter	1-3	Timeout value in seconds; range is 0-255
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 9 characters, minimum 7 characters			

NOTE

Rev. 0I and earlier versions of PP101 required a full three-digits value for [timeout]. Later versions allow one to three digits (i.e. 1, 01, and 001 all signify a one-second timeout value).

Example

```
<STX> Z42 045 <ETX>{LRC}
```

Packet requests a single key entry from the PINpad unit and tells it to wait up to 45 seconds for the entry before returning to the idle state. The PINpad unit sends the key value to the controller.

Protocol

Controller	Transmission Direction	PINpad
Z42 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs) user presses key

Z43 Return Key Value

Sends a key value to the controller in response to Z42 Request Key Value.

Category Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments Upon receipt of Z42 Request Key Value, the PINpad returns the ASCII key value of the entered key to the master device via Packet Z43, or a '?' if the timeout limit expires. Use Packets Z42 and Z43 when you want the PINpad to return the *key value* entered; use Packets Z40 and Z41 messages when you want the PINpad to return the *code* representing the key entered.

NOTE

PINpad 1000SE Mode

In PINpad 1000SE mode, the usage of Packets Z42 and Z43 is dictated by the message Z2 or Z3 display packet that immediately precedes them.

- If the Z2 or Z3 packet is MACed correctly, or if the message in the Z2 or Z3 packet matches, then Packets Z42 and Z43 have full functionality and all keystrokes are returned.
- If this is not the case, then the PINpad does not return numeric keystrokes '0' - '9' (0x30 - 0x39) in the response Packet Z43.

See Non-MACed Z2/Z3 Message Matching Rules for details on what ‘matching’ means in this context.

PINpad 1000 Mode

In PINpad 1000 mode, Packets Z42 and Z43 can be used with full functionality without MAC or matching message validation. If a Z2 or Z3 packet is received with a MAC, the MAC is ignored and the message is displayed. Even if the MAC value is incorrect, the MAC field is simply ignored and the Z43 returns all keypad strokes including numeric keys.

For key values, see the following table:

Key Pressed	1	2	3	4	5	6	7	8	9	*	0	#	/[a]	F1	F2	F3
Key Value	1	2	3	4	5	6	7	8	9	*	0	#	/	A	B	C

a. '/' in the above table indicates backspace

Packet Format

```
<STX> Z43 [key] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z43	packet type	3	Return Key Value
[key]	packet parameter	1	ASCII of the key pressed • Range is indicated in the table above • Value is `?' if timed out
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 7 characters, minimum 7 characters			

Example

```
<STX> Z43 * <ETX>{LRC}
```

This message packet indicates the key [*] has been pressed.

Protocol

Controller	Transmission Direction	PINpad
		customer presses key
	<------	Z43 packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		

Z50 Request String Input

Requests a string of key inputs to be entered from the keypad.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments

The controller sends this packet request key inputs from the PINpad keyboard after the PINpad displays one or more messages requesting the customer's key inputs (Z2 Display a String or Z3 Display Rotating Messages). This packet specifies whether the key inputs are displayed or not, the maximum number of key entries, and how long the PINpad has to wait for input before timing out.

A timeout value (in seconds) must be specified. If no keys are pressed before the specified timeout, the PINpad returns to its idle state.

The PINpad device waits for a string input from its keypad, then returns to the controller the ASCII equivalent of the pressed keys. The customer must press [ENTER] to end a string input and return a Z51 Return String Input packet.

The PINpad device can accept a null entry for Packet Z50.

During the Z50 session, only 72 Cancel Session Request from the controller or the PINpad [CLEAR] key can cancel the session.

- If data entry is not initiated, pressing [CLEAR] will cancel the operation and send an [EOT] to the controller.
- If data entry is initiated, the PINpad device clears the entry, redisplays the previous prompt, and restarts data entry.

See Z51 Return String Input for details on how the PINpad unit responds to the Z50 request.

Packet Format

```
<STX> Z50 [echo flag] [timeout] [max-entry] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z50	packet type	3	Request String Input
[echo flag]	packet parameter	1	Echo Flag • 0 = Echo input as asterisks (*) • 1 = Echo input as characters (numbers) • 2 = Do not echo input
[timeout]	packet parameter	3	Timeout value in seconds; range is 000-255
[max entry]	packet parameter	2	*optional, defaults if omitted* Maximum Acceptable Keypad Input Length • Range: 01-49 • Default: 49
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 12 characters, minimum 10 characters			

Example

```
<STX> Z50 0 120 <ETX>{LRC}
```

The PINpad device waits up to 120 seconds for keypad input, with asterisks echoed on the display in response to key entry.

Protocol

Controller	Transmission Direction	PINpad
Z50 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs) user keypad entry

Z51 Return String Input

Directs the PINpad device to return a string of ASCII values of the keys entered to the controller. Use this packet following the Z50 Request String Input packet.

Category Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

NOTE

Extended message validation functionality is only available in version 4E3002x and later releases of the firmware, and depends on the security status of Packets Z2 and Z3. For further details on this application, please refer to the Prompt Table for Z2/Z3 Authentication.

Comments Upon receipt of Z50 Request String Input, the PINpad device returns to the controller the ASCII equivalent of the pressed keys (0-9), as a string, when the [ENTER] key is pressed. The PINpad returns a '?' if no keys are pressed before the specified timeout.

NOTE

PINpad 1000SE Mode

In PINpad 1000SE mode, the usage of Packets Z50 and Z51 is dictated by the message Z2 or Z3 display packet that immediately precedes them.

- If the Z2 or Z3 packet is MACed correctly, or if the message in the Z2 or Z3 packet matches, then packet Z51 has full functionality and all keystrokes are returned.
- If this is not the case, then the PINpad returns <EOT> and the PINpad displays the error message "PACKET ERR B."

See Non-MACed Z2/Z3 Message Matching Rules for details on what 'matching' means in this context.

PINpad 1000 Mode

In PINpad 1000 mode, Packets Z50 and Z51 can be used with full functionality without MAC or matching message validation. If a Z2 or Z3 packet is received with a MAC, the MAC is ignored and the message is displayed. Even if the MAC value is incorrect, the MAC field is simply ignored and the Z51 returns all keypad strokes including numeric keys.

Packet Format

```
<STX> Z51 [entry] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z51	packet	3	Return String Input
[entry]	packet parameter	0-49	Keypad character input as ASCII string; '?' if timeout; null if only [ENTER] was pressed
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 55 characters, minimum 6 characters			

Example

```
<STX> Z51 123456 <ETX>{LRC}
```

The PINpad sends the controller the keypad entry 123456.

Protocol

Controller	Transmission Direction	PINpad
Z50 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs) Customer presses keys
	<------	Z51 packet or <EOT> (see PINpad 1000SE Mode for more details)
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	

Key Value Table

Key	1	2	3	4	5	6	7	8	9	0	F1	F2	F3
Keycode	1	2	3	4	5	6	7	8	9	0	A	B	C

Master/Session Message Packets

When the PINpad device is set in the Master/Session mode (1DES or 3DES), the following message packets and formats are supported.

NOTE

The default mode of the PINpad at initial power up is PP1000 mode, MS 1DES mode.

Functional Listing of PINpad Device Messages

The messages sent to and from the PINpad device to manipulate operations or control specific PINpad functions are divided into three functional groups. These groups include packets for interactive diagnostic tests, and standard and custom communication.

Interactive Diagnostic Test

Interactive tests between the PINpad unit and the controller run only upon request. These tests use the VeriFone-defined message Packets 01-15, and can be run during the same session that you load master keys, use the MKI module or on request from the PINpad controller.

See other packets listed under Management Packets.

Message	Description
02	02 Transfer Master Key
04	04 Check Master Key
08	08 Select Master Key

Standard Communication

The standard messages sent between the PINpad device and the controller follow the VISA message packet format and allow the PINpad unit to be programmed with standard VISA prompts and control the PINpad display. There is sufficient variation in Packets 70 and 71 to merit specific discussions in this chapter, as well as in the DUKPT Message Packets chapter.

Message	Description
70	70 Request PIN Entry*
71	71 Transfer PIN Block*

NOTE

If using the optional DUKPT method, message Packets 70 and 71 have been redefined to meet the DUKPT algorithm specification by VISA.

See DUKPT Message Packets for details of redefinitions.

Custom Communication

These message packets were created to provide the PINpad device with special prompts and data entry requirements for custom applications. The request and response messages pass between the controller and the PINpad, allowing the controller to customize prompts and control PINpad operations. There is sufficient variation in Packets Z60 and Z62 to merit specific discussions in this chapter, as well as in the DUKPT Message Packets chapter.

Message	Description
Z60	Z60 Accept and Encrypt PIN*
Z62	Z62 Accept and Encrypt PIN, Display Custom Messages*

NOTE

If using the optional DUKPT method, message Packets Z3, Z60, and Z62 have been redefined to meet the DUKPT algorithm specification by VISA.

See DUKPT Message Packets for details of redefinitions.

02 Transfer Master Key

Sends a master key to the PINpad device for storage in one of the ten master key memory locations.

Category Interactive Diagnostic Test

Comments The master device uses this packet to send a master key to the PINpad. The response from PINpad to master device depends on the PINpad Key Management Option register.

The PINpad supports 10 sets of single, double, or triple length keys. Single keys can be replaced by double or triple length of key without restriction, and vice versa.

Packet 02 exists in two formats, with a communication protocol that depends on the size of the Master Key Field in ASCII:

Communication Protocol	Size of Master Key Field in ASCII
Key-only Format	1DES (16AH)
GISKE Key Block Format	3DES GISKE mode (120AH)

NOTE

When the PINpad receives Packet 02 (1DES or 3DES Master Key), it updates the master key in RAM and sets the currently transferred master key ID as the currently selected master key ID in PINpad.

- The packet overwrites any master key previously stored at the specified memory location and automatically verifies that the PINpad receives the same key that is sent.
- If there is any valid master key in the PINpad, the currently selected master key ID is always available. 17 Set Key Management Mode can be used to erase all the master keys stored in the PINpad.

Before transferring the master key, verify if you are overwriting a key by using 04 Check Master Key.

This option is disabled when the unit is set for DUKPT.

Packet Format

```
<SI> 02 [address] [hhh...hh] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
02	packet type	2	Transfer Master Key
[address]	packet parameter	1	Master Key ID Address; Range: 0-9 GISKE KLK: 'F'
[hhh...hh]	packet parameter	16 or 120	ASCII message in ASCII • 16AH - 1DES mode for single length key • 120AH - GISKE mode for Double/Triple Length Key (including KEY Block Header, Master Key, and MAC) See *GISKE Key Block Specification* VPN - 22986.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 126 characters, minimum 22 characters			

Example

```
<SI> 02 0 0123456789ABCDEF <SO>{LRC}
```

This packet loads master key 0123456789ABCDEF into master key memory location 0.

Protocol

Controller	Transmission Direction	PINpad
02 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect
	<------	02 packet echo
ACK if LRC and key echo ok NAK if LRC incorrect (EOT after 3 NAKs) EOT if LRC correct but key echo incorrect	------>	PINpad stores new master key only upon receipt of ACK. EOT terminates session.
	<------	EOT

Key Characteristics

This section describes the details of PINpad Key Attributes, Key Version and Key Length.

Key Attributes

On erasure, a master key's usage attribute is set to 0, version is set to 0, and length set to 1DES.

NOTE

Each key has it's own Key Attribute Register, Key Version Register and Key Length Register.

Key Attributes Registers	Comments
[XX]	Value – Definition • 'AN' – ANY * • 'K0' – Key Encryption or Wrapping • 'G0' – MAC Generation • 'M0' – MAC Verification • 'P0' – Pin Encryption • '00' = ISO 9797-1, MAC Algorithm 1 – 56 bits • '10' = ISO 9797-1, MAC Algorithm 1 – 112 bits • '20' = ISO 9797-1, MAC Algorithm 2 – 112 bits • '30'= ISO 9797-1, MAC Algorithm 3 – 112 bits • '40'= ISO 9797-1, MAC Algorithm 4 – 112 bits • '50'= ISO 9797-1, MAC Algorithm 5 – 56 bits • '60'= ISO 9797-1, MAC Algorithm 5 – 112 bits **Note:** The original GISKE (ASCII-Hex) Key Usage Attribute value is saved in the RAM (2bytes). **Note:** ANY means that Key is available in PINpad, but the Key was not loaded using GISKE format.

NOTE

These Key Attributes Registers details apply to 1DES master key, 3DES master key (GISKE), and KLK (GISKE).

Key Length

Length	Comments
1DES	Single length key, Key Length Register = 00
3DES	Double length key, Key Length Register = 01
3-Key 3DES	Triple length key, Key Length Register = 10
Reserved	11

Key Version

The version of an incoming GISKE format key must be greater than or equal to the version set in the key attribute table for all keys (e.g.: 1DES master key, 3DES master key (GISKE) and KLK (GISKE)).

Summary of Rules – GISKE Key version:

- If the Key Version of the New Key is greater than or equal to the Current Key Version, then OK – the PINpad updates the new key.
- If the Key Version of the New Key is less than the Current Key Version, then Error – the PINpad rejects the new key.

NOTE

This key version comparison is only carried out to the key that is replacing, not to any other keys.

KLK

GISKE KLK is loaded in clear if KLK is not currently present in the PINpad. The following rules apply:

- The version of the incoming key is not checked.
- The version of the stored key is the version carried in the message.
- The stored key attribute will be set to that carried by GISKE which should be ‘K0.’

GISKE KLK is loaded in cipher text if KLK attribute in storage location is ‘K0’ and KLK present flag in the PINpad is set. The new GISKE KLK load is protected by the previous GISKE KLK. The following rules apply:

- The current and new KLK key must be a double length key.
- The version of the key is checked against the stored version.
- The version of the stored key is the version carried in the message.
- The stored key usage attribute will be set to that carried by GISKE which should be ‘K0.’

<table>
<tr><th>Summary of Rules</th><th colspan="4">KLK present</th><th>KLK not present</th></tr>
<tr><td>Loading clear text KLK</td><td colspan="4">Error – PINpad returns error message</td><td>Ok – PINpad stores first KLK.</td></tr>
<tr><td rowspan="6">Loading cipher text KLK</td><td></td><td colspan="3">Response</td><td rowspan="6">Error – PINpad returns error message</td></tr>
<tr><td>NOT encrypted with previous KLK</td><td colspan="3">Error – PINpad returns error message</td></tr>
<tr><td rowspan="5">Encrypted with previous KLK</td><td></td><td colspan="2">Response</td></tr>
<tr><td>Incorrect key version</td><td colspan="2">Error – PINpad returns error message</td></tr>
<tr><td rowspan="3">Correct key version</td><td></td><td>Response</td></tr>
<tr><td>Key Attribute <> “KEK”</td><td>Error - PINpad returns error message</td></tr>
<tr><td>Key Attribute = “KEK”</td><td>PINpad store KLK & it’s attributes</td></tr>
</table>

3DES

All 3DES key loads will be in GISKE format. No existing unit uses 3DES mode, therefore there is no backward compatible issue here.

3DES master keys will be loaded in clear text without cryptographic protection if KLK present flag is clear in the PINpad. The MAC value will be all zero bytes. The following rules apply:

- The version of the incoming key is not checked.
- The version of the stored key is the version carried in the GISKE message.
- The stored key attribute will be set to that carried by GISKE.

3DES master keys will be loaded in cipher text under protection of KLK if KLK present flag is set. The following rules apply:

- The KLK must be 3DES.
- The version of the key is checked against the stored version.
- The version of the stored key is the version carried in the message.
- The stored key usage attribute will be set to that carried by GISKE.

<table>
<tr><th>Summary of Rules –
3DES master key loading</th><th colspan="2">KLK is loaded
(current key attribute register in PINpad = GISKE format)</th><th>KLK is NOT loaded
(PINpad KLK present flag is clear)</th></tr>
<tr><td>Clear text 3DES Master Key loading</td><td colspan="2">Error – PINpad returns error message</td><td>PINpad stored 3DES Key</td></tr>
<tr><td rowspan="3">Cipher text 3DES Master Key loading</td><td></td><td>Response</td><td rowspan="3">Error – PINpad returns error message</td></tr>
<tr><td>Incorrect key version</td><td>Error - PINpad returns error message</td></tr>
<tr><td>Correct key version</td><td>PINpad decrypts & stores 3DES Key
Master Key Attribute = GISKE format
Length = 3DES</td></tr>
</table>

1DES

1DES master keys loaded in short-form method will have the ‘ANY’ and 1DES attributes set.

1DES master keys in GISKE format will be loaded in GISKE clear text without cryptographic protection if KLK present flag is clear in the PINpad. The MAC value will be all zero bytes.

The following rules apply:

- The version of the incoming key is not checked.
- The version of the stored key is the version carried in the GISKE message.
- The stored key attribute will be set to that carried by GISKE.

1DES master keys in GISKE format will be loaded in cipher text under protection of KLK if KLK present flag is set. The following rules apply:

- The KLK master key must be 3DES.
- The version of the key is checked against the stored version.
- The version of the stored key is the version carried in the message.
- The stored key attribute will be set to that carried by GISKE.

Master Key Addressing

The range is 0-9.

Key Length information associated with each key is used to identify whether the a key is a single/double/triple length key).

Communication Protocol - Key-only Format

Each key stored in the PINpad contains its own key attributes. However, this is information is not available when key is loaded using the key-only format (as comparing to the GISKE communication protocol). Therefore, the PINpad sets the following default attributes to the key:

Key Attributes	Value	Hex	Definition
Key Usage	'AN'	0x41, 0x4E	Any, no special restrictions
Key Algorithm	'D'	0x44	DES
Key Mode of Use	'N'	0x4E	No special restrictions
Key Version	'00'	0x30, 0x30	version = zero
Key Length	'1'	0x31	single length key

The single-DES communication protocol between Master Device and PINpad is described below.

