PRISM

TRUSTED TRANSACTIONS

A subsidiary of NET1 UEPS Technologies, Inc.

Key Component Entry Device (KCED) Installation & User Guide

(for Prism HSMs)

Document Number: 0560-00157

Version: 11

Issue Date: September 2021

Document Information	
Title	Key Component Entry Device (KCED) Installation & User Guide
Document Number	0560-00157
Document Version	11
Client	Prism
Synopsis	This guide describes the installation and usage of the KCED in conjunction with the TSM500 and TSM500i family of hardware security modules (HSMs) supplied by Prism.
Issue Date	September 2021

Amendment History

Version	Description	Date
1	Original	30/06/2001
2	Updated power-supply pictures	
3	Modified to suit VeriFone SC5000.	08/07/2003
4	Changed Pinpad references to Key Component Entry Device	09/03/2004
5	Added note stating which KCED firmware is compatible with TSM310 and TSM410. Updated DB9 port connection info for the TSM410.	13/06/2006
6	Updated version number of Document	04/08/2006
7	Updated Prism logos, included new TSM410 photo & new KCED photo with labelling	17/05/2007
8	Updated to include the TSM500 HSM and ML30 terminal. Removed references to TSM310 and TSM400.	07/07/2010
9	Updated images. Removed SC5000 references.	30/04/2013
10	Updated images and text to accommodate the iPP320 terminal.	12/03/2014
11	Updated images and text to accommodate the Lane 3000 terminal. Removed references to ML30 and TSM410.	01/09/2021

Table of Contents

1. Scope

This guide describes the process for installing the Key Component Entry Device (KCED) for use with the TSM500 and TSM500i hardware security modules (HSMs) supplied by Prism. The guide also gives information on using the KCED. TSM500 refers to both the TSM500-PCIe / TSM500i-PCIe and TSM500-NSS / TSM500i-NSS.

2. Unpack and Check Contents

Unpack and verify the contents of the shipping boxes. If anything is missing or damaged, please contact the supplier.

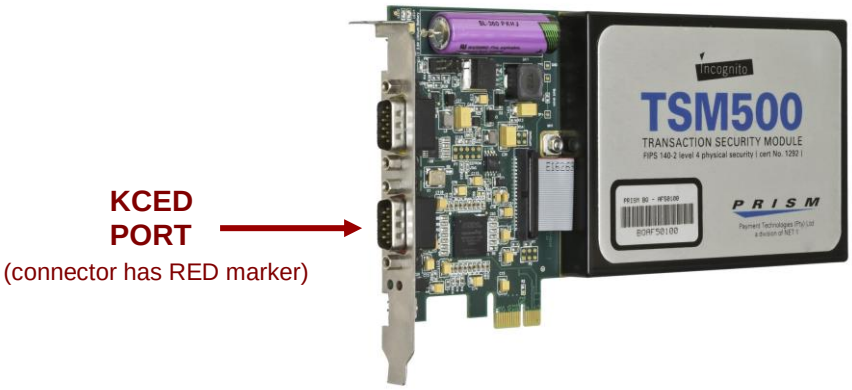
KCED kit:

- KCED - a pin pad terminal with custom KCED firmware developed by Prism (the terminal used is typically an Ingenico Lane 3000 or Ingenico iPP320).
- Serial cable, permanently attached to the KCED
- Universal switching +9V DC Power Supply with integrated DC Jack Cable
- AC Mains Cable (not supplied to countries outside of South Africa)

Example of KCED Kit
(Exact terminal & accessories may differ from picture)

3. HSM Overview

Prism manufactures various HSMs that require the Key Component Entry Device to enter keys in component form. The TSM500-PCIe HSMs fit inside a Server and connect to the KCED via their connector bracket. The TSM500-NSS connects via a connector on it's front panel. **The KCED connection points for each HSM are illustrated below.**



TSM500-PCIe Hardware Security Module

TSM500-NSS Hardware Security Module

4. KCED Hardware Installation

For successful installation of a KCED onto any of the TSM500-PCIe, it is not necessary to remove the HSM from the PC server case. Connection to these HSMs is via the rear connector plate of the HSM.

For the TSM500-NSS connection is simply via the marked connector on the front panel.

STEP 1: Ensure that the TSM500-PCIe has been correctly installed in the PC / Server. *TSM500-PCI Installation Guide* (Doc. No. PR-D2-0859).