Controller	Transmission Direction	PINpad
request packet: `<SI>02[n][hhhhhhhhhhhhhhhh]<SO>{LRC}`	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	response packet: `<SI>02[n][hhhhhhhhhhhhhhhh]<SO>{LRC}`
ACK = LRC OK, and key echo OK NAK = LRC incorrect (EOT after 3 NAKs) EOT if LRC correct but key echo is incorrect	------>	The PINpad saves new master key ONLY upon receipt of ACK. EOT terminates the entire session.
	<------	EOT

Sample Packet of Key-only Format

```
<SI>0200123456789ABCDEF<SO>{LRC}
```

This sample packet requests the PINpad to load master key 0123456789ABCDEF into location '0'.

Communication Protocol - GISKE Key Block Format

The 3DES communication protocol between Master Device and PINpad is documented in the following section.

Sample Packet of GISKE Key Block Format

```
<SI>0200123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF01
23456789ABCDEF0123456789ABCDEF012345678901234567890123<SO>{LRC}
```

This sample packet requests the PINpad to load GISKE Key Block (120 bytes, shown below) to address [0].

GISKE Key Block:

```
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF012345678
9ABCDEF0123456789ABCDEF012345678901234567890123
```

Response Format

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
02	packet type	2	Transfer Master Key
[r]	packet parameter	1	Response Code [0 – 9] • 0 – No Error • 1 – Error, PINpad in incorrect KMM (for details, see Rules of Key Management Switching) • 2 – Error, incorrect Key Usage / Mode of Use / Algorithm / Key Length • 3 – Error, version error • 4 – Error, KLK already exists, new KLK is not encrypted from the previous KLK • 5 – Error, GISKE decryption/MAC error. • 6 – Error (This error is not applicable to the PINpad 1000SE). • 7 – Error, Inappropriate Master key addressing.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example Response

```
<SI> 02 0 <SO>{LRC}
```

Communication Protocol

Controller	Transmission Direction	PINpad
request packet: `<SI>02[r][hhh.hhh]<SO>{LRC}`	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	response packet: `<SI>02[r]<SO>{LRC}`
ACK = LRC OK, No error, and key echo OK NAK = LRC incorrect (EOT after 3 NAKs) EOT if LRC correct but key echo is incorrect	------>	The PINpad saves new master key ONLY upon receipt of ACK. EOT terminates the entire session.
	<------	EOT

04 Check Master Key

Verifies if the PINpad device has a master key already stored in a specific master key memory location.

Category Interactive Diagnostic Test

Comments The controller sends the request packet to verify if a master key is in a specific location. The PINpad device checks the key address and sends a response packet back to the controller indicating whether there is or is not a resident master key in that memory location. The PINpad unit has 10 master key memory locations. Use Packet 04 before sending new keys to prevent the accidental overwriting of a master key.

Packet 04 has two types of communication format:

- Key-only Format
- GISKE Key Block Format

The communication format depends on the PINpad Key Management setting and length of the key at [address]. The usage of the communication protocol is described in following table.

PINpad Key Management Setting	Key Length at [address]	Communication Protocol Used
1DES mode	1DES (single length key)	Key-only Format
	3DES (single/ double/triple length key)	GISKE Key Block Format **Note:** If a single/double/triple length key stored in the PINpad contains the Key Attributes information, then the Master Device will understand the GISKE Key Block Format communications protocol.
Mixed or 3DES mode	1DES (single length key)	GISKE Key Block Format
	3DES (double/triple length key)	GISKE Key Block Format

The formats for both the request to the PINpad unit and the response from the PINpad unit are shown below.

NOTE

This option is disabled when the PINpad unit is set for DUKPT.

Request Format

```
<SI> 04 [address] <SO>{LRC}
```

Request Format Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
04	packet	2	Master Key Check
[address]	packet parameter	1	Master Key Address Range: 0-9 KLK address: F
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Key-only Format Response Format

```
<SI> 04 [response code] <SO>{LRC}
```

Key-only Format Response Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
04	packet type	2	Master Key Check
[response]	packet parameter	1	Response Code Range: • 0 = No Master Key at address • F = Master Key at address
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Key-only Format Examples

```
<SI> 045 <SO>{LRC}
```

Packet requests the PINpad device check for the presence of a master key at its master key Memory Location 5.

```
<SI> 040 <SO>{LRC}
```

Response packet indicates memory location doesn't contain master key (0).

```
<SI> 04F <SO>{LRC}
```

This response packet indicates the memory location contains master key (F).

GISKE Key Block Format Response Format

```
<SI> 04 [r] [kua] [a] [MOUA] [kv] [kl] <SO>{LRC}
```

GISKE Key Block Format Response Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
04	packet	2	Master Key Check
[r]	packet parameter	1	Response Code • 0 - No Master Key at [address] • F - Master Key present at [address]
[kua]	packet parameter	2	Key Usage Attribute (optional); used only if Master Key Present at address [a] *Value – Definition* • 'AN' – ANY * • 'K0' – Key Encryption or Wrapping • 'G0' – MAC Generation • 'M0' – MAC Verification • 'P0' – Pin Encryption • '00' = ISO 9797-1, MAC Algorithm 1 – 56 bits • '10' = ISO 9797-1, MAC Algorithm 1 – 112 bits • '20' = ISO 9797-1, MAC Algorithm 2 – 112 bits • '30'= ISO 9797-1, MAC Algorithm 3 – 112 bits • '40'= ISO 9797-1, MAC Algorithm 4 – 112 bits • '50'= ISO 9797-1, MAC Algorithm 5 – 56 bits • '60'= ISO 9797-1, MAC Algorithm 5 – 112 bits **Note:** The original GISKE (ASCII-Hex) Key Usage Attribute value is saved in the RAM (2bytes). **Note:** ANY means that Key is available in the PINpad, but the Key was not loaded using GISKE format.
[a]	packet parameter	1	Algorithm Attribute (optional); used only if Master Key Present at address [a] *Value* *Definition* *[value stored in Key Attributes register]* • 'D' DES [0] • Reserved [1] • Reserved [2] • Reserved [3] • 'T' TDES [4] • Reserved [5] ~ [F]

Type	Field	Length	Description
[MOUA]	packet parameter	1	Mode of Use Attribute (optional); used only if Master Key Present at address [a] *Value* *Definition* *[value stored in Key Attributes register]* • 'N' No special restrictions [0] • 'E' Encryption only [1] • 'D' Decryption only [2] • Reserved [3] • '0' IV [4] • 'G' MAC Generate [5] • 'V' MAC Verify [6] • 'C' Calculate = generate or verify [7] • Reserved [8] ~ [F]
[kv]	packet parameter	2	Key Version (optional); used only if Master Key Present at address [a] [kv] is a two-digit ASCII character version number, optionally used to prevent re-injection of old keys. If not used, this field is normally filled with ASCII '0' (0x30). **Note:** The PINpad allocates 1 byte (per key) for each key version register.
[kl]	packet parameter	1	Key Length (optional); used only if Master Key Present at address [a] Key Lengths can be: • "1" - single length key • "2" - double length key • "3" - triple length key **Note:** The PINpad allocates 1 byte (per key) for each key version register.
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 13 characters, minimum 13 characters			

NOTE

To save storage space in RAM, both the Algorithm Attribute and the Mode of Use Attribute are individually converted to [x], a Hex number ranging form 0 ~ F (4 bits). In the response packet, the PINpad converts the each attribute number back to characters used in GISKE specification.

Protocol

Controller	Transmission Direction	PINpad
04 request packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	PINpad checks requested memory location for 04 response packet
		04 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT

08 Select Master Key

Selects one of the 10 possible master keys (0-9) stored in the PINpad master key memory locations.

NOTE

This option is disabled when the PINpad unit is set for DUKPT.

Category Interactive Diagnostic Test

Comments The master device sends this packet to the PINpad to select one of the ten possible master keys (0-9). VeriFone recommends that the controlling device always send this packet first before sending a packet requesting PIN entry (70/Z60/Z62).

VeriFone recommends that the master device should always send this packet first before sending a packet (e.g. Packet 70) to request PIN entry.

Packet Format `<SI> 08 [address] <SO>{LRC}`

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
08	packet type	2	Select Master Key
[address]	packet parameter	1	Master Key address Range: 0-9
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example `<SI> 08 7 <SO>{LRC}`

Selects master key 7.

Protocol

Controller	Transmission Direction	PINpad
08 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
		PINpad makes selected master key current
		No response, if incorrect Master Key is selected (see Note).
	<------	EOT

NOTE

If Master Key address does not contain any key, the PINpad will still set the currently selected key as the active master key due to the backward compatibility requirements. Functions requiring the usage of the "empty" active master key are responsible to carry out the error code response

70 Request PIN Entry

Causes the PINpad to cycle the display through the following prompts until a PIN is entered:

```
TOTAL
$xxxx.xx (Amount of sale from the controller)
ENTER PIN
PUSH "ENTER"
```

Category Standard Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments After cycling through the display messages and receiving entry of a PIN, the PINpad alternately displays the following two lines until the [CLEAR] key is entered or another packet is sent to the PINpad.

```
PROCESSING
PIN PAD
```

If the PINpad device is set as DUKPT, this message packet has been redefined.

See DUKPT Message Packets for details of redefinitions.

The PINpad device will only execute message 72 Cancel Session Request, while it waits for the customer's PIN entry. Any message packets requesting a PINpad display (e.g., Z2, Display A String) must precede Packet 70 in order for the message to be displayed before PIN entry.

Packet Format

```
<STX> 70.[account#] <FS> [working key] [amount] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
70	packet type	2	Request PIN Entry
.	hexadecimal	1	Command Delimiter; period: '.' Hex value: '2Eh'
[account#]	packet parameter	8-19	Card account number
<FS>	packet parameter	1	Field separator; Value: `1Ch'

Type	Field	Length	Description

[working key]	packet parameter	16 or 120	[working key] - encrypted working key (encrypted session key)
			The size of the [working key] indicates which packet format is used.
			• 16AH - 1DES mode for single length key
			  • If Zero Key Support is enabled, and if the encrypted working key is all zero-filled, the currently selected master key will be used as the working key.
			  • If Zero Key Support mode is disabled, the passed key is used regardless of the encrypted key value.
			• 120AH - 3DES mode for Double/Triple Length Key (including KEY Block Header, Master Key, and MAC) with Empty GISKE Session Key Support. See *GISKE Key Block Specification* VPN - 22986.

[amount]	packet parameter	3-7	The amount to be displayed on the PINpad including implicit decimal point
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 153 characters, minimum 34 characters			

NOTE

Zero Key Support and Empty GISKE Session Key Support are controlled by a switch in the Key Management Option register which is set using 17 Set Key Management Mode, and checked using 18 Check Key Management Options Register Mode.

Example

```
<STX> 70. 0123456789012345678 <FS> 01234567891234569.99 <ETX>{LRC}
```

This packet contains an account number of 0123456789012345678, a working key of 0123456789123456, and an amount of $9.99.

Protocol

The communication protocol sequence is included under the 71 Transfer PIN Block communication protocol.

71 Transfer PIN Block

Encrypts and sends the customer-entered PIN block to the controller.

Category Standard Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments In PINpad 1000 mode, the PINpad sends this packet in response to the request packets 70 Request PIN Entry, Z60 Accept and Encrypt PIN, and Z62 Accept and Encrypt PIN, Display Custom Messages.

If the PINpad device is set as DUKPT, this message packet has been redefined.

See DUKPT Message Packets for details of redefinitions.

After a Packet 71 is sent to the controller, the PINpad waits for an ACK, then re-initializes variables. Therefore, the delay between the ACK and the next message packet (e.g., Z2, Display A String) should be 5ms.

Packet Format

```
<STX> 71.[func key] [pin length] [01] [pin] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
71	packet	2	Transfer PIN Block
.	hexadecimal	1	Command Delimiter; period: '.' Hex value: '2Eh'
[func key]	packet parameter	1	Value is 0 Function key feature not implemented.
[pin length]	packet parameter	2	PIN length; range is 00, 04-12
[01]	packet parameter	2	Format of PIN block before encryption; value is `01'
[pin]	packet parameter	16	64-bit encrypted PIN block represented as 16 hex digits Length is 0 if null PIN is entered.
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 27 characters, minimum 27 characters

Example

```
<STX> 71. 0 12 01 0123456789101112 <ETX>{LRC}
```

This message packet indicates that the PIN length is 12.

If there is an error, the error message is shown on the PINpad LCD. Details of the PINpad LCD error messages are shown in Prompts and Error Messages.

Protocols

Packet 70

Controller	Transmission Direction	PINpad
70 packet	------>	
		ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
		Cycles through these messages:
		TOTAL $xxxx.xx ENTER PIN PUSH "ENTER"
	<------	
		Customer enters PIN
		PINpad displays "*" characters in echo to customer keystrokes.
	<------	Packet 71
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	Alternately display: PROCESSING PIN PAD

Packet Z60

Controller	Transmission Direction	PINpad
Packet Z60	------>	
		ACK = LRC OK
		NAK = LRC incorrect
	<------	(EOT after 3 NAKs)
		Customer enters PIN
		PINpad displays "*" characters in echo to customer keystrokes.
	<------	Packet 71
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
		Alternately display:
		PROCESSING PIN PAD

Packet Z62

Controller	Transmission Direction	PINpad
Packet Z62	------>	
		ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	Alternates the Z62-specified messages.
		Customer enters PIN
		PINpad displays "*" characters in echo to customer keystrokes.
	<------	Packet 71
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
		Displays the Z62-specified messages.

Z60 Accept and Encrypt PIN

Directs the PINpad device to accept the customer PIN, create and encrypt the PIN block and transmit it to the controller.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet must be preceded by a display packet, such as Packet Z2 or Z3, that requests the customer's PIN number, and also be followed by the PIN transmittal Packet 71.

Upon receipt of this packet and the customer PIN number, the PINpad forms a formatted clear-text PIN block, based on the customer account number and PIN number, and encrypts this formatted clear-text PIN block to obtain a cipher-text PIN block to send to the master device via Packet 71 (refer to VISA PIN Processing Specifications, version 2.0, 3/1988).

PIN entry is limited to a minimum of 4 digits and a maximum of 12 digits; null entry is not allowed.

If the PINpad device is set as DUKPT, this message packet has been redefined.

See DUKPT Message Packets for details of redefinitions.

Packet Format

```
<STX> Z60. [account] <FS> [working key] <ETX> {LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z60	packet	3	Accept and Encrypt PIN
.	delimiter	1	Command Delimiter; period: '.' Hex value: '2Eh'
[account]	packet parameter	8-19	Card Account Number
<FS>	packet parameter	1	Field separator

Type	Field	Length	Description

[working key]	packet parameter	16 or 120	[working key] - encrypted working key (encrypted session key)
			The size of the [working key] indicates which packet format is used.
			• 16AH - 1DES mode for single length key
			  • If Zero Key Support is enabled, and if the encrypted working key is all zero-filled, the currently selected master key will be used as the working key.
			  • If Zero Key Support mode is disabled, the passed key is used regardless of the encrypted key value.
			• 120AH - 3DES mode for Double/Triple Length Key (including KEY Block Header, Master Key, and MAC) with Empty GISKE Session Key Support. See *GISKE Key Block Specification* VPN - 22986.

<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 147 characters, minimum 32 characters			

Zero Key Support and Empty GISKE Session Key Support are controlled by a switch in the Key Management Option register which is set using 17 Set Key Management Mode, and checked using 18 Check Key Management Options Register Mode.

Example

```
<STX> Z60.0123456789012345678 <FS> 0123456789123456 <ETX>{LRC}
```

This packet contains an account number of 0123456789012345678 and a working key of 0123456789123456.

Protocol

The communication protocol sequence is included under the 71 Transfer PIN Block communication protocol.

Z62 Accept and Encrypt PIN, Display Custom Messages

Directs the PINpad device to alternate up to two messages, accept customer PIN, create and encrypt the PIN block, then display the specified processing message after transmitting the PIN block to the controller.

Category Custom Communication Packet

Comments The PINpad echoes the customer PIN entry with asterisks on the display.

Packet Z62 adds the capability to specify up to two display messages or prompts before PIN entry, specify the PIN length, allow null PIN entry, and specify display processing message after the PIN entry.

NOTE

The User Definable Character (UDC) function is supported in this packet for [message1], [message2], and [process msg]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

NOTE

If the PINpad device is set as DUKPT, this message packet has been redefined.

See DUKPT Message Packets for details of redefinitions.

Packet Format

```
<STX> Z62.[account#] <FS> [working key] [min pin] [max pin] [null flag]
[message1] <FS> [message2] <FS> [process msg] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z62	packet type	3	Encrypt PIN/Display Custom Messages
.	delimiter	1	Command Delimiter; period: '.' Hex value: '2Eh'
[account]	numeric	8-19	Card account number
<FS>	field separator	1	Field separator

Type	Field	Length	Description

[working key]	packet parameter	16 or 120	[working key] - encrypted working key (encrypted session key)
			The size of the [working key] indicates which packet format is used.
			• 16AH - 1DES mode for single length key
			  • If Zero Key Support is enabled, and if the encrypted working key is all zero-filled, the currently selected master key will be used as the working key.
			  • If Zero Key Support mode is disabled, the passed key is used regardless of the encrypted key value.
			• 120AH - 3DES mode for Double/Triple Length Key (including KEY Block Header, Master Key, and MAC) with Empty GISKE Session Key Support. See *GISKE Key Block Specification* VPN - 22986.

[min pin]	packet parameter	2	Minimum Acceptable PIN length; Range is 04-12
[max pin]	packet parameter	2	Maximum Acceptable PIN length; Range is 04-12
[null flag]	packet parameter	1	Null PIN status: • Y = Null PINs allowed • N = Null PINs not allowed
[message1]	packet parameter	0-16	Message to alternate with [message2] until customer presses key (UDC function is supported in this packet)
<FS>	field separator	1	Field separator. Optional, only present when next message follows
[message2]	packet parameter	0-16	Message to alternate with [message1] until customer presses key (UDC function is supported in this packet)
<FS>	field separator	1	Field separator. Optional, only present when next message follows
[process msg]	packet parameter	0-16	Processing message displayed after PIN entry
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 255 characters, minimum 39 characters

NOTE

The User Definable Character (UDC) function is supported in this packet for [message1], [message2], and [process msg]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

NOTE

Zero Key Support and Empty GISKE Session Key Support are controlled by a switch in the Key Management Option register which is set using 17 Set Key Management Mode, and checked using 18 Check Key Management Options Register Mode.

Examples

```
<STX> Z62. 4000000000006 <FS> 0123456789ABCDEF 04 12 Y THANKYOU<FS>
PLEASE ENTER PIN <FS> PLEASE WAIT <ETX>{LRC}
```

Upon receipt of this packet, the PINpad alternately displays THANKYOU and PLEASE ENTER PIN until the customer presses the first key. The customer can skip entering the PIN (nulls allowed) by pressing [ENTER]. Otherwise, the PIN entry must be four to twelve digits long. After PIN entry, until the master device responses to the Packet 71 (such as, an <ACK>) in response to the encryption block, the PINpad displays PLEASE WAIT.

```
<STX> Z62. 4000000000006 <FS> 0123456789ABCDEF 06 08 N <FS>
MESSAGE2 <FS> PROCESSING <ETX>{LRC}
```

Upon receipt of this packet, the PINpad alternately displays ‘blank’ (MESSAGE1) and MESSAGE2 until the customer enters a 6-8 digit PIN number, followed by the ENTER key, with no null PIN entry allowed. After PIN entry, until the master device responses to the Packet 71 (such as, an <ACK>) in response to the encryption block, the PINpad displays PROCESSINGMSG.

NOTE

The Rev. 0l and earlier PP101 won't display "blank" for example 2.

```
<STX> Z62. 4000000000006 <FS> 0123456789ABCDEF 06 08 N MESSAGE1<ETX>{LRC}
```

Upon receipt of this packet, the PINpad displays MESSAGE1 (with no alternating message) until the customer enters a 6-8 digit PIN number, followed by the ENTER key, with no null PIN entry allowed. After PIN entry, until the master device responses to the Packet 71 (such as, an <ACK>) in response to the encryption block, the PINpad displays a blank screen processing message.

Protocol

The communication protocol sequence is included under the 71 Transfer PIN Block communication protocol.

MAC Packets

This section describes the master-session MAC generation of message packets by the PINpad 1000SE device.

Preauthorization Packets

Message	Description
Z66	Z66 Request MAC
Z67	Z67 Return MAC

There are two kinds of MAC algorithms to be used. One is ANSI (Standard - ANSI is the industry standard) and another is BPI (Customer - BPI, Bank of Philippine Islands, is the customer's name; this algorithm is specified by BPI).

Z66 Request MAC

Directs the PINpad device to generate the Message Authentication Code (MAC) of the current packet.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet is used by the master device to direct the PINpad to generate the MAC of the current packet. If it is the first Z66 packet, the PINpad starts the MAC generation. If it is the last Z66 packet, the PINpad completes the MAC calculation from the current packet and returns the MAC to the master device with a Z67 packet. Otherwise, the PINpad calculates the MAC from the current packet and keeps it in memory.

VeriFone imposes the following size rules on the [message for MAC] field.

Packet Type	Size of X	Maximum Message Size	Apply to Message Sequence	Comments
Key-only Format mode	• ASCII: X = 0, 1, 2 – 27, 28 • Binary: X = 0, 2, 4 – 26, 28	224 bytes 224 bytes	00 – 99	
GISKE Key Block Format mode	• ASCII: X = 0, 1, 2 – 14, 15 • Binary: X = 0, 2, 4 – 12, 14	120 bytes 112 bytes	00 – 99	Due to of the size of GISKE Key Block, the size of message is reducing to 120 bytes.

Packet Format

```
<STX> Z66[packet flag] [sequence no.] [master key pointer] <FS> [working key] <FS> [second key] <FS> [message for MAC] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z66	message	3	Request MAC
[packet flag]	message parameter	1	Packet flags identify whether the packet uses BPI or ANSI algorithm, whether the data is ASCII or binary, as well as packet position. • 0 = BPI-specific, ASCII, last packet • 1 = BPI-specific, ASCII, first/middle packet • 2 = BPI-specific, binary, last packet • 3 = BPI-specific, binary, first/middle packet • 4 = ANSI standard, ASCII, last packet • 5 = ANSI standard, ASCII, first/middle packet • 6 = ANSI standard, binary, last packet • 7 = ANSI standard, binary, first/middle packet
[sequence #]	numeric	2	Range: 00-99
[master key pointer]	numeric	1	Optional; Range: 0-9
<FS>	message parameter	1	Field separator
[working key]	message parameter	16 or 120	Optional when PINpad is in PP1000 mode • 16AH - 1DES mode for single length key • 120AH - GISKE mode for Double/Triple Length Key. See *GISKE Key Block Specification* VPN - 22986.
<FS>	message parameter	1	Field separator
[second key]	numeric	1	Optional Second Master Key Pointer; Range: 0-9
<FS>	message parameter	1	Field separator
[message for MAC]	message parameter	0-64 8*X	ASCII message or ASCII-coded Binary data • For ASCII data, X= 0 - 28 • For Binary data, X= 0, 2, 4, 6,..., 26, 28 (See Notes and Remark, below, for detail)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 255 characters, minimum 12 characters			

Example

```
<STX> Z66 3 00 2 <FS> 0123456789123456 <FS> <FS> 0123456789ABCDEF <ETX>{LRC}
```

NOTE

1. For PINpad 1000 and PINpad 1000SE modes, there is no limit on the number of packets. The packet sequence increments the numeric sequence counter inside the packet for the first 100 packets, 0-99, and then keeps sending the 99 numeric sequence counter, with no errors. Thus, a 103-packet sequence would cycle through the following counters: 0, 1, 2, 3, 4, 5... 97, 98, 99, 99, 99, 99.
2. 8*X in [message for MAC] represents the number of 8-byte (or character) blocks. For ASCII data, all values of X from 0 - 28 are allowed. For Binary data, only 0, 2, 4, 6,...., 26, 28 are permitted. (X = 2 * N, where N = 0 to 14). For example,
   - X = 0 - no message data
   - X = 1 - 8 bytes of message data
   - X = 2 - 16 bytes of message data
   - X = 3 - 24 bytes of message data
   - ...
   - X = 27 - 216 bytes of message data
   - X = 28 - 224 bytes of message data

   For Binary data, only 0, 2, 4, 6,...., 26, 28 are permitted. (X = 2 * N, where N = 0 to 14).

   Do not use ASCII messages for Mac-ing that include ETX(0x03)or SO(0x0E). These can't use these combinations in the [message] because they are reserved control characters that will trigger control functions
3. If the length of [message for MAC] is not multiple of 8 in the final Z66 packet, then the PINpad will automatically pad it with zeros (ASCII 30h) internally.
4. An example of 8 bytes data block for an ASCII message "AMT$1.99" is "414D5424312E3939".
5. ASCII-coded binary message is two HEX digits represent a byte value, like above conversion result.
6. If the Working Key is loaded in 1DES Key-only Format, either ANSI (standard) MAC or BPI (customer's) MAC is used (which is depending on the status of the flag in the Z66 packet).
7. If the Working Key is loaded in the GISKE format, the PINpad uses the MAC algorithm that is specified in the Key Usage Attributes of GISKE key block.
8. When the Key Length and the MAC Algorithm do not match, an error code (key attribute / usage error) is returned. Example: a single length key is used with a 3DES MAC algorithm.
9. MAC Algorithms used: ISO 9797-1 MAC Algorithm 1 - 56 bits, MAC Algorithm 1 - 112 bits, MAC Algorithm 2 - 112 bits, MAC Algorithm 3 - 112 bits, MAC Algorithm 4 - 112 bits, MAC Algorithm 5 - 56 bits, MAC Algorithm 5 - 112 bits.
10. The GISKE working key can only be a single or double length key. Master key used to encrypt the working key can be a single, double or triple length key (GISKE Length Encryption Rule still applied here). If a triple length GISKE working key is used in Z66, the work key error is returned.
11. The GISKE working key can not be used in BPI MAC request, because the MAC algorithm used by the BPI is not part of the ANSI ISO MAC Standard. Working Key Error is returned if BPI MAC-Request uses GISKE working key.

Protocol

The communication protocol sequence is included in Message Authentication Code (MAC) under Z66/Z67 Protocol, with examples for both Normal Condition and Error Condition.

Z67 Return MAC

Signals the controller in response to Z66 Request MAC.

Category Custom Communications Packet

Comments Packet Z67 sends three types of messages to the controller:

- A signal that the PINpad is ready for the next Z66 packet
- An error code if there is any error during the MAC session
- The MAC value

Packet Format

```
<STX> Z67[process code] [MAC field] <ETX>{LRC}
```

Elements

Packet	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z67	message	3	Return MAC
[process code]	message parameter	1	Process Code; Range: 0-9 • 0 = no error and MAC follows • 1 = ready for next Z66 packet and no MAC follows • 2 = out-of-order error and no MAC follows • 3 = [pointer] error and no MAC follows • 4 = [second key] error and no MAC follows • 5 = packet frame error and no MAC follows • 6 = [flag] error • 7 = [message] error • 8 = [working key] error / GISKE Key Usage, Algorithm, Mode of Use or Key Length Error • 9 = incorrect key attributes of the master key (first or second)
MAC field	message parameter	16	Optional MAC Value, only sent when no error
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 23 characters, minimum 7 characters

Example

```
<STX> Z671 <ETX>{LRC}
```

Ready for next Z66 packet; no MAC follows.

Protocol

The communication protocol sequence is included in Message Authentication Code (MAC) under Z66/Z67 Protocol, with examples for both Normal Condition and Error Condition.

Message Authentication Code (MAC)

The Message Authentication Code (MAC) module operates in conjunction with custom communication packets Z66 Request MAC and Z67 Return MAC and is used between the PINpad device and controller. MAC-ing is supported when the PINpad is set as "Master/Session" or master and DUKPT. MAC utilizes some techniques of DES to ensure that the message sent is an authentic message and has not been fraudulently changed.

The algorithm used to calculate the MAC is fully compatible with the ANSI X9.19 standard, based on Financial Institution Retail Message Authentication. There are two modes of operation within this standard:

- Cipher Block Chaining (CBC)
- 64-bit Cipher Feedback (CFB-64)

The Cipher Block Chaining (CBC) mode of operation is used for MAC calculation in PINpad device implementation.

ANSI (Standard) MAC Algorithms

The algorithm used to calculate the MAC is fully compatible with ANSI X9.19 1986 (ANSI 1DES MAC), Financial Institution Retail Message Authentication. Within this standard, there are two modes of operation, Cipher Block Chaining (CBC) and 64 bit Cipher Feedback (CFB-64). In the PINpad 1000SE implementation, the Cipher Block Chaining (CBC) will be used for MAC calculation.

The master key and the working key for MAC calculation can be downloaded with Packet Z66 if necessary. The selection of these keys depends on the first Z66 packet configurations within each MAC session, they are summarized as following:

[pointer]	[working key]	Selection
present	present	Master key selected by the [pointer] is used to decrypt the working key.
present	absence	Master key selected by [pointer] is used as the working key. • PP1000SE mode: Working key is no longer optional due to security concerns. • PP1000 mode: Working key can be an optional entry
absence	present	Current active master key is used to decrypt the working key.
absence	absence	Current Active Master Key is used as the working key. • PP1000SE mode: Working key is no longer optional due to security concerns. • PP1000 mode: Working key can be an optional entry

After the MAC calculation, there is one more optional procedure that can be used for increased protection against exhaustive key determination. This operational procedure can be turned on or off by the second key field of the initial Z66 packet. If this second key was provided with the initial Z66 packet, the optional procedure generates the final MAC using the second key as the master key pointer. If there is no second key provided, no optional procedure will take place on the current MAC.

NOTE

The second key is used on a session-by-session basis. Each second key field of the initial Z66 packet defines its own optional procedure ON/OFF status during that MAC session. For more details about the MAC optional procedure, refer to Section 2.4.4.5 of the ANSI X9.19 standard.

After the MAC calculation process is complete, a 64-bit MAC is generated. This MAC value will be return to the master device with the Z67 packet. If there is any error during the MAC process session, Packet Z67 will be returned with an error code set in [code].

BPI (Customer) MAC Algorithms

The algorithm used to calculate the MAC is fully compatible with BPI's specification that is summarized as following:

1. The message stream is divided into 64-bit (8byte) block.
2. If the length of the last block is less than 8 bytes, pad it with binary 0 to make it 8 bytes long.
3. EXOR-ed the first block with the second block.
4. EXOR-ed the previous step result with next block.
5. Repeat Step 4 till the last block been EXOR-ed.
6. Encrypt the final result with DES key.
7. The encrypted result is the MAC.

The master key and the working key for MAC calculation can be downloaded with Packet Z66 if necessary. The selection of these keys depends on the first Z66 packet configurations within each MAC session. They are summarized as following:

[pointer]	[working key]	Selection
present	present	Master key selected by the [pointer] is used to decrypt the working key.
present	absence	Master key selected by [pointer] is used as the working key. • PP1000SE mode: Working key is no longer optional due to security concerns. • PP1000 mode: Working key can be an optional entry

[pointer]	[working key]	Selection
absence	present	Current active master key is used to decrypt the working key.
absence	absence	Current Active Master Key is used as the working key. • PP1000SE mode: Working key is no longer optional due to security concerns. • PP1000 mode: Working key can be an optional entry

After the MAC calculation, there is one more optional procedure that can be used for increased protection against exhaustive key determination. This optional procedure can be turn on/off by the [second key] field of the initial Z66 packet. If this second key was provided with the initial Z66 packet, the optional procedure will be taken to generate the final MAC using the [second key] as the master key pointer. If there is no [second key] provided, no optional procedure will be taken on the current MAC. One thing to note is that this [second key] is used on session-by-session basis. Each [second key] field of the initial Z66 packet defines its own optional procedure on/off status during that MAC session. The optional procedures are

1. The master key selected by [second key] will be used to decrypt the MAC result.
2. The previous result is encrypted with original DES key, the result is the final MAC.

After the MAC calculation process is complete, a 64-bit MAC is generated. This MAC value will be return to the controller with the Z67 packet. If there is any error during the MAC process session, Packet Z67 will be returned with an error code set in [code].

MAC Process Session

When the first Z66 packet is received, the PINpad device enters the MAC process session. If this packet is also the last packet, the Z67 packet is returned to the master device and the PINpad reverts back to the non-MAC state and all the MAC working data in memory will be erased. If the Z67 packet is not the last packet, the PINpad calculates the MAC from the current Z66 packet then returns the Z67 packet to signal the master device that the PINpad is ready for next Z66 packet. This MAC process session continues for every Z66 packet received until the last Z66 packet is received. When the last Z66 is received, the PINpad calculates the MAC from this packet and generates and returns the Z67 packet.

NOTE

If any other packet is received during the MAC session, the entire MAC process aborts and no packet is returned. All MAC working data in memory is erased and the newly received packet will be processed normally.

During the MAC process session, all Z66 packets are checked for correct sequence as they are received. The correct sequence should be 00, 01, 02,....,99, with a maximum of one hundred Z66 packets in one MAC session. If any Z66 packet is received out of sequence during a MAC session, that packet is ignored and the PINpad still returns the Z67 packet to signal the master device to send the next Z66 packet. If the last Z66 packet is received out of sequence, no MAC will be generated; the Z67 packet returns to the master device with an "Out of Order" error code, and the PINpad device returns to its idle state.

The following are normal and error condition sequences for a MAC session.

Normal Condition

Controller	Transmission Direction	PINpad
Send first Z66 MAC request	---Z66--->	Receive
Wait		Process
Receive	<---Z67---	Send Ready Packet
Send next Z66 MAC request	---Z66--->	Receive
Wait		Process
Receive	<---Z67---	Send another Ready Packet
...	...	...
Send last Z66 MAC request	---End Z66--->	Receive
Wait		Calculate MAC
Receive	<---Z67---	Send MAC

Error Condition

Controller	Transmission Direction	PINpad
Send first Z66 MAC request	---Z66--->	Receive
Wait		Process
Receive	<---Z67---	Send Ready Packet
Send next Z66 MAC request	---Z66--->	Receive
Wait		Process
Receive	<---Z67---	Send another Ready Packet
...	...	...
Send last Z66 MAC request	---End Z66--->	Receive out of order

Controller	Transmission Direction	PINpad
Wait		Process
Receive	<---Z67---	Send Out of Order Error

Z66/Z67 Protocol

This protocol combines Z66 Request MAC and Z67 Return MAC.

Controller	Transmission Direction	PINpad
Z66 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	Z67 packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		

DUKPT Message Packets

This section discusses the message packets and formats that are supported when the PINpad device is set to DUKPT or Master/Session DUKPT mode. When the unit is set only as "Master/Session," message packets and formats in this section are not supported.

NOTE

The default mode of the PINpad at initial power up is PP1000 mode, MS 1DES mode.

Two DUKPT modes are implemented in the PINpad. The PINpad can run in either 1DES DUKPT mode or 3DES DUKPT mode in each DUKPT Engine.

NOTE

All keys associated with a DUKPT Engine are erased when a DUKPT engine switches between 1DES DUKPT mode and 3DES DUKPT mode.

Multiple DUKPT Engines

The PINpad supports three DUKPT engines. See 19 Select a DUKPT Engine for more details.

The default DUKPT engine is set to "0". DUKPT engine is set to "0" at the start of each power cycle.

DUKPT Overview

Before actual operation, a highly secure module known as a "key loading device" utilizes a derivation key to load a unique initial Key Serial Number (KSN) and a unique initial PIN Encryption Key (PEK) into the PINpad device. The derivation key used to encrypt the initial KSN may also be used for thousands of PINpad loads. An encryption counter incorporated in the key-loading process is automatically set to zero.

Once the PINpad receives its KSN and PEK, it sets its own encryption counter to zero. During the generation of each encrypted PIN block, the PINpad unit outputs the current serial number (a concatenation of the initial KSN and the encryption counter). This produces a new encryption key utilized to encrypt the PIN entry and create the PIN block for each transaction.

Encryption during a transaction occurs as follows:

1. The controller sends an account number to the PINpad, then the PINpad device requests and receives PIN entry via the keyboard.
2. The PINpad device generates the clear-text PIN block using the account number and PIN.
3. Using the generated PEK, based on the encryption counter that is updated after each transaction, the PINpad does a special encryption to the PIN block using the DES algorithm and PEK. The PINpad then sends the encrypted PIN block with current KSN (the concatenation of the initial KSN and the encryption counter) to the controller.
4. The controller then appends the encrypted PIN block and current KSN to a request packet and forwards the completed request packet to the host. While this is occurring, the PINpad performs internal key processing tasks.

Functional Listing of PINpad Messages

The messages sent to and from the PINpad to manipulate operations or control specific PINpad functions are divided into several functional groups. These groups include packets for interactive diagnostic tests, and standard and custom communication.

Interactive Diagnostic Test

Interactive tests between the PINpad and the controller run only upon request. These tests use the VeriFone-defined message Packets 01, 05, 06, 09, 11 and 12 and are listed under Management Packets.

Message	Description
19	19 Select a DUKPT Engine
25	25 Check DUKPT Engine

Preauthorization Packets

Message	Description
60	60 Pre-Authorization: PIN Entry Request
62	62 Pre-Authorization: Transaction Amount Authorization Request
63	63 Pre-Authorization: Transaction Amount Authorization Response
66	66 Pre-Authorization: PIN Entry Test Request

Standard Communication

The standard messages sent between the PINpad unit and the controller follow the VISA message packet format and allow the PINpad to be programmed with standard VISA prompts and control the PINpad display. There is sufficient variation in Packets 70 and 71 to merit specific discussions in this chapter, as well as in the Master/Session Message Packets chapter.

Message	Description
70	70 Request PIN Entry
71	71 Transfer PIN Block
76	76 PIN Entry Test Request

Key Loading Device to PINpad Packets

Message	Description
90	90 Load Initial Key Request
91	91 Load Initial Key Response

Custom Communication

These message packets were created to provide the PINpad with special prompts and data entry requirements for custom applications. The request and response messages pass between the controller and the PINpad, allowing the controller to customize prompts and control PINpad operations. There is sufficient variation in Packets Z60 and Z62 to merit specific discussions in this chapter, as well as in the Master/Session Message Packets chapter.

Message	Description
Z60	Z60 Accept and Encrypt PIN
Z62	Z62 Accept and Encrypt PIN (with Custom Prompts)

19 Select a DUKPT Engine

Selects one of the available DUKPT engines.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

The master device sends this packet to the PINpad to select one of the DUKPT engines ("0", "1", or "2"). VeriFone recommends that the master device should always send this packet first before sending a packet (e.g. Packets 60, 62, 66, 70, 76, 90, 61, 62, etc.) to request for DUKPT function.

NOTE

The default DUKPT engine is set to "0".

Packet Format