STEP 2: Connect the DC plug (from the DC power supply) to the back of the DB9 connector on the KCED serial cable.

STEP 3: **FOR TSM500-PCIE:**
Connect the DB9 connector from the KCED (with DC jack connected) to the appropriate DB9 connector (with **RED** marking) on the TSM500-PCIe rear connector bracket.

FOR TSM500-NSS:
Connect the DB9 connector from the KCED (with DC jack connected) to the front panel connector labelled “KCED” on the TSM500-NSS.

STEP 4: Connect the DC power supply to the mains and switch on.

STEP 5: After power-up you should see the following start-up message displayed on the LCD of the KCED:

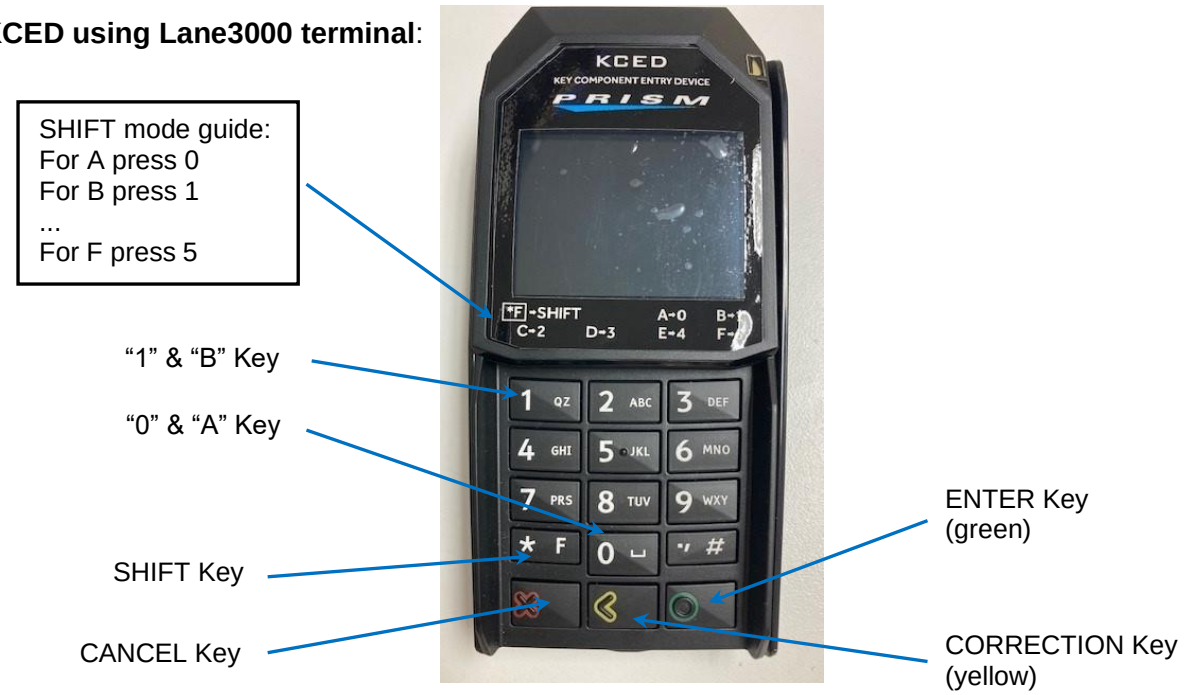
SmartCard Term v2.00 (the version must be v2.00 or later)