```
<SI> 19 [a] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
19	packet type	2	Select a DUKPT Engine
[a]	packet type	1	DUKPT Engine: "0", "1", or "2"
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example

```
<SI> 19 2 <SO>{LRC}
```

Selects second DUKPT engine.

Protocol

Controller	Transmission Direction	PINpad
19 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)
	<------	19 packet echo

Controller	Transmission Direction	PINpad
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
		PINpad selects specified DUKPT engine
	<------	EOT to terminate process

NOTE

If there is any packet format error, PINpad does not echo the response packet back to the master device. Incorrect packet format can include out of range DUKPT engine, incorrect packet type, incorrect packet length, etc.

25 Check DUKPT Engine

Identifies which one of the available DUKPT engines is selected.

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

The master device sends this packet to the PINpad to check the current active DUKPT engines ("0", "1", or "2").

Request Format

```
<SI> 25 <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
25	packet type	2	Check DUKPT Engine
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 5 characters, minimum 5 characters			

Response Format

```
<SI> 25 [a] <SO>{LRC}
```

Elements

Type	Field	Length	Description
<SI>	start of packet	1	ASCII Shift In Control Character; Value: `0Fh'
25	packet type	2	Check DUKPT Engine
[a]	packet type	1	DUKPT Engine: "0", "1", or "2"
<SO>	end of packet character	1	ASCII Shift Out Control Character; Value: `0Eh'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example

```
<SI>25<SO>{LRC}
```

Requests check of DUKPT Engine.

```
<SI>251<SO>{LRC}
```

Responds that DUKPT Engine "1" is active.

Protocol

Controller	Transmission Direction	PINpad
25 request packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		(EOT after 3 NAKs)
	<------	25 response packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	EOT to terminate process

60 Pre-Authorization: PIN Entry Request

Creates and encrypts the PIN block.

Category

Preauthorization packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet is to create and encrypt the PIN block. This packet must be preceded by a display packet such as Packet Z2 or Z3 and followed by the PIN transmittal packet 71. The terminal must then transmit Packet 62 to the PINpad device.

PIN length must be in the range of 4-12 digits. PIN length less than 4 digits is not allowed and results in an error beep. Null PIN entry is not allowed and also results in an error beep.

Packet Format

```
<STX> 60 [primary account#] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
60	packet type	2	PIN Entry Request
[primary account#]	packet parameter	8-19	Card Account Number
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 24 characters, minimum 13 characters			

Example

```
<STX> 60012345678987654321O <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
60 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		User PIN entry; asterisks are displayed.
	<------	Packet 71 with the encrypted PIN block

Controller	Transmission Direction	PINpad
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	
	<------	Alternately display: PROCESSING PIN PAD

62 Pre-Authorization: Transaction Amount Authorization Request

Displays the transaction amount, accepts the authorization code from the card holder through the keypad, and transmits the response 63 Pre-Authorization: Transaction Amount Authorization Response back to the controller.

Category

Preauthorization packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet must be preceded by 60 Pre-Authorization: PIN Entry Request. The transaction amount is displayed along with the following messages:

```
TOTAL

$XXXXX.XX

ENTER Y/9 KEY TO

APPROVE

ENTER N/6 KEY TO

DECLINE
```

After the user presses either the Y/9 or N/6 key, the key is converted into either "0" for approval or "1" for declination.

If the previous PIN entry (via Packet 60) was invalid, a Packet 63 with a decline response code is sent without any message display and the entry request. The amount display is limited to xxxxx.xx format. And the maximum length of [amount] is 7 digits, including the decimal point.

Packet Format

```
<STX> 62 [C/D] [amount] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
62	packet type	2	Transaction Amount Authorization Request
[C/D]	packet parameter	1	Credit/Debit Indicator; Value: '43h/44h'
[amount]	packet parameter	3-7	Transaction Amount; must include decimal point
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 13 characters, minimum 9 characters			

Example

```
<STX> 62C9.99 <ETX>{LRC}
```

The amount in this packet is $9.99 (credit).

Protocol

Controller	Transmission Direction	PINpad
62 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect Display alternately: TOTAL $XXXXX.XX ENTER Y/9 KEY TO APPROVE ENTER N/6 KEY TO DECLINE
	<------	63 packet after user enters the authorization code through the keypad
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	

63 Pre-Authorization: Transaction Amount Authorization Response

Responds to 62 Pre-Authorization: Transaction Amount Authorization Request with either Approval or Declination code.

Category Preauthorization packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments After user enters response code from the keypad, the code will be converted into "0" for approval or "1" for declination.

Packet Format

```
<STX> 63 [code] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
63	packet type	2	Transaction Amount Authorization Response
[code]	packet parameter	1	Response Code: • 0 = Approval • 1 = Declination
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

Example

```
<STX> 630 <ETX>{LRC}
```

Protocol The communication protocol sequence is included under the Z62 Accept and Encrypt PIN (with Custom Prompts) communication protocol.

66 Pre-Authorization: PIN Entry Test Request

Tests PIN entry encryption with preset PIN '1234.'

Category Preauthorization packet

Comments This packet functions the same as 60 Pre-Authorization: PIN Entry Request, except that the PIN is not entered from the keypad. It is preset by the PINpad as '1234.'

Packet Format

```
<STX> 66 [primary account#] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
66	packet type	2	PIN Entry Test Request
[primary account#]	packet parameter	8-19	Card Account Number
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 24 characters, minimum 13 characters			

Example

```
<STX> 66012345678987654321O <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
66 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	Packet 71 with PIN = '1234'
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
	<------	Alternately display: PROCESSING PIN PAD

70 Request PIN Entry

Cycles through the following prompts until a PIN is entered:

```
TOTAL

$XXXXX.XX (Amount of sale from the controller)

ENTER PIN

PUSH "ENTER"
```

Category Standard Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments After a customer enters a PIN number and presses 'ENTER,' the PINpad displays PROCESSING and PIN PAD until the [CLEAR] key is entered or another packet is sent to the PINpad.

PIN length must be in the range of 4-12 digits. PIN length of less than 4 digits is not allowed and results in an error beep. Null PIN entry is not allowed and also results in an error beep.

The amount display is limited to xxxxx.xx format. And the maximum length of [amount] is 7 digits, including the decimal point.

Packet Format

```
<STX> 70 [account#] <FS> [C/D] [amount] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
70	packet type	2	Request PIN Entry
[account#]	packet parameter	8-19	Card Account Number
<FS>	packet parameter	1	Field separator; Value: `1Ch'
[C/D]	packet parameter	1	Credit/Debit Indicator; Value: '43h/44h'
[amount]	packet parameter	3-7	Transaction Amount; must include decimal point
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 33 characters, minimum 18 characters			

Example

```
<STX> 700123456789012345678 <FS> C9.99 <ETX>{LRC}
```

The amount in this packet is $9.99 (credit).

Protocol The communication protocol sequence is included under the 71 Transfer PIN Block communication protocol.

71 Transfer PIN Block

Encrypts and sends the PIN block to the controller in response to a PIN request.

Category Standard Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments Transmittal follows a PIN request (Packets 60, 66, 70, 76, Z60, or Z62) and PIN entry from user.

NOTE

After the PIN block is sent, the PINpad can take up to 4 seconds to reschedule future keys. To prevent corruption in future key encryption, the PINpad will NAK all incoming packets until the key rescheduling is completed.

Packet Format

```
<STX> 71 0 [key serial number] [pin] <ETX>{LRC}
```

Elements No error condition:

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
71	packet type	2	Transfer PIN Block
0	packet parameter	1	Value must be 0. Reserved for future release as a Function Key Indicator. This feature is not implemented in version 4E3002x and earlier releases of the firmware.
[key serial number]	packet parameter	10-20	Key Serial Number; hexadecimal (leading F's suppressed); included only if PIN is entered Length is 0 if no PIN entered
[pin]	packet parameter	16	64-bit Encrypted PIN Block, represented as 16 hex digits Length is 0 if no PIN entered
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 42 characters, minimum 6 characters (for null entry)

When there is no error in the 76 packet, the PINpad will respond with Packet 71 as above.

Example

```
<STX> 710[key serial number]0123456789123456 <ETX>{LRC}
```

This message packet has a key serial number and the PIN length is 16.

```
<STX> 710 <ETX>{LRC}
```

This is a null entry.

Protocol

Controller	Transmission Direction	PINpad
Packet 60/66/70/76/Z60/Z62	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
		Display standard/custom prompts
		Customer enters PIN
		PINpad displays "*" characters in echo to customer keystrokes.
	<------	Packet 71
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		
		rotate standard/custom specified displays

76 PIN Entry Test Request

Requests PIN entry test.

Category Standard Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments This packet functions the same as 70 Request PIN Entry except that the PIN is not entered from the keypad. Instead, the PIN is preset to "1234." After encryption, the PINpad displays PROCESSING and PIN PAD until the [CLEAR] key is pressed or another packet is sent to the PINpad.

Packet Format

```
<STX> 76 [account#] <FS> [C/D] [amount] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
76	packet type	2	Request PIN Entry Test
[account#]	packet parameter	8-19	Card Account Number
<FS>	packet parameter	1	Field Separator; Value: '1CH'
[C/D]	packet parameter	1	Credit/Debit Indicator; Value: '43h/44h'
[amount]	packet parameter	3-7	Transaction Amount; must include the decimal point
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 33 characters, minimum 18 characters			

Example

```
<STX> 76012345678987654321O <FS> C9.99 <ETX>{LRC}
```

The amount in this packet is $9.99.

Protocol

Controller	Transmission Direction	PINpad
76 packet	------>	
	<------	ACK = LRC OK
		NAK = LRC incorrect
	<------	Packet 71 with PIN = '1234'
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		

90 Load Initial Key Request

Loads the initial key to the PINpad device.

Category

Key Loading Device to PINpad Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

After the initialization of 21 future keys, the PINpad will respond with 91 Load Initial Key Response with confirmation status. If the PINpad receives a transaction packet before Packet 90 is loaded, the error message ERR-NO KEY is displayed.

Packet Format

```
<STX> 90 [initial PIN encryption key] [key serial number] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
90	packet type	2	Load Initial Key Request
[IPEK]	packet parameter	16 or 32	Initial PIN Encryption Key; hexadecimal 16 - 1DES Mode 32 - 3DES Mode
[KSN]	packet parameter	20	Key Serial Number; hexadecimal; (leading F's included)
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 57characters, minimum 41 characters

NOTE

The difference between DUKPT 1DES mode and DUKPT 3DES mode is in the size of the Initial PIN Encryption Key.

Example

```
<STX> 90123456789101112101234567891011121314 <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
90 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect

Controller	Transmission Direction	PINpad
	<------	Initialization of 21 future keys; Packet 91 with confirmed status
ACK = LRC OK NAK = LRC incorrect (EOT after 3 NAKs)	------>	

91 Load Initial Key Response

Responds to 90 Load Initial Key Request with confirmation status to the controller.

Category Key Loading Device to PINpad Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments If 21 future keys are successfully initialized, a positive confirmation response (0) is sent via Packet 91; otherwise a negative confirmation response (1) is sent via Packet 91.

Packet Format

```
<STX> 91 [CS] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
91	packet type	2	Load Initial Key Response
[CS]	packet parameter	1	Confirmation Status: • 0 = Confirmed • 1 = Not Confirmed • 2 = Error – Incorrect Key Length
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 6 characters, minimum 6 characters			

NOTE

Confirmation Status – 2 indicates that the length of the Initial PIN Encryption Key does not comply with 1DES or 3DES mode. Example follows.

Initial PIN Encryption Key length (via packet 90) sent by Master Device	Current DUKPT Mode	[CS] Response
16	3DES	2
32	1DES	2

Example

```
<STX> 91 1 <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
	------>	91 packet
ACK = LRC OK	------>	
NAK = LRC incorrect		
(EOT after 3 NAKs)		

Z60 Accept and Encrypt PIN

Directs the PINpad device to accept the customer PIN, create and encrypt the PIN block, and transmit the PIN block to the controller.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet must be preceded by a display packet, such as Packet Z2 or Z3, and followed by the PIN transmittal Packet 71.

The PIN length must be in the range of 4-12 digits. PIN length of less than 4 digits is not allowed and results in an error beep. Null PIN entry is not allowed and also results in an error beep.

NOTE

During the Z60 session, only 72 Cancel Session Request from the controller or the PINpad [CLEAR] key can cancel the session.

- If data entry is not initiated, pressing [CLEAR] cancels the operation and sends an [EOT] to the controller.
- If data entry is initiated, the PINpad unit clears the entry, redisplays the previous prompt and restarts data entry.

Any message packet requesting a PINpad display (e.g., Z2, Display A String) must precede Z60 for the message to be displayed before PIN entry.

Packet Format

```
<STX> Z60.[account#] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z60	packet type	3	Accept and Encrypt PIN
.	hexadecimal	1	Command Delimiter; period: '.' Hex value: '2Eh'
[account#]	packet parameter	8-19	Card Account Number
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character
Packet Length: maximum 26 characters, minimum 15 characters			

Example

```
<STX> Z60.4000000000006 <ETX>{LRC}
```

Protocol

Controller	Transmission Direction	PINpad
Z60 packet	------>	
	<------	ACK = LRC OK NAK = LRC incorrect customer PIN entry; asterisks are displayed

Z62 Accept and Encrypt PIN (with Custom Prompts)

Combines the PIN entry request, display specifications, and transmittal into one message packet.

Category

Custom Communication Packet

Support Mode

PINpad 1000	PINpad 1000SE
✔	✔

Comments

This packet directs the PINpad device to alternate up to two displays every 3 seconds, get user input of PIN, encrypt the PIN, send the encrypted PIN to the controller and display the specified processing message. The function is quite similar to Z60 Accept and Encrypt PIN, but Packet Z62 allows programmers to specify display messages to display in rotation before the PIN entry, identify the PIN length, allow null PIN entries, and display the processing message after the PIN entry. Display messages that are longer than 16 bytes will be displayed right-justified with the extra message bytes ignored.

The PIN length can be 4-12 digits. PIN entries of 1-3 digits are treated as errors, generating an error beep. Null PIN entry is also accepted. If a null PIN is entered, the [pin] field of return Packet 71 is set to null.

NOTE

During the Z62 session, only Packet 72 from the controller or the PINpad [CLEAR] key can cancel the session.

- If data entry is not initiated, pressing [CLEAR] cancels the operation and sends an [EOT] to the controller.
- If data entry is initiated, the PINpad clears the entry, redisplays the previous prompt and restarts data entry.

NOTE

The User Definable Character (UDC) function is supported in this packet for [message1], [message2], and [process msg]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

Packet Format

```
<STX> Z62.[account#] <FS> [min pin] [max pin] [null flag] [message1] <FS>
[message2] <FS> [processing message] <ETX>{LRC}
```

Elements

Type	Field	Length	Description
<STX>	start of packet	1	ASCII Start of Text Control Character; Value: `02h'
Z62	packet type	3	Encrypt PIN/Display Custom Messages

Type	Field	Length	Description
.	hexadecimal	1	Command Delimiter; period: '.' Hex value: '2Eh'
[account#]	packet parameter	8-19	Card Account Number
<FS>	packet parameter	1	Field Separator
[min pin]	packet parameter	2	Minimum Acceptable PIN Length; Range: 04-12, null PIN permitted
[max pin]	packet parameter	2	Maximum Acceptable PIN Length; Range: 04-12, null PIN permitted
[null flag]	packet parameter	1	Null PIN status: • Y = Null PINs allowed • N = Null PINs not allowed
[message1]	packet parameter	0-16	Message to alternate with [message2] until customer presses key (UDC function is supported in this packet)
<FS>	packet parameter	1	Field Separator
[message2]	packet parameter	0-16	Message to alternate with [message1] until customer presses key (UDC function is supported in this packet)
<FS>	packet parameter	1	Field Separator
[processing message]	packet parameter	0-16	Processing Message Displayed After PIN Entry
<ETX>	end of packet character	1	ASCII End of Text Control Character, Value:`03h'
{LRC}	block code check	1	Error Check Character

Packet Length: maximum 255 characters, minimum 23 characters

NOTE

The User Definable Character (UDC) function is supported in this packet for [message1], [message2], and [process msg]. This extends the maximum packet length, since 5 characters can be used to for each UDC. See User Definable Character (UDC) Functions for more details.

Examples

```
<STX>Z62.4000000000006<FS>0412YMESSAGE 1<FS>MESSAGE 2<FS>PROCESSING
MSG<ETX>{LRC}
```

The PINpad alternately displays 'MESSAGE 1' and 'MESSAGE 2' until a PIN number or a null PIN is entered. A null PIN is generated by pressing the 'ENTER' key. Only a PIN number with length ranges from 4 to 12 digits is accepted. Each PIN digit is echoed with an asterisk '*'. As soon as the PIN number has been entered, the third message 'PROCESSING MSG' will be shown.

```
<STX> Z62.4000000000006 <FS> 0412YTHANK YOU <FS> PLEASE ENTER PIN <FS>
PROCESSING MSG <ETX>{LRC}
```

The PINpad alternately displays THANK YOU and PLEASE ENTER PIN until the customer presses the first key. A null PIN is generated by pressing the [ENTER] key only. PIN numbers must be between 4 and 12 digits in length. Each PIN digit is echoed with an asterisk ("*"). After the PIN entry, the third message PROCESSING MSG will be displayed.

```
<STX>Z62.4000000000006<FS>0608NMESSAGE 1<FS><FS>PROCESSING MSG<ETX>{LRC}
```

The PINpad alternately displays 'MESSAGE 1' and 'MESSAGE 2' until a PIN number or a null PIN is entered. No null PIN is allowed; only a PIN number with PIN length ranges from 6 to 8 digits is accepted. Each PIN digit is echoed with an asterisk '*'. As soon as the PIN number has been entered, the third message 'PROCESSING MSG' will be shown.

Protocol

The communication protocol sequence is included under the 71 Transfer PIN Block communication protocol.

Customizable Command Specification

This section discusses PINpad support of special prompt display and data entry requirement programmability.

Introduction

The master device should be able to send the PINpad special prompts and data entry requirements for customizing the PINpad. Under control of the master device, the PINpad may:

- Display a single message
- Display rotating messages at about 3 second interval
- Display user definable character functions
- Display user definable character functions
- Request a single keystroke entry from the customer
- Request a keystroke sequence from the customer, and echo the input on the PINpad display
- Request PIN number from the customer, build and encrypt the PIN block, and echo the customer's input as asterisks
- Down load user defined prompt table (supported in version 4E3002x and later releases of the firmware)

Prompt Tables

The PINpad has several prompt tables:

- a fixed, static prompt table located in ROM
- a downloadable prompt table located in RAM

NOTE

Prompt tables are only available in version 4E3002x and later releases of the firmware.

The PINpad allows both fixed and downloadable prompt tables to contain User Definable Characters (UDC). See User Definable Character (UDC) Functions for details. This allows applications to have the ability to send UDCs in the MACed Z2/Z3 packets. See Prompt Table for Z2/Z3 Authentication for details on the fixed prompt table, stored in ROM.

In order to have Customizable Commands (Packets Z40, Z41, Z42, Z43, Z50, and Z51) operational in the PINpad 1000SE Mode, data authentication requires that the contents of Packets Z2 and Z3 must be MACed or the message text in the packet must match on messages in the prompt table.

Downloadable Prompt Table

The number of prompt messages in the prompt table is not limited, but the overall RAM table packet size is limited to 100 bytes.

In certain circumstances the RAM table may be erased from memory, if the master key that was used to load the RAM prompt table is erased. The conditions for erasure are:

- All Master Keys are erased - can occur for a number of reasons: if a key is loaded in a second key loading session (in PINpad 1000SE mode), certain Packet 17 mode changes, cold power reset, or RAM checksum correction (CRC corruption)
- Using 02 Transfer Master Key to replace the old master key with the new master key, where the old master key was used to load the RAM prompt table.
- Loading a new RAM table, using Z10 Load Prompt Table.

Z2/Z3 MACing Rules

An authenticated Packet Z2/Z3 is MACed using a selected Master key as the MAC key. The MAC key used to verify this packet must be 112 bits in length to meet the November, 2003 Visa PED requirements (Appropriate algorithms and key sizes will change slowly over time, as computing capability expands to make brute force attacks more feasible) and must also be tagged as a MAC verification key with appropriate GISKE attributes for specifying MAC usage and algorithm. Version 4E3003x and later releases of the firmware enforce the 112-bit MAC key rule. This MAC key will use the ANSI/ISO MACing algorithms for MACing, available as indicated by the GISKE Key Usage attributes. See *GISKE Key Block Specification* VPN - 22986 for details of MAC algorithms.

Data fields need to be MACed including the all characters inside the range of ‘A’ to ‘Z’ (0x41 ~ 0x5A), and UDCs (e.g.: <US>4E72, all five characters need to be MACed), clear display flag <SUB> and field separator <FS>. If the message contains numeric characters, such as ‘0’ ~ ‘9’ (0x30 ~ 0x39) that are not user-defined characters, then these characters are ignored during the MACing. Characters outside the range of ‘A’ ~ ’Z’ are also ignored. Ignoring these character allows dynamic messages which contain debit/credit amounts to be MACed using static MAC values stored in terminal applications (static because the MAC is over the static text portion of the message). This alleviates the need for the terminal application to dynamically generate MACs over dynamically changing amount fields. When formulating the clear message to be MACed, wherever a non-MACable character is found, the PINpad removes it from the MACing input with the characters shifted left so that there is no gap.

If the last MAC input is not on an even 8-byte boundary, the last block will be right-padded with 0x30's ('0'). The four left most bytes (8 hex digits) of the resulting cryptogram will be used for the MAC value.

NOTE

In PP1000 mode, the Z2/Z3 MACing rules are not used. If MACed Z2 or Z3 packets are received, they are processed as normal Z2 or Z3 packets. The MAC data (MAC value) in the packet is ignored, but response as if it were valid (MAC OK), message is displayed in the LCD.

Non-MACed Z2/Z3 Message Matching Rules

The Z2/Z3 matching rules are for PINpad 1000SE mode only. Characters outside the range of 'A' ~ 'Z' (0x41 ~ 0x5A) will not be part of matching. For characters inside the range of 'A' ~ 'Z' (0x41 ~ 0x5A), the match must be exact. UDCs must be part of the matching.

NOTE

In PP1000 mode, the Z2/Z3 matching rules are not used.

Prompt Rule Summary

The following rules apply to message usage and keypad entry with prompt tables:

- The message in a Z2 or Z3 packet must be MACed or must match a message in the RAM or ROM prompt table list of messages.
- If **not** MACed and clear text **not** found in either prompt table, then Z40 (response Z41) and Z42 (response Z43) will return only non-numeric keys (CLEAR, ENTER, BACKSPACE), and soft function keys (F1, F2 and F3). If numeric keys (0 through 9) are pressed, error beep, ignore the key press.
- If **not** MACed and clear text **not** found in either prompt table, the Z50 (response Z51) is disabled.
- If **not** MACed and clear text found in prompt table(s) (either ROM or RAM), then Z40 (response Z41), Z42 (response Z43), Z50 (response Z51) are enable. All keypad input is allowed.
- If MACed, then Z40 (response Z41), Z42 (response Z43), Z50 (response Z51) are enable. All keypad input is allowed.
- If the MAC value or data is incorrect, an EOT will be returned (see MACed Z2 Display a String or MACed Z3 Display Rotating Messages for more details) and an error message will appear on the PINpad display (PACKET ERR A).
- If Packet Z50 is sent and it is not enabled, an EOT will be returned and an error message will be display on the LCD (see Z51 Return String Input for more details).

The above usage rules are also shown in the following table formats.

PINpad 1000	Allow Message Display (Z2/Z3)	Allow Numeric Key Entry	Allow Alpha Key Entry (functional key)
Z40 / Z42 Packet Behavior in combination with Z2 / Z3 packets			
MACed Z2 \ Z3Packets			
• MAC = OK	yes	yes	yes
• MAC = Bad	yes	yes	yes
Non - MACed Z2 \ Z3Packets			
• Messages Matched = OK	yes	yes	yes
• Messages Matched = Bad	yes	yes	yes
Z50 Packet Behavior in combination with Z2 / Z3 packets			
MACed Z2 \ Z3Packets			
• MAC = OK	yes	yes	yes
• MAC = Bad	yes	yes	yes
Non - MACed Z2 \ Z3Packets			
• Messages Matched = OK	yes	yes	yes
• Messages Matched = Bad	yes	yes	yes

PINpad 1000SE	Allow Message Display (Z2/Z3)	Allow Numeric Key Entry	Allow Alpha Key Entry (functional key)
Z40 / Z42 Packet Behavior in combination with Z2 / Z3 packets			
MACed Z2 \ Z3Packets			
• MAC = OK	yes	yes	yes
• MAC = Bad	**no**	**no**	**no**
Non - MACed Z2 \ Z3Packets			
• Messages Matched = OK	yes	yes	yes
• Messages Matched = Bad	yes	**no**	yes
Z50 Packet Behavior in combination with Z2 / Z3 packets			
MACed Z2 \ Z3Packets			
• MAC = OK	yes	yes	yes
• MAC = Bad	**no**	**no**	**no**
Non - MACed Z2 \ Z3Packets			
• Messages Matched = OK	yes	yes	yes
• Messages Matched = Bad	yes	**no**	**no**

User Definable Character (UDC) Functions

PINpad 1000SE mode supports User Definable Character (UDC) display in Z2, Z3, Z8, and Z62. UDC is supported in the ROM and RAM prompt tables. A control character, <US> is used to define the start of a user-defined character. The next four bytes define what display segments will be displayed for that character. The LCD segment map is shown in Figure 8.

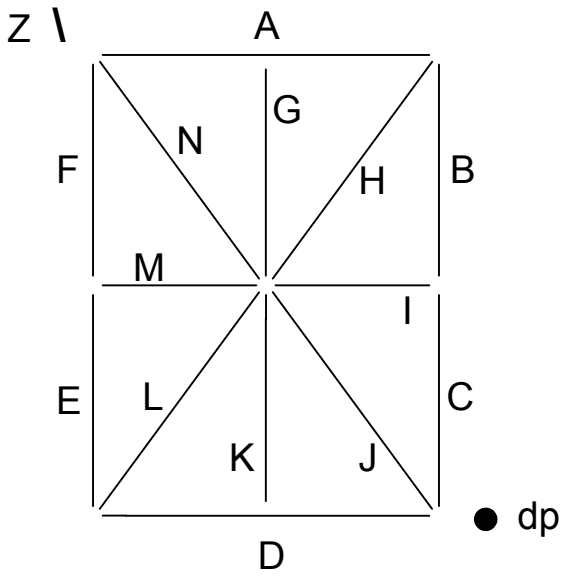


Figure 8 PINpad 1000SE LCD Segment Map

NOTE

1. A maximum of 16 UDCs are allowed in a message block (16 display characters per block).
2. The total number of UDCs per packet is limited to 48, due to the size of RxBuf. (Only Applicable to Z3)
3. A maximum number of 16 characters per message block rule is enforced, if message block contains UDC.
4. Last 16 characters of a message block are displayed, if message block contains no UDC and display characters are more than 16 characters.

	Byte 1	Byte 2	Byte 3	Byte 4
Display Segments Labels	J I H G	D E F Z	dp C B A	K L M N

UDC Character Examples

The character "8" has the following bits set in the display segment data:

```
J I H GD E F Zdp C B AK L M NDisplay Segments Labels
0 1 0 01 1 1 00 1 1 10 0 1 0Binary
4   E   7   2 Hex
```

The character "I" has the following bits set in the display segment data:

```
J I H GD E F Zdp C B AK L M NDisplay Segments Labels
0 0 0 11 0 0 00 0 0 11 0 0 0Binary
1   8   1   8 Hex
```

Default Existing Character Library

The PINpad 1000SE unit uses the following existing character library:

LCD Display	Control Character	LCD Display	Control Character	LCD Display	Control Character	LCD Display	Control Character
	00 00	!	00 E0	“	20 01	#	58 6A
$	1A 5A	%	E2 47	&	AC 53	‘	20 00
(	00 00	)	00 00	*	F0 0F	+	50 0A
,	00 04	-	40 02	.	00 80	/	20 04
0	2E 74	1	00 60	2	4C 32	3	48 72
4	42 62	5	8A 12	6	4E 52	7	00 70
8	4E 72	9	4A 72	:	10 08	;	00 06
<	A0 00	=	48 02	>	00 05	?	40 B8
@	0C 7A	A	46 72	B	58 78	C	0E 10
D	18 78	E	4E 12	F	46 12	G	4E 50
H	46 62	I	18 18	J	08 60	K	A6 02
L	0E 00	M	26 61	N	86 61	0	0E 70
P	46 32	Q	8E 70	R	C6 32	S	4A 52
T	10 18	U	0E 60	V	80 61	W	86 64
X	A0 05	Y	20 09	Z	28 14	'0	0F F0
0.	2E F4	1.	00 E0	2.	4C B2	3.	48 F2
4.	42 E2	5.	8A 92	6.	4E D2	7.	00 F0
8.	4E F2	9.	4A F2				

UDC Packet Example

Example of using Packet Z2 - Display a String, to display the character 8 as a UDC:

```
<STX>Z2<SUB>1234567<US>4E72<ETX>{LRC}
```

The above packet would display 12345678 on the PINpad 1000SE display.

Communication Examples

The following are examples of communication flow for operating the PINpad 1000SE device when set for DUKPT. Examples include the initialization sequence, transaction sequence and other sequences (e.g., when customers cancel a PIN or a transaction at various stages of the communication flow).

Initialization Sequence

The following initialization sequence needs to be done at start-up or whenever a PINpad has lost power.

	Controller	Transmission Direction	PINpad
Cancel Session Request	72 Packet	------>	Clear any PINpad operation
		<------	ACK
	Z7 Packet	------>	Disable *CANCEL REQUESTED* message
			ACK
		<------	
	Z8 Packet	------>	Selected *IDLE* message
		<------	ACK

The PINpad is now ready for a transaction.

Transaction Sequence

The following is a sequence for a normal transaction flow.

	Controller	Transmission Direction	PINpad
ENTER YOUR PIN Prompt	Z2 Packet	------>	
		<------	ACK
Accept and Encrypt PIN	Z60 Packet	------>	
		<------	ACK
	wait for PIN entry		
Transfer PIN Block		<------	Customer enters PIN
			71 Packet
	ACK	------>	
$X.XX AMT Prompt	Z2 Packet	------>	
		<------	ACK
Request Key Code	Z40 Packet	------>	
		<------	ACK
	wait for confirmation entry		
Return Key Code		<------	Z41 Packet
	ACK	------>	
THANK YOU Prompt	Z2 Packet	------>	
		<------	ACK
Cancel Session Request	72 Packet	------>	
		<------	ACK

The PINpad device is ready for the next transaction.

Customer Cancels PIN

The following sequence describes what happens when a customer cancels (clears) a PIN entry during a transaction.

	Controller	Transmission Direction	PINpad
ENTER YOUR PIN Prompt	Z2 Packet	------>	
		<------	ACK
PIN Request	Z60 Packet	------>	
		<------	ACK
	wait for PIN entry		
[CLEAR] Pressed			Customer presses [CLEAR] key
	EOT	<------	
			EOT
ENTER YOUR PIN Prompt	Z2 Packet	------>	
		<------	ACK
PIN Request	Z60 Packet	------>	
		<------	ACK
	wait for PIN entry		
PIN		<------	71 Packet
	ACK	------>	
$X.XX AMT Prompt	Z2 Packet	------>	
		<------	ACK
PINpad Request Key Code	Z40 Packet	------>	
		<------	ACK
	wait for confirmation entry		
Return Key Code		<------	Z41 Packet
	ACK	------>	
THANK YOU Prompt	Z2 Packet	------>	
		<------	ACK
Cancel Session Request	72 Packet	------>	
		<------	ACK

The PINpad device is ready for the next transaction.

Customer Cancels at Amount Verification

The following example shows what happens when a customer cancels the transaction at the "Amount Verification" prompt.