5. Using the KCED

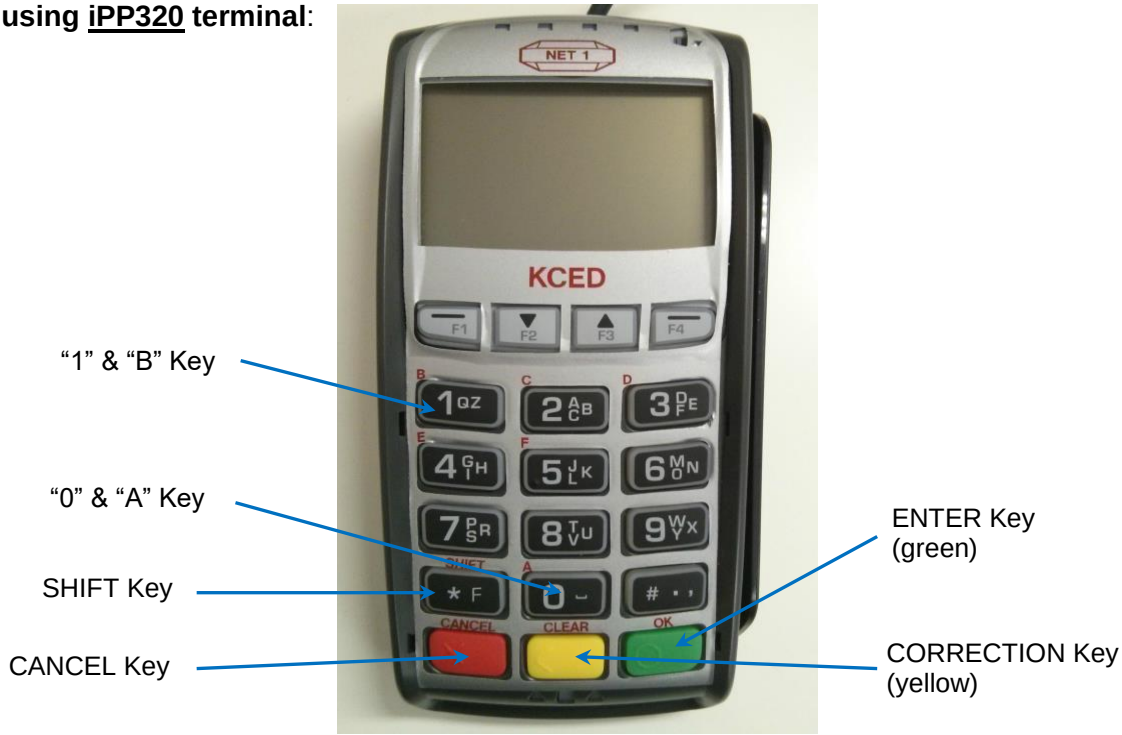
The KCED makes use of commercially available pin pad terminals with custom KCED firmware provided by Prism. Depending on date of purchase, the terminal used may differ.

The iPP320 keypad comes fitted with a key-identity overlay that identifies the "SHIFT" key and the hexadecimal keys "A" – "F". The two pictures below identify the various keys on the two most common terminals used for the KCED.

KCED using Lane3000 terminal:



KCED using <u>iPP320</u> terminal:



To enter the digits 0 through 9 press the appropriate button on the keypad.

To enter the letters A – F first press the **SHIFT** key on the keypad, which is located in the top right corner of the keypad. This will put the system into shift-lock mode and you will see the "**^**" character in the top right of the screen. In this mode the buttons marked 0, 1, 2, 3, 4 and 5 are used for A through F. To deactivate the shift-lock mode press the **SHIFT** key again and the "**^**" character will disappear from the top right of the screen indicating that the system is in normal mode once again.

The Correction key may be used to delete the previous key entered. The functions of the Correction and Cancel keys are further described in Section 6.

The area used on the KCED screen is 16 characters wide by 2 lines high.

If the HSM is expecting a key entry and there is no activity on the keypad (i.e. no key presses on the KCED for a specified period of time), then the HSM will cause the KCED to display a message similar to that shown below.

```
Timeout error
Please try again
```

Should the timeout between key presses for the entry of key components be insufficient they can be increased. This timeout can be modified via the appropriate API call to the HSM.

Other possible error messages are:

```
Comms error
Please try again
```

and

```
Overflow error
Please try again
```

There are three types of keys: single, double and triple length keys. Keys can be entered in two or three components. The components are stored in the HSM and are combined to produce the key.

A ***single length*** key component is 64 bits long, which means that for each component you need to enter 16 hexadecimal (hex) digits into the KCED, where each hex-digit represents 4 bits of data.

A ***double length*** key component is 128 bits long, which means that for each component you need to enter 32 hexadecimal (hex) digits into the KCED, where each hex-digit represents 4 bits of data. Key entry is divided into 2 parts owing to the 16 character width of the screen.

A ***triple length*** key component is 192 bits long, which means that for each component you need to enter 48 hexadecimal (hex) digits into the KCED, where each hex-digit represents 4 bits of data. Key entry is divided into 3 parts owing to the 16 character width of the screen.