	Controller	Transmission Direction	PINpad
ENTER YOUR PIN Prompt	Z2 Packet	------>	
		<------	ACK
PIN Request	Z60 Packet	------>	
		<------	ACK
	wait for PIN entry		
Transfer PIN Block		<------	71 Packet
	ACK	------>	
THANK YOU Prompt	Z2 Packet	------>	
$X.XX AMT Prompt		<------	ACK
Cancel Session Request	Z40 Packet	------>	
Request Key Code		<------	ACK
	wait for confirmation entry		
Return Key Code			Customer presses [CLEAR] key
		<------	Z41 Packet
	ACK	------>	
ENTER YOUR PIN Prompt	Z2 Packet	------>	
		<------	ACK
PIN Request	Z60 Packet	------>	
		<------	ACK
	wait for PIN entry		
Transfer PIN Block		<------	71 Packet
	ACK	------>	
$X.XX AMT Prompt	Z2 Packet	------>	
		<------	ACK
Request Key Code	Z40 Packet	------>	
		<------	ACK
	wait for confirmation entry		
Return Key Code		<------	Z41 Packet
	ACK	------>	
THANK YOU Prompt	Z2 Packet	------>	
		<------	ACK
Cancel Session Requested	72 Packet	------>	
		<------	ACK

The PINpad device is ready for the next transaction.

Troubleshooting and Service

VeriFone follows stringent quality control standards in the manufacture of PINpad 1000SE terminals. Each unit that leaves the factory receives numerous tests to ensure quality and reliable operation. However, should you encounter a problem in operation, read this section for possible causes and solutions.

NOTE

Perform only those adjustments or repairs specified in this guide. For all other services, contact your local VeriFone distributor or service provider. Service conducted by parties other than authorized VeriFone representatives may void the product warranty.

NOTE

The PINpad 1000SE terminal comes equipped with tamper-evident labels. Do not, under any circumstance, attempt to disassemble the device.

Troubleshooting

During normal, day-to-day operation of the PINpad 1000SE unit, minor malfunctions may occur. The following sections detail the PINpad 1000SE unit's troubleshooting guidelines, diagnostic modes, and error messages:

- The troubleshooting guidelines provided in the following section identify various problems and suggest appropriate corrective actions.
- The diagnostic modes allow users to perform various tests and operations using the PINpad keypad.
- The error messages catalog the different prompts and error messages that may appear on the PINpad display panel.

If problems persist or are not described below, contact your local VeriFone representative for assistance.

Display Panel Does Not Work

1. Check all the cable connections.
2. The cable connecting the PINpad 1000SE to the controller may be defective. Try a different cable.
3. Check the controller's AC outlet to be sure the outlet is supplying sufficient power. Substitute the controller's power pack with another power pack.
4. The controller's application program might not be loaded correctly; download the application program and try again.

5 Run the display reliability test (see DISP TST for more information).

6 If the problem persists, contact your local VeriFone representative for assistance.

Keypad Fails to Respond

1 Check your display panel. If no characters or the wrong characters are displayed, refer to the "solutions" for the previous problem.

2 Run the keypad reliability test (see KEY TST for more information).

3 If the keypad test shows no problems, but pressing a function key does not perform the expected action, refer to the documentation for the relevant application.

4 If the problem persists, contact your local VeriFone representative for assistance.

Diagnostics

The PINpad 1000SE has two built-in diagnostics modes. See Level 1 Diagnostic and Level 2 Diagnostic for performing various tests and operations using the PINpad keypad.

Error Messages

Appendix D lists the different prompts and error messages that may appear on the PINpad display panel. If you see any of these messages, refer to Prompts and Error Messages, or to your application's reference manual for an explanation of the message.

Cleaning and Care

For normal dirt, use a clean cloth slightly dampened with water and a drop or two mild soap. For stubborn stains, use alcohol or an alcohol-based cleaner.

Never use thinner, trichloroethylene, or ketone-based solvents — they can deteriorate plastic or rubber parts. Do not spray cleaners or other solutions directly onto the keypad or display.

Because your PINpad device can be damaged by liquids, do not spray liquid cleaners directly on the unit. Always apply the cleaner to the cloth before cleaning the PINpad.

VeriFone Service and Support

For PINpad 1000SE device problems, contact your local VeriFone representative or service provider.

For PINpad 1000SE product service and repair information:

- (USA) VeriFone Service and Support Group, 1-800-834-9133, Monday–Friday, 8 A.M.–7 P.M. eastern time
- (International) Contact your local VeriFone representative

For PINpad 1000SE supplies:

- VeriFone Online Store at *www.store.verifone.com*
- (USA) VeriFone Customer Development Center, 1-800-233-0522, Monday–Friday, 7 A.M.–5 P.M. mountain time
- (International) Contact your local VeriFone representative

Returning a Terminal

Before returning an PINpad 1000SE terminal to VeriFone, you must obtain a Merchandise Return Authorization (MRA) number. The following procedure describes how to return one or more terminals for repair or replacement (U.S. customers only):

NOTE

International customers, please contact your local VeriFone representative for assistance with your service, return, or replacement.

1. Gather the following information from the printed labels (Figure 9) on the bottom of *each* PINpad 1000SE unit you are returning:
   - Product ID, including the model and part number. For example, “PINPAD 1000SE” and “PTID xxxxxxxx”
   - Serial number (S/N xxx-xxx-xxx)
2. Within the U.S., call VeriFone toll-free at 800-834-9133.
3. Select the MRA option from the automated message. The MRA department is open Monday–Friday, 8 A.M.–7 P.M., EST.
4. Give the MRA representative the information gathered in Step 1.

   If the list of serial numbers is long, you can fax the list, along with the information gathered in Step 1, to the MRA department at 502-329-5947.
   - Please address the fax clearly to the attention of the “VeriFone MRA Dept.”
   - Include a telephone number where you can be reached and your fax number.
   - You will be issued MRA number(s) and the fax will be returned to you.

NOTE

One MRA number must be issued for each terminal you return to VeriFone, even if you are returning several of the same model.

5 Describe the problem and provide the shipping address to return the repaired or replacement unit.

6 Provide the shipping address where the repaired or replacement unit must be returned.

7 Keep a record of the following items:

- Assigned MRA number(s)
- VeriFone serial number assigned to the PINpad 1000SE terminal you are returning for service or repair (terminal serial numbers are located on the bottom of the unit (see Figure 9)
- Shipping documentation, such as airbill numbers used to trace the shipment
- Model(s) returned (model and part numbers are located on the bottom of each terminal)
- Model(s) returned (model numbers are located on the VeriFone label on the bottom of the PINpad 1000SE terminal)

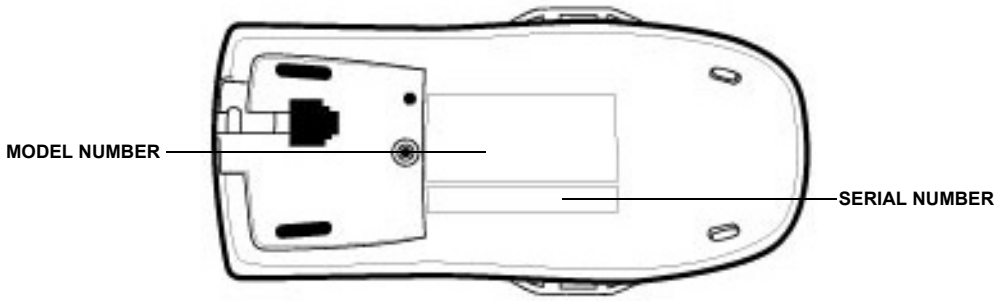


Figure 9 Information Labels on Bottom of PINpad 1000SE

Accessories and Documentation

VeriFone produces accessories and documentation for the PINpad 1000SE unit, as listed below. When ordering, refer to the part number in the left column.

- VeriFone Online Store at www.store.verifone.com
- USA: VeriFone Customer Development Center, 1-800-233-0522, Monday–Friday, 7 A.M.–5 P.M., MST
- International: Contact your VeriFone representative

NOTE

Cables with -xx part number suffixes have multiple available lengths.

VeriFone Cleaning Kit

02746-01	Cleaning kit

Cables

Contact your local VeriFone distributor to determine which cable fits your needs.

07042-xx	4PC plug to MOD10 plug, coiled (Omni 32xx, 33xx, 36xx, or 37xx Series Terminals)
10441-xx	4PC plug to 6-pin DIN plug, coiled (most Tranz terminals)
01582-xx	4PC plug to 6-pin DIN plug, straight (most Tranz terminals)
03021-xx	4PC plug to 6-pin mini-DIN plug, coiled (Omni 4xx and 7000MPD terminals, as well as Everest and Everest *Plus* terminals)

Power Supply

CPS04951-1B	DC power supply

PC/AT Interface Kits

10776-01	4PC plug to DB25 plug (most IBM PC or compatible computers)
10776-02	4PC plug to DB9 plug (most IBM AT or compatible computers)

Supplementary Hardware

E-100674051	Stand adapter
E-100675051	Privacy shield

Documentation

22900	*PINpad 1000SE Certifications and Regulations*
22901	*PINpad 1000SE Quick Installation Guide*
22902	*PINpad 1000SE Installation Guide*
22906	*PINpad 1000SE Stand Adapter Quick Installation Guide*

Features and Specifications

This chapter discusses power requirements, dimensions, and other specifications of the PINpad 1000SE unit.

Unit Power Requirements

PINpad 1000SE unit: 6-14 V DC maximum power 36.5mA

Serial Interface

The PINpad 1000SE device serial interface is implemented through a software UART that drives an output port (transmit) and an interrupt pin (receive) of the processor. The connector interface is implemented through the modular four-position, four-conductor connector.

Temperature

Operating temperature: 0^{o} to 40^{o} C (32^{o} to 104^{o} F)

NOTE

Battery-backed memory can be corrupted if the PINpad 1000SE device is stored in an environment that is warmer than 50^{o} C (122^{o} F) or cooler than 10^{o} C (50^{o} F).

Humidity

Relative humidity: 15% to 90%; no condensation

External Dimensions

- Length: 150 mm (5.90 in)
- Width: 68 mm (2.68 in)
- Depth: 37 mm (1.46 in)

Weight

Unit weight: 190 gms (6.67 oz.)

Shipping weight: 330 g (.15 lb.)

The shipping weight includes: shipping carton, unit, one *PINpad 1000SE Quick Installation Guide*, and one *PINpad 1000SE Certifications and Regulations*.

Accessories

Cables

Part Number	Description
10441-01	Coiled cable.6M TRANZ/OMNI 3xx (stretches to approximately 7 ft.)
10441-02	Coiled cable 1.1M TRANZ/OMNI 3xx (stretches to approximately 15 ft.)
03021-00	Coiled cable.75M OMNI 4xx/TRANZ 4xx (stretches to approximately 9 ft.)

PC Interface Kit

Part Number	Description
10776-01	PINpad interface kit to PC (25-pin serial port connector)
10776-02	PINpad interface kit to PC (9-pin serial port connector)

Key Insertion

PIN Encryption

The PINpad device encrypts personal identification numbers (PINs) entered at its keypad and transmits via the controller to the host during a transaction.

To encrypt this confidential data, the PINpad 1000SE device uses both the Master/Session method of key management and the DUKPT (Derived Unique Key Per Transaction) in conjunction with the ANSI x3.92 DES encryption algorithm.

Master/Session Key Insertion

You can create and insert master keys into the PINpad with two methods:

- Automatically, by using VeriFone's PC-based SecureKit Key Insertion product (Part P006-216-11-MK, SecureKit 2.1)
- Manually, from the PINpad device keypad

Manual insertion affords a lower level of security, and also requires the manual insertion of identical master keys into the host. However, because it does not require the key injection software or additional equipment, manual insertion may be used for development purposes.

NOTE

Manual key insertion is not available if the PINpad device is set for the DUKPT method.

Following are the procedures for inserting each master key into the PINpad unit from its keypad.

Display	Response
1. (idle prompt)	Press [ENTER] immediately followed by [1].
2. WHICH MKEY?	Press a key from 0 to 9. The numeric value of the key corresponds to the address of a master key (you can have up to 10 master keys).

Display	Response
3. ENTER OLD MKEY	If no key exists for the address you selected, this message does not appear and you can skip to Step 4. If this message appears, enter any pre-existing key assigned to this address. If you make an error, the PINpad device displays "INVALID MKEY" and returns to the idle prompt. For example, if you select the hexadecimal character D, you must enter the decimal number 13 on the keypad followed by [ENTER].
4. ENTER NEW MKEY	Create a key consisting of 16 hexadecimal characters. Enter the decimal equivalent of each character using the table below. Press [ENTER] after each of the 16 entries. Hex Character Decimal Equivalent • 0 0 • 1 1 • 2 2 • 3 3 • 4 4 • 5 5 • 6 6 • 7 7 • 8 8 • 9 9 • A 10 • B 11 • C 12 • D 13 • E 14 • F 15 Be sure you have the new master key written down and stored in a safe place. The next prompt asks you to enter it again for verification.
5. ********########	The PINpad device displays "*" for the first eight entries and "#" for the remaining eight entries.

Display	Response
6. ENTER AGAIN	Enter the new master key again for confirmation. If you enter the incorrect key, the unit displays "INVALID MKEY" and returns to the idle prompt. The old key is retained as the valid master key.
7. MKEY ENTERED	If the master key was entered successfully, this message appears for 3 seconds. The display then returns to the idle prompt.

DUKPT Key Insertion

DUKPT Key insertion may be accomplished by using VeriFone's PC-based SecureKit Key Insertion product (Part P006-216-11-MK, SecureKit 2.1)

To inject a PINpad device when set as a DUKPT unit, set the "PINpad Device type" as a "PINpad 102 (DUKPT)" in the system configuration setup menu.

ASCII Table

Decimal Value	Hexadecimal Value	ASCII Character	Decimal Value	Hexadecimal Value	ASCII Character
0	00	^@ NUL	32	20	SPC
1	01	^A SOH	33	21	!
2	02	^B STX	34	22	"
3	03	^C ETX	35	23	#
4	04	^D EOT	36	24	$
5	05	^E ENQ	37	25	%
6	06	^F ACK	38	26	&
7	07	^G BEL	39	27	'
8	08	^H BS	40	28	(
9	09	^I HT	41	29	)
10	0A	^J LF	42	2A	*
11	0B	^K VT	43	2B	+
12	0C	^L FF	44	2C	,
13	0D	^M CR	45	2D	-
14	0E	^N SO	46	2E	.
15	0F	^O SI	47	2F	/
16	10	^P DLE	48	30	0
17	11	^Q DC1	49	31	1
18	12	^R DC2	50	32	2
19	13	^S DC3	51	33	3
20	14	^T DC4	52	34	4
21	15	^U NAK	53	35	5
22	16	^V SYN	54	36	6
23	17	^W ETB	55	37	7
24	18	^X CAN	56	38	8
25	19	^Y EM	57	39	9
26	1A	^Z SUB	58	3A	:
27	1B	^[ESC	59	3B	;
28	1C	^\ FS	60	3C	
29	1D	^] GS	61	3D	=
30	1E	^^ RS	62	3E	
31	1F	^_ US	63	3F	?

Decimal Value	Hexadecimal Value	ASCII Character	Decimal Value	Hexadecimal Value	ASCII Character
64	40	@	96	60	`
65	41	A	97	61	a
66	42	B	98	62	b
67	43	C	99	63	c
68	44	D	100	64	d
69	45	E	101	65	e
70	46	F	102	66	f
71	47	G	103	67	g
72	48	H	104	68	h
73	49	I	105	69	i
74	4A	J	106	6A	j
75	4B	K	107	6B	k
76	4C	L	108	6C	l
77	4D	M	109	6D	m
78	4E	N	110	6E	n
79	4F	O	111	6F	o
80	50	P	112	70	p
81	51	Q	113	71	q
82	52	R	114	72	r
83	53	S	115	73	s
84	54	T	116	74	t
85	55	U	117	75	u
86	56	V	118	76	v
87	57	W	119	77	w
88	58	X	120	78	x
89	59	Y	121	79	y
90	5A	Z	122	7A	z
91	5B	[	123	7B	{
92	5C	\	124	7C	|
93	5D	]	125	7D	}
94	5E	^	126	7E	
95	5F	_	127	7F	DEL

APPENDIX D

Prompts and Error Messages

This appendix alphabetically lists and defines the standard prompts and messages for the PINpad 1000SE device.

Messages or prompts that appear in rotation are shown together with a slash (/) separating the individual messages.

Message	Definition
BAD RAM	This prompt indicates the RAM test has failed.
CANCEL REQUESTED	After the PINpad device has received Packet Z7, this prompt is displayed whenever the [CLEAR] key is pressed or the controller requests a cancel termination.
CLEARING MKEYS	The terminal has detected an invalid MKEY and the user has pressed [CLEAR] to continue. The PINpad will clear all Master Keys and restart itself.
DES OK	This prompt indicates the DES Algorithm Reliability Test is passed.
ENTER AGAIN	This prompt requests you to enter the new master key again for verification.
ENTER NEW MKEY	This prompt requests you to enter the new master key (16 hexadecimal characters; use the decimal equivalents 0-9 for 0-9, 10-15 for A--F; See Appendix). Press [ENTER] after each hexadecimal character. Also be sure you have the new master key written down and stored in a safe place. The next prompt "ENTER AGAIN" will ask you to reenter the new master key for verification. *For test purposes, you can load the master key 0123456789ABCDEF, which translates into 0-15 decimal.*
ENTER N/6 KEY TO APPROVE	Press [N/6] key to decline the purchase amount.