6. Entering Key Components

The sequence will begin with the text shown below displayed on the KCED screen. Press OK on the KCED keypad to proceed to the next screen.

```
Ready for Entry
of 1st component
```

At this point the key component may be entered using the “0” to “9” and “A” to “F” keys.

If you press the red Cancel key (“RED”) at any point during the key entry process, the HSM will abort and cause the KCED to display the following message:

```
Entry of compo-
nents ABORTED
```

If at any point you enter the wrong digit you can make a correction by using the yellow Correction key on the keypad. This button functions in the same way as a backspace button functions on a PC. Pressing the yellow Correction key deletes one character at a time. If you are deleting in the second part of a double length component, deleting character 17 and then pressing the Correction key returns you to the first part of the component (i.e. to character 16).

At any point the key entry process can be aborted by pressing the red Cancel key on the keypad, which results in the key entry being terminated with an error.

If you are entering a **single length component** the screen will look like the sample below. Press OK (green key) to proceed to the next screen.

```
Component 1     ^
0123456789ABCDEF
```

When you have entered all characters in a key component, press the OK key to accept and proceed to the next step. (The OK key only works when all the characters in a component are present.) The KCED screen will display the following message:

```
Comp1 entered
Successfully
```

If you are entering a **double length component** the screen will look like the sample below:

```
Comp1 1st part ^
0123456789ABCDEF
```

When you are entering a double length component, after entering the 16th digit the screen will display the second part (i.e. “Comp1 2nd part”) and you can type in the remaining 16 hex digits for the 1st component and press OK.

As with entering a single length component, you will then be presented with the following text displayed on the screen:

```
Comp1 entered
Successfully
```

Press the green OK key to proceed to the next screen and the following text is displayed on the screen.

```
Ready for Entry
of 2nd component
```

Press OK to proceed to the next screen and the following text will be displayed on the screen.

```
Comp2 1st part
```

Proceed to type in both parts of the second component and press OK to proceed to the next screen.

```
Comp2 entered
Successfully
```

Press OK and the last screen, as shown below, will then be displayed – the message remains on the screen for about 2 seconds and is then cleared.

```
All components
Entered OK
```

If you are entering a **triple length component** the screen will look as follows:

```
Comp1 1st part ^
0123456789ABCDEF
```

When you are entering a triple length component, after entering the 16th digit the screen will display the second part (i.e. “Comp1 2nd part”) and you can type in the next 16 hex digits for the 1st component. After entering the second 16 digits the screen will display the third part (i.e. “Comp1 3rd part”) and you can enter the last 16 digits and press OK.

As with entering a single length component, you will then be presented with the following text displayed on the screen:

```
Comp1 entered
Successfully
```

Press the green OK key to proceed to the next screen and the following text is displayed on the screen.

```
Ready for Entry
of 2nd component
```

Press OK to proceed to the next screen and the following text is displayed on the screen.

```
Comp2 1st part
```

Type in all three parts of the second component and press OK and the following text is displayed on the screen.

```
Comp2 entered
Successfully
```

Press OK and the last screen, as shown below will then be displayed – the message remains on the screen for about 2 seconds and is then cleared.

```
All components
entered OK
```

Please note: It is possible to have ***three*** components, in which case the third component procedure will follow the same pattern as for the previous two.

7. Acronyms & Abbreviations

AC	Alternating Current
API	Application Programming Interface
DC	Direct Current
hex	hexadecimal (0, 1, 2, …9, A, B, … F)
HSM	Hardware Security Module
KCED	Key Component Entry Device (or Hand Held Terminal)
LCD	Liquid Crystal Display
PC	Personal Computer
RJ	Registered Jack (connector standard)
TSMxxx	Prism's range of HSMs (also known as Transaction Security Modules)

8. Support

Support is provided during business hours (weekdays 8:00 to 17:00 South African Standard Time, GMT+02). Services that are not covered by a warranty may be subject to a standard charge rate.

Send a support request via e-mail to info@prism.co.za. Although we endeavour to attend to all support requests as soon as possible, please allow up to 1 working day for a response.

Before contacting support, please consult the *TSM500 and TSM-WEB User Guide*. This guide will help you to quickly resolve common problems, and also indicates the information you should supply in a support request in order to ensure prompt and accurate service.

You can also contact us via telephone: +27 31 2675500

Visit our website: www.prism.co.za