Message	Definition
ENTER OLD MKEY	This prompt appears only if there is a master key already in the location to be changed. You must enter the current master key in the location (see instructions under ENTER NEW MKEY) so the PINpad can verify that it is the correct master key to change or press [*] to cancel the operation. If the verification is good, the "ENTER NEW MKEY" prompt is displayed. Otherwise "INVALID MKEY" is displayed.
ENTER PIN / PUSH "ENTER" / TOTAL / $ purchase amount	Alternate PIN entry request messages that appear (rotating) if the controller sends the PINpad the 70 message packet. The TOTAL message appears first then display amount of your purchase, followed by the prompt to enter your PIN, indicating the consumer PIN is required to complete the transaction.
ENTER Y/9 KEY TO APPROVE	Press [Y/9] key to approve the purchase amount.
ERR-BAD COM	This prompt shows that SUART Loopback Test has failed.
ERR-BAD DES	This prompt shows that the DES Algorithm Reliability Test has failed.
ERR-BAD PROM	This prompt shows that the PROM CKSUM test has failed.
ERR-NO KEY	This prompt indicates that a transaction has been initiated and there is no initial key initialized. Press [CLEAR] to return to the idle prompt.
ERR-NO MKEY	This prompt indicates that a transaction has been initiated and there is no master key present in the selected master key location. The transaction is canceled.
FILLING MEMORY	After the Power Cycle Memory Test has been initiated, this prompt is displayed to show that the PINpad unit is filling each nonvolatile memory location with uniquely known data for checking on power-up.
INVALID MEMORY	This prompt indicates that the Power Cycle Memory Test has failed.
INVALID MKEY	This prompt indicates that the old master key and the new master key are not matched during Master Key Insertion. If this prompt appears during the idle mode, it indicates that the PINpad has detected a memory corruption error. Press [CLEAR] to reinitialize memory. (Master Key and custom prompts must be reloaded.)

Message	Definition
INVALID MKEY INFO	This prompt indicates the presence of a Master Key Attributes Error. The selected master key is not allowed to use due to the invalid key usage, key algorithm, key mode, key version, key length. (For more information, see *GISKE Key Block Specification* VPN - 22986.)
KEY TST	This prompt indicates that the PINpad device has entered the keypad test in which the display echoes the key as each key is pressed. Check to see that pressing a key causes the display to show the value for that key in all 16 display positions, including the [#] key that echoes as an inverted "A." Press [CLEAR] to exit the keypad test.
MKEY ENTERED	This prompt indicates that the master key just entered has been verified and successfully loaded. The display returns to the idle prompt after three seconds.
PACKET ERR 0	This prompt is displayed with a short error beep when the PINpad has detected a packet that does not the correct format for user definable character function. The prompt will stay until you press any key.
PACKET ERR 1	This prompt is displayed with a short error beep when the PINpad has detected a packet that does not have an account number. The prompt will stay until you press any key.
PACKET ERR 2	This prompt is displayed with a short error beep when the PINpad has detected a packet with an account number less than eight digits long. The prompt stays until you press any key.
PACKET ERR 3	This prompt is displayed with a short error beep when the PINpad has detected a packet with an account number more than 19 digits long. The prompt stays until you press any key.
PACKET ERR 4	This prompt is displayed with a short error beep when the PINpad has detected a packet with invalid characters in the account number. The prompt stays until you press any key.
PACKET ERR 5	This prompt is displayed with a short error beep when the PINpad has detected a packet with invalid characters in the encrypted working key or C|D field error. The prompt stays until you press any key.
PACKET ERR 6	This prompt is displayed with a short error beep when the PINpad has detected a packet with minimum PIN length greater than maximum PIN length (see Z62 Accept and Encrypt PIN (with Custom Prompts)). The prompt stays until you press any key.

Message	Definition
PACKET ERR 7	This prompt is displayed with a short error beep when the PINpad has detected a packet with a NULL flag not set to "Y" or "N" (Q5 Alternate PROCESSING Prompt). The prompt will stay until you press any key.
PACKET ERR 8	This prompt is displayed with a short error beep when the PINpad has detected an [amount] digits is not within 3-8 digits, not including decimal point. The prompt will stay until you press any key.
PACKET ERR 9	This prompt is displayed with a short error beep when the PINpad has detected a packet with invalid working key attributes. The prompt will stay until you press any key. (For more information, see *GISKE Key Block Specification* VPN - 22986.)
PASSWORD	This prompt indicates that a password is required before you are allowed to enter into the Diagnostic Level 1 or Diagnostic Level 2 mode.
PIN PAD	This prompt indicates that the prompt "PIN PAD" has been chosen as the companion message of "PROCESSING." (See Option 0: PIN PAD / PIN PAL toggle under Q5 Alternate PROCESSING Prompt.)
PIN PAL	This prompt indicates that the prompt "PIN PAL" has been chosen as the companion message of "PROCESSING." (See Option 1: PIN PAD / PIN PAL toggle under Q5 Alternate PROCESSING Prompt.)
PIN VER number month year	This is the start-up prompt which displays the PINpad device version number and its release date.
PP INOPERATIVE	Indicates the PINpad device has transacted more than one million times, or low-battery problem has resulted in data loss. When this occurs, the PINpad device must be returned to VeriFone for initialization or maintenance. Call the VeriFone Customer Support Hot Line or contact your VeriFone representative.
PROCESSING PIN PAD	The standard processing message after Packets 70 or Z60 has been completed.
PROCESSING PIN PAL	The alternate processing message after Packets 70 or Z60 has been completed.
PROM OK	This prompt indicates that the PROM checksum test has passed.
RAM TST BEGIN	This prompt indicates the beginning of the RAM test.
RAM TST OK	This prompt indicates the RAM test has passed.
SUART OK	This prompt indicates the SUART LOOPBACK test has passed.
SUART TEST	Indicates the UART loopback test is in progress. Wait for the result. Press [*] to cancel the test and return to the idle prompt.
THANK YOU	This prompt is displayed after the PINpad device has received Packet Q2 from the controller.

Message	Definition
TOTAL / $amount of sale / ENTER PIN / PUSH ENTER	These prompts are alternately displayed after the PINpad device has received Packet 10 or 70. The TOTAL message appears first then amount of your purchase, followed by the prompt to enter your PIN, indicating the PIN is required to complete the transaction.
WHICH MKEY?	This prompt asks which master key is to be changed, following entry of the correct password. Master key locations range from 0 to 9.
FUNC NOT ALLOWED	The PINpad does not allow user to enter single length master key via keypad, due to the incorrect key management mode (when key management mode is in the 3DES mode).
******** `0.`0.`0.`0.`0.`0.`0.`0. MEMORY OK	These prompts are alternately displayed during the Power Cycle Memory Test. It will alternately flash this message and one of the two messages at right to indicate that it is running. Press [CLEAR] to end this test. • The "*" and "`0." are for you to check if the display segments can be lit and free from "ghosts." • "MEMORY OK" means the nonvolatile RAM is okay.
`0.`0.`0.`0.`0.`0.`0.`0. ******** *`0,	These prompts are shown in the "DISP TST" in Diagnostic Level 1. Please ensure the display segments are lit and free from "ghosts." If any segments do not illuminate, contact your VeriFone representative. The PINpad device immediately returns to the idle prompt after these have been shown.
<- - - - - - - - (scrolling arrow)	This is the standard idle prompt.
******** ########	The PINpad echoes each character of a master key entered through the keypad with a "#" or "*." The "#" represents the first eight entries and the "*" represents the remaining eight entries.
0 =CHG PROC MSG	Press the [0] key. The PINpad allows you to change the PROCESSING companion message from PINpad to PIN PAL, or from PIN PAL to PINpad.
1 = ONE MEM TST	Press the [1] key. The PINpad performs a RAM test, then returns to the idle prompt.
2 = CON MEM TST	Press the [2] key. The PINpad performs a RAM test continuously until [CLEAR] is pressed.
3 = PROM CKSUM	Press the [3] key. The PINpad verifies the checksum of its PROM content.
4 = KEY TST	Press the [4] key. The PINpad allows you to check the validity of the keypad until [CLEAR] is pressed.
5 = DISP TST	Press the [5] key. The PINpad device checks if the display is working properly.

Message	Definition
6 = SHOW SER NUM	Press the [6] key. The PINpad device displays the serial number stored in memory.
7 = SUART LOOP	Press the [7] key. The PINpad device checks validity of the software UART, the receiver and transmitter circuitries.
1 = P.C. MEM TST	Press the [1] key. The PINpad device performs the PULSE CYCLE memory test which does a destructive nonvolatile RAM test used in the manufacturing "burn in" process.
2 = INIT MKEY RAM	Press the [2] key. The PINpad device clears all master key RAM memory.
3 = LANGUAGES	Press the [3] key. The PINpad device allows you to select a different prompt language.
4 = DSP ALL MSG	Press the [4] key. The PINpad device allows you to display each individual prompt for the language selected.

APPENDIX E

Built-In Prompt Tables

ID	English	Spanish
1	0=SHOW BAUD RATE	0=CAMB MEN PROC
2	1=ONE MEM TST	1=UNA PRBA MEM
3	2=CON MEM TST	2=CON PRBA MEM
4	3=PROM CKSUM	3=PROM CKSUM
5	4=KEY TST	4=PRBA TECLA
6	5=DISP TST	5=PRBA PANTALL
7	6=SHOW SER NUM	6=MUESTRA # SER
8	7=SUART LOOP	7=SUART VUELTA
9	1=P.C. MEM TST	1=PC PRUEBA MEM
10	2=INIT MKEY RAM	2=INIC MAEST MEM
11	3=LANGUAGES	3=LENGUAJES
12	4=DSP ALL MSG	4=MSTR TODOS MNS
13	PROCESSING	PROCESANDO
14	PIN PAD	PIN PAD
15	PROCESSING	PROCESANDO
16	PIN PAL	PIN PAL
17	CANCEL REQUESTED	SESION CANCELADA
18	THANK YOU	GRACIAS
19	TOTAL	TOTAL
20	INVALID MEMORY	MEMORIA INV
21	DES OK	DES OK
22	ENTER AGAIN	ENT. OTRA VEZ
23	ENTER NEW MKEY	CLAV MAEST NUEVA
24	ENTER OLD MKEY	CLAV MAEST VIEJA
25	PROM OK	PROM OK
26	ERR-BAD COM	ERR-MALA COM.
27	ERR-BAD PROM	ERR-PROM DANADO
28	ERR-NO MKEY	NO CLAVE MAESTRA
29	FILLING MEMORY	LLENANDO MEMORIA
30	INVALID MKEY	CLAV MAESTRA INV
31	BAD RAM	ALG. RAM
32	MKEY ENTERED	CLAV MAEST ACEP.
33	PACKET ERR	ERR EN PAQ.
34	SUART OK	SUART OK

ID	English	Spanish
35	SUART TST	SUART PRUEBA
36	4E3001I 05/03	4E3001I 05/03
37	KEY TST	P.F REINTENTE
38	RAM TST BEGIN	PRUEBA RAM COMEN
38	RAM TST OK	PRUEBA RAM BIEN
40	WHICH MKEY ?	CUAL CLAV MAEST
41	ERR-BAD DES	ERR-ALG. DES
42	MEMORY OK	MEMORIA OK
43	PIN PAD	PIN PAD
44	PIN PAL	PIN PAL
45	PASSWORD	ENTRE CLAVE
46	ENTER PIN	ENTRE PIN
47	PUSH "ENTER”	ENTRE "ENTRAR"'
48	1=ENGLISH	1=ENGLISH
49	2=SPANISH	2=SPANISH
50	3=GERMAN	3=GERMAN
51	4=ITALIAN	4=ITALIAN
52	5=NORWEGIAN	5=NORWEGIAN
53	6=FINNISH	6=FINNISH
54	7=SWISS	7=SWISS
55	8=GREEK	8=GREEK
56	ENGLISH	ENGLISH
57	SPANISH	SPANISH
58	GERMAN	GERMAN
59	ITALIAN	ITALIAN
60	NORWEGIAN	NORWEGIAN
61	FINNISH	FINNISH
62	SWISS	SWISS
63	GREEK	GREEK
64	8=DSP BAUD RATE	8=DSP BAUD RATE
65	5=SET BAUD RATE	5=SET BAUD RATE
66	1=1200 BPS	1=1200 BPS
67	2=2400 BPS	2=2400 BPS
68	3=4800 BPS	3=4800 BPS
69	4=9600 BPS	4=9600 BPS
70	1200 BPS	1200 BPS
71	2400 BPS	2400 BPS
72	4800 BPS	4800 BPS
73	9600 BPS	9600 BPS
74	ERR-NO KEY	ERR-NO KEY
75	DUKPT	DUKPT

ID	English	Spanish
76	DUKPT END LIFE	DUKPT END LIFE
77	ENTER Y/9 KEY TO	ENTER Y/9 KEY TO
78	APPROVE	APPROVE
79	ENTER N/6 KEY TO	ENTER N/6 KEY TO
80	DECLINE	DECLINE
81	9=DSP KEY MGT	9=DSP KEY MGT
82	6=SET KEY MGT	6=SET KEY MGT
83	0=MASTER SESSION	0=MASTER SESSION
84	1=DUKPT	1=DUKPT
85	2=MASTER+DUKPT	2=MASTER+DUKPT
86	MASTER SESSION	MASTER SESSION
87	DUKPT	DUKPT
88	MASTER+DUKPT	MASTER+DUKPT
89		
90		
91	2=LANGUAGES	2=LENGUAJES
92	3=DSP ALL MSG	3=MSTR TODOS MNS
93	4=SET BAUD RATE	4=SET BAUD RATE
94	5=SET KEY MGT	5=SET KEY MGT
95	PLS WAIT	PLS WAIT
96	PP1000 TDES	PP1000 TDES
97	19200BPS	19200BPS
98	RESET COMPLETE	RESET COMPLETE
99	CLR COMPLETE	CLR COMPLETE
100	VERIFONE	VERIFONE
101	INVALID MKEY INFO	INVALID MKEY INFO
102	UNKNOW ERROR	UNKNOW ERROR
103	0=CHG PROC MSG	0=CHG PROC MSG
104	5=19200 BPS	5=19200 BPS
105	DUKPT-0 END LIFE	DUKPT-0 END LIFE
106	DUKPT-1 END LIFE	DUKPT-1 END LIFE
107	DUKPT-2 END LIFE	DUKPT-2 END LIFE
108	PP1000SE TDES	PP1000SE TDES
109	PED CERTIFIED	PED CERTIFIED
110	FUNC NOT ALLOWED	FUNC NOT ALLOWED

Prompt Table for Z2/Z3 Authentication

The following ROM Prompt Message table is only available in version 4E3002x and later releases of the firmware. These prompts are used with packets Z2 Display a String and Z3 Display Rotating Messages.

NOTE

The ROM prompt table contains only alphabetical characters. Non alphabetical characters and User Definable Characters are not stored in the ROM prompt table.

ID	ROM Prompt Table Message
0	ID
1	NO
2	PO
3	ZIP
4	EMP
5	JOB
6	GOV
7	CODE
8	DATE
9	IDNO
10	DEPT
11	PONO
12	USER
13	DATA
14	CLOCK
15	JOBNO
16	EQUIP
17	ENTER
18	EMPNO
19	DIVNO
20	BADGE
21	MOSYN
22	CLIENT
23	SERIAL
24	NUMBER
25	VEHTAG
26	DEPTNO

ID	ROM Prompt Table Message
27	SOCSEC
28	DRIVER
29	USERID
30	POSTAL
31	AHORRO
32	EQUIPCD
33	ENTERID
34	READING
35	CONTROL
36	WORKORD
37	VEHICLE
38	REENTER
39	CLOCKNO
40	PAYROLL
41	ENTERRC
42	ENTERSS
43	FINANCE
44	SAVINGS
45	ENTEREMP
46	ODOMETER
47	IDNUMBER
48	DIGITZIP
49	ENTERLIC
50	ENTERHUB
51	CASHBACK
52	DIVISION
53	ENTERREF
54	ENTERJOB
55	PONUMBER
56	GOVBADGE
57	SECURITY
58	DATEMMYY
59	CUSTOMER
60	MMDDYYYY
61	DRIVERID
62	ENTERTAG
63	CHECKING
64	ENTERMENU
65	ENTERDATA
66	ENTERDRVR
67	ENTERDEPT

ID	ROM Prompt Table Message
68	EQUIPCODE
69	DRIVERSID
70	ENTERAUTH
71	JOBNUMBER
72	WORKORDER
73	ENTERCARD
74	ENTERCODE
75	ENTERCLUB
76	ENTERYOUR
77	VEHICLEID
78	ENTERFOOD
79	CORRIENTE
80	ENTREDEPTO
81	ENTERSTORE
82	REENTERVEH
83	CUSTOMERID
84	ENTERVALUE
85	ENTERPHONE
86	ENTERROUTE
87	ENTERFLEET
88	ENTERJOBID
89	ENTREDATOS
90	ENTERJOBNO
91	ENTERCUSTID
92	REENTERYOUR
93	ENTERCLIENT
94	ENTERAMOUNT
95	ENTERSOCSEC
96	ENTERMEMBER
97	ROUTENUMBER
98	PLEASEENTER
99	ENTERUSERID
100	FLEETNUMBER
101	ENTERSTREET
102	ENTERCARDID
103	ENTERDRIVER
104	ENTERKEYFOB
105	ENTERDEPTNO
106	ENTERPOINTS
107	ENTERACCOUNT
108	ENTERCUSTREF

ID	ROM Prompt Table Message
109	ENTERMESSAGE
110	ENTERSECCODE
111	ENTERTRAILER
112	ENTERLOYALTY
113	CUSTOMERCODE
114	SECURITYCODE
115	ENTERPRODUCT
116	ENTERZIPCODE
117	DRIVERNUMBER
118	ENTERLICENSE
119	ENTERFLEETNO
120	ENTERCARWASH
121	ENTERVEHICLE
122	ENTERCONTROL
123	REENTERCNTRL
124	ENTERSERVICE
125	GOVERNMTBADGE
126	ENTEREMPLOYEE
127	ENTERIDNUMBER
128	ENTERDRIVERID
129	ENTERFLEETPIN
130	ENTERCASHBACK
131	ENTERODOMETER
132	ENTREIDCHOFER
133	ENTRENUMVEHIC
134	ENTREODOMETRO
135	ENTERPERSONAL
136	DRIVERLICENSE
137	ENTERFREQUENT
138	ENTERDIGITZIP
139	ENTERCUSTOMER
140	ENTERVERIPASS
141	PLEASEREENTER
142	ENTERCHARGETO
143	VEHICLENUMBER
144	ENTERCUSTDATA
145	REENTERDRIVID
146	ENTERUSERDATA
147	ENTERCUSTCODE
148	ENTERLOCATION
149	POSTALFINANCE

ID	ROM Prompt Table Message
150	ENTERREFERENCE
151	ENTERAUTHNUMBR
152	ENTERHUBNUMBER
153	ENTERHUBOMETER
154	ENTERTRAILERID
155	ODOMETERNUMBER
156	ENTERDRIVERLIC
157	ENTERTRAILERNO
158	REENTERCONTROL
159	PREVIOUSSTREET
160	REENTERVEHICLE
161	ENTREIDUSUARIO
162	ENTEREXPIRDATE
163	ENTERVEHICLEID
164	ENTERBIRTHDATE
165	ENTERDOBMMDDYY
166	ENTERFLEETDATA
167	REENTERZIPCODE
168	REENTERSECCODE
169	ODOMETERREADING
170	ENTERMEMBERSHIP
171	ENTEREXPIRATION
172	REENTERODOMETER
173	REENTERDRIVERID
174	ENTERCUSTOMERID
175	RESTRICTIONCODE
176	PREVIOUSZIPCODE
177	ENTERFLEETNUMBER
178	REMAININGBALANCE
179	ENTERROUTENUMBER
180	ENTERDRIVERNUMBER
181	ENTERCUSTOMERCODE
182	ENTERSECURITYCODE
183	ENTERCUSTOMERDATA
184	ENTERVEHICLENUMBER
185	ENTERDRIVERLICENSE
186	ENTEREXPIRATIONDATE
187	ENTERODOMETERREADING
188	ENTERRESTRICTIONCODE

Manual Diagnostic Procedures

There are two built-in diagnostics modes, Level 1 Diagnostic and Level 2 Diagnostic. From these modes, user can perform various tests and operation using the PINpad keypad.

Level 1 Diagnostic

You'll need your system password to enter Diagnostic Level 1 Upon entry, the PINpad will cycle through a menu of eight available diagnostics, which include changing messages, performing one-time and continuous RAM, PROM check, UART loopback tests, and display baud rate. To access this diagnostic level:

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press 83746 followed by [ENTER].
	If the password is incorrect, the display will return to idle prompt. Otherwise, the PINpad will repeatedly cycle through the diagnostic menu until a selection is made.
/=SHOW P SER NUM 0=CHG PROC MSG 1=ONE MEM TST 2=CON MEM TST 3=PROM CKSUM 4=KEY TST 5=DISP TST 6=SHOW SER NUM 7=SUART LOOP 8=DSP BAUD RATE 9=DSP KEY MGT	The terminal will cycle through the maintenance and diagnostic menu. Press the numeric key (0-9) that corresponds to the desired selection. If you want to return to the idle prompt, press [CLEAR]. **Note:** According to the mode setting, different mode might have different menu items (TBD).

SHOW P SER NUM

Select the backspace to display the Permanent Unit Serial Number (PUSN).

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press Backspace.
/=SHOW P SER NUM…	
serial number	Indicates the permanent unit serial number. Compare the serial number to the one on the external label.
	Press [CLEAR] to return to idle prompt.

CHG PROC MSG

Select option 0 to toggle between PIN PAD/PROCESSING (the default) or PIN PAL/PROCESSING displays.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [0].
0=CHG PROC MDG…	
PIN PAL/ PIN PAD	Indicates you toggled to the PIN PAL/PIN PAD display. Displays for three seconds then returns to the idle prompt.

ONE MEM TST

Select option 1 to initiate a single RAM memory test.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [1].
1=ONE MEM TST…	
RAM TST BEGIN	The PINpad will run the RAM memory test.
RAM TST OK	RAM test completed without error. Idle prompt follows.

CON MEM TST

Select option 2 to initiate a continuous RAM test.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [2].
2=CON MEM TST…	
RAM TST BEGIN	The PINpad runs the continuous RAM test.
RAM TST OK	Press and hold down [CLEAR] to return to the idle prompt.

PROM CKSUM

Select option 3 to initiate a PROM checksum test from the PINpad.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [3].
3=PROM CKSUM…	
PROM OK	Indicates test completed without error. Idle prompt follows.

KEY TST

Select option 4 to initiate a keypad reliability test.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [4].
4=KEY TST…	
xxxxxxx	Press any key on the keyboard.
	Number 0-9 or an upside down A (for [ENTER] key) is repeated 8 times on the display.
	Press [CLEAR] to return to idle prompt.

DISP TST

Select option 5 to verify the PINpad display is working properly.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [5].
5=DISP TST…	
0'0'0'0'0'0 ******	These three tests patterns will appear, one after another, on the display panel.
*'0.	Check that all segments of the pattern are lighting properly. Be sure the third test only display three characters.
	If more characters are display, the display is "ghosting."
	If some of the segments are not lit, or if the display does not match what you see in this manual then the unit need to be repaired.
	After displaying the sets, the PINpad returns to the idle prompt.

SHOW SER NUM

Select option 6 to display the serial number stored internally for the PINpad.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [6].
6=SHOW SER NUM…	
serial number	Shows the unit serial number.
	Press [CLEAR] to return to idle prompt.

SUART LOOP

Select option 7 to check the receiver/transmitter circuitry.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [7].
7=SUART LOOP…	
SUART TST	Indicates UART loopback test started. Wait for results.
SUART OK/ ERR-BAD COM	If "SUART OK" is displayed, the test was successful. If "ERR-BAD COM" is displayed, the test failed.

DSP BAUD RATE

Select option 8 to display the PINpad current baud rate.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].
Menu cycle...	Press [8].
8=DSP BAUD RATE…	
xxxx BPS	Displays the current baud rate in one of 1200 / 2400 / 4800 / 9600 / 19200 BPS for 3 seconds then return to idle prompt.

DSP KEY MGT

Select option 8 to display the PINpad current key management mode.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [3].
PASSWORD	Press **83746** followed by [ENTER].

Display	Response
Menu cycle... 9=DSP KEY MGT…	Press [9].
Xxxxxxx	Displays the current key management, it will be one of the following: • 'MASTER SESSION' • 'DUKPT' • 'MASTER+DUKPT' • 'SEMP/4B'

Level 2 Diagnostic

Diagnostic level 2 allow you to reinitialize and clear RAM and select and display different prompt languages and set PINpad baud rate.

NOTE

This level requires an additional diagnostic password and is intended for field service and manufacturing personnel only.

To access this diagnostic level:

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER]. If the password is incorrect, the display will return to idle prompt. Otherwise, the PINpad will repeatedly cycle through the diagnostic menu until a selection is made.
1=P.C.MEM TST 2=INIT MKEY RAM 3=LANGUAGES 4=DSP ALL MSG 5=SET BAUD RATE 6=SET KEY MGT	The terminal will cycle through the menus. Press the numeric key (1-6) that corresponds to the desired selection. **Note:** According to the mode setting, different mode might have different menu items (TBD).

P.C. MEM TST

Select option 1 to perform the nonvolatile RAM initialization test used in the manufacturing "burn-in" process. In nonvolatile initialization, the master key buffer is emptied and the correct master key checksum is calculated.

CAUTION

This option should be used to reinitialize the PINpad only.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].

Display	Response
Menu cycle...	Press [1].
1=P.C.MEM TST…	
FILLING MEMORY	The PINpad loads each memory location with unique data.
********	These prompt are display repeatedly unless the unique data in one of the memory locations was changed, and will prompt as: Press [CLEAR] in any case to return to the idle prompt.
"0.'0.'0.'0.	
MEMORY OK	
********	
ILLEGAL MEMORY	

INIT MKEY RAM

Select option 2 to clear all master keys RAM.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].
Menu cycle...	Press [2].
2=INIT MKEY RAM…	

LANGUAGES

Select option 3 to set the language displayed in prompts.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].
Menu cycle...	Press [3].
3=LANGUAGES…	
Menu cycle...	This menu shows the language available in the operating system. Press the numeric key (1-8) that corresponds to the desired language.
1=ENGLISH	
2=SPANISH	
(language)	The selected language name will appear for confirmation. For example, If you selected "2," the display will show "SPANISH."
	Press [CLEAR] to return to the idle prompt.

DSP ALL MSG

Select option 4 to display each individual prompt for the language selected in "LANGUAGES".

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].
Menu cycle...	Press [4].
4=DSP ALL MSG…	
0=CHG PROC MSG	Press [ENTER].

Display	Response
1=ONE MEM TST	Press [ENTER].
2=CON MEM TST …	The PINpad will continue to display another prompt each time you press [ENTER] until it reaches the end of the prompt table. Press [CLEAR] to return to the idle prompt.

SET BAUD RATE

Select option 5 to set the RS-232 baud rate of PINpad.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].
Menu cycle...	Press [5].
5=SET BAUD RATE…	
1=1200 BPS 2=2400 BPS 3=4800 BPS 4=9600 BPS 5=19200 BPS	Alternate display these 5 prompts, by entry one of 1~5 to select the desired baud rate. **Note:** Pressing [CLEAR] will return to idle prompt without setting. Pressing other key, the PINpad will alternate display these 5 prompts again for re-entry.
xxxx BPS	To display set baud rate for 3 seconds then return to idle prompt.

SET KEY MGT

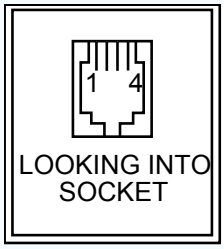
Select option 6 to set the key management mode of PINpad.

Display	Response
(idle prompt)	Press [CLEAR] immediately followed [2].
PASSWORD	Press **844747746** followed by [ENTER].
Menu cycle...	Press [6].
6=SET KEY MGT…	
0=MASTER SESSION 1=DUKPT 2=MASTER+DUKPT	Alternate display these prompts, by entry one of 0~2 to select the desired key management. When changing the key management mode of PINpad, key erasing rules are applied, please refer to the 15 Refresh PINpad Key Management Mode for more details. **Note:** Pressing [CLEAR] will return to idle prompt without setting. Pressing other key, the PINpad will alternate display these 4 prompts again for re-entry.
xxxxxxxx	To display set key management for 3 seconds then return to idle prompt.

APPENDIX A

Pinouts

The table in this appendix shows the pinouts for the PINpad 1000SE connector.

Connector	Pin	Description
	1	Circuit ground
	2	Serial receive (serial data to PINpad)
	3	Serial transmit (serial data from PINpad)
	4	+9 volts DC (VDC) unregulated power

AC *Alternating Current*--used as a primary source of power by power packs and power supplies.

ACK The acknowledgement control character sent from one device to another to indicate the message packet transmitted passed the block check.

Algorithm A set of rules for solving a problem.

Alphanumeric Capable of utilizing both alphabetic and numeric characters such as a display panel, keypad or computer keyboard.

Application A program consisting of special codes stored in memory used to control a PINpad and its operations.

ASCII An abbreviation for American Standard Code for Information Interchange. This standard code is used for transmitting data and is composed of 128 characters in 7-bit binary format.

Authorization The host computer determines if the requestor is authorized to transfer funds using account history and PIN entry.

Bar code Optical binary code imprinted on merchandise in retail stores.

Bar code wand A pencil- or wand-shaped optical scanner for reading bar codes.bar code, in a left-to-right or right-to-left direction.

Baud The number of times per second that a system, especially a data transmission channel, changes state. The state of a system may represent a bit, digit, or symbol. For a POS terminal, the baud rate indicates the number of bits per second that are transmitted or received by the terminal's serial ports and modem.

Buffer An electronic device within the terminal that allows for the temporary storage of data.

Character An element of a given character set. Also, the smallest unit of information in a record. A letter, numeral, or other symbol to express information.

Code The set of rules for representing data by groups of binary digits.

Companion Message The message that displays in rotation with another message.

Control Characters Transmitted characters having special or significant meaning to the receiving device.

Controller The master device or terminal that directs the PINpad's operations in the application.

Custom Prompts Information on the display panel created specially for a particular company or user.

Data Information used by the PINpad device that relates to a specific transaction or operation. Information prepared, often in a particular format, for a specific purpose. Data is to be distinguished from applications or program instructions.

Debit Card Used in many of the same transactions as a credit card except no credit is given and the holder must have funds in his or her account to immediately cover the transaction.

Decryption A decoding process that allows a terminal or host computer with the correct keys to decrypt and read previously encrypted data.

Destructive Diagnostic A process that reads or writes data, erasing what was originally stored.

Diagnostics Techniques employed for detection and isolation of malfunctions and errors in programs, systems, and devices. In a diagnostic test, a program or routine is run to detect failures or potential failures. These tests and routines help detect and isolate problems in a terminal or peripheral device.

Display Panel The small screen on the PINpad that shows numerals, letters, and punctuation symbols in selected fonts, graphics in various formats, information entered from the keypad, as well as system prompts and messages.

Download To transfer files or data from a host

computer or sending terminal over a communication link to a receiving terminal.

DUKPT *Derived Unique Key Per Transaction*–a method used to enhance security provided by PIN encryption.

Echo A process where the receiving device retransmits or "echoes back" transmitted data so that the originating device can ensure that the data sent was received correctly.

Electronic Signature Like the signature on a check, the PIN is the electronic checking account signature.

Encryption An encoding process using master or transaction keys that makes confidential data unreadable to unauthorized persons.

EOT The End of Transmission control character sent from one device to another to indicate the end of each transmission.

Error Message A message that is displayed on the PINpad device when data is entered incorrectly.

External Label or Serial Number The serial number printed on the label on the bottom of the PINpad unit casing.

File A collection of records.

File authentication A process through which one proves and verifies the origin of a file, the identity of the sender, and the integrity of the information it contains.

Firmware The basic instructions built into the PINpad, stored in ROM, and executed automatically.

Fixed prompt A system prompt or message stored as part of system firmware in terminal memory. Fixed prompts appear on the terminal display to alert the user to specific system occurrences or malfunctions, and to prompt the user to enter specific information or select options.

Flag A programmed indicator, such as a symbol, signal, character or digit used for identification.

Hexadecimal The hexadecimal number system has a base of 16 and uses the symbols 0-9 and A--F.

Host An authorizing center computer used to process transactions; also called a host computer.

Idle Prompt The information shown on the display panel when the PINpad device is not performing an operation and is waiting for a customer to begin a transaction.

Internal Serial Number The serial number of the PINpad device stored in memory.

Input The data to be processed by the PINpad device and the host computer.

Instant Checking Electronic and virtually immediate transfer of funds from one bank account to another when the financial transaction takes place.

I/O Short for *Input, Output*.

I/O Device The PINpad device is one; equipment used to submit data to the host and to provide information from it.

Line cord A telephone-type cord with modular plugs on each end to connect the base station to a dial-up telephone line.

Key A control field.

Loopback A method of testing in which a known data item is sent to a device and returned to be checked.

Message Packet Format A method of framing messages, rather than exact timing, which allows devices to recognize the beginning and end of each block or message.

Microcomputer A small computer with less memory capacity and speed than the larger mainframes and minicomputers.

NAK Short for *Negative Acknowledgement Character*. The control character sent from one device to another to indicate the message packet transmitted did not pass the block check.

Packet A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a composite whole through a packet switching network. Any message that exceeds the maximum size is partitioned and carried as several packets.

Password A group of characters that identify a user to the system so that they can gain access to the system or part of that system. Passwords are used to ensure the security of computer systems by regulating the amount of access freedom. The password used to enter system mode is called the *system mode password*. In the VeriFone Global Template file system, each file group (Groups 1–15) also has its own password.

Peripheral device In a computer system, any equipment that provides the processing unit with outside communication. Typical peripheral devices for a POS terminal include PINpads, bar code wands, and check readers.

PIN *Personal Identification Number*. A 4- to 16-digit confidential code or electronic signature used by card holders to identify themselves as the proper users of a credit or debit card to the host computer.

POS terminal A terminal used at the *point of sale*, which is usually at a merchant site where a customer pays for goods or services received. Information concerning the sale can be entered into the terminal and transmitted to a remote host computer for verification and processing.

Prompt A short message, sent from a process to a user, indicating that the process expects the user to present fresh data. For example, a prompt appears on the terminal display asking the user to enter specific information.

Protocol An agreement that governs the procedures used to exchange information between cooperating entities. For example, protocols govern the format and timing of messages exchanged between devices in a communication system, such as between a terminal and a host computer.

Scroll To move all or part of the information displayed on a screen up or down, left or right, to allow new information to appear.

SI Short for *Shift In*; the beginning of PINpad device message packet.

SO Short for *Shift Out*; the end of message packet delimiter.

STX Short for *Start of Text*, the beginning of a PINpad message packet.

SUART Short for Software Universal Asynchronous Receiver/Transmitter. See UART.

Transmission Sequence Typical sequence of communications between devices for a particular message packet.

UART Short for *Universal Asynchronous Receiver/Transmitter*; a device chip which provides the connection of the PINpad device (a serial I/O device) to the microprocessor.

Variable A string of characters that denotes some value stored within the computer and that can be changed during execution. A variable may be internal to a program, in which case it is held in memory, or external if the program must perform an input operation to read its value.

Void To clear or delete a transaction.

INDEX

Q

R

S

T

U

V

Z

VeriFone, Inc.
2099 Gateway Place, Suite 600
San Jose, CA, 95110 USA
Tel: (800) VeriFone (837-4366)

www.verifone.com

PINpad 1000SE

Reference and Programmers Guide

VeriFone Part Number 22903, Revision E