Security Policy for Payment Pebble tCR2.1 PED

Thumbzup UK Limited
Suite 105 Viglen House
Alperton Lane
London
HA0 1HD
United Kingdom

Document Control

Title	Security Policy for Payment Pebble tCR2.1 PED
Document Number	PL-THB-18322
Document Version	1.11
Publish Date	December 22, 2020 at 01:20:57 AM
Current Status	Approved
Confidentiality Level	Public

Revision History

Date	Version	Author	Change notes
2018/05/28	1.0	Selwyn Jackson	Initial version
2018/10/30	1.1	Selwyn Jackson	Updated images
2018/10/30	1.2	Selwyn Jackson	Updated key table
2019/03/27	1.3	Selwyn Jackson	Added guidance for cardholders
2019/06/03	1.4	Selwyn Jackson	Updated label
2019/06/03	1.5	Selwyn Jackson	Updated firmware version
2020/02/24	1.6	Selwyn Jackson	Updated firmware version images
2020/05/30	1.7	Selwyn Jackson	Updated firmware version images to v3.2.6
2020/07/07	1.8	Selwyn Jackson	Added .x to hardware versions in captions Added inspection of the versions Updated environmental conditions Updated device deactivation and firmware updates
2020/07/26	1.9	Selwyn Jackson	Bluetooth changed to Bluetooth Low Energy
2020/12/04	1.10	Selwyn Jackson	Added unattended mode; Version 3.2.7
2020/12/16	1.11	Selwyn Jackson	Added installation details for unattended mode

Document Approval

Date	Version	Approval Description / References
2018/05/29	1.0	https://jira.thumbzup.com/browse/DOC-61
2018/11/06	1.1	https://jira.thumbzup.com/browse/DOC-124
2019/03/25	1.2	https://jira.thumbzup.com/browse/DOC-156
2019/03/28	1.3	https://jira.thumbzup.com/browse/DOC-160
2019/06/04	1.4	https://jira.thumbzup.com/browse/DOC-181
2019/11/18	1.5	https://jira.thumbzup.com/browse/DOC-296
2020/02/24	1.6	https://jira.thumbzup.com/browse/DOC-335
2020/05/30	1.7	https://jira.thumbzup.com/browse/DOC-395
2020/07/07	1.8	https://jira.thumbzup.com/browse/DOC-406
2020/07/27	1.9	https://jira.thumbzup.com/browse/DOC-431
2020/12/16	1.10	https://jira.thumbzup.com/browse/DOC-542
2020/12/22	1.11	https://jira.thumbzup.com/browse/DOC-546

Table of Contents

1. Introduction....5
2. Purpose....5
3. General description....5
3.1. Product description....5
3.2. Product type....6
3.3. Product identification....6
4. Installation and user guidance....7
4.1. Initial inspection....7
4.2. Guidelines....8
4.3. Communications and security protocols....8
4.4. Configuration....8
5. Operation and maintenance....9
5.1. Periodic inspection....9
5.2. Self-test....10
5.3. Roles and Responsibilities....10
5.4. Tamper response....10
5.5. Privacy shield....10
5.6. Firmware updates....11
5.7. Device activation and deactivation....11
5.8. Battery charging....11
5.9. Environmental conditions....11
6. Security....12
6.1. Security....12
6.2. PIN entry....12
6.3. Communications....14
6.4. Software Management....14
7. Key Management....14
7.1. List of keys in tCR2.1....15
7.2. Firmware application program interfaces (APIs)....15
8. Reference documents....15
9. Glossary....16

1. Introduction

The Payment Pebble® tCR2.1 is a small mPOS PED device that is used in conjunction with a smart phone. A unique PIN entry method is used to ensure that the PIN is not compromised when using the smart phone as the user interface for the tCR2.1.

Various security mechanisms are used to ensure that the device tCR2.1 is secure. Any attempts to access or penetrate it the tCR2.1 will cause in all sensitive data in the tCR2.1 to be destroyed and the device self-destructs and becomes totally unusable.

2. Purpose

This document provides the policies for the security requirements as required by B20 in the PCI POI Version 5.1 Security Requirements [1]. It describes how the device should be used to maintain security and to comply with PCI. Any deviation from the approved use of the device will invalidate the PCI PTS POI approval. This document can be placed in the public domain.

3. General description

3.1. Product description

The tCR2.1 is a small device that connects to a smart phone via Bluetooth Low Energy (BLE) or USB. All communications between the tCR2.1 and the smart phone is done through these ports. The USB port is also used for charging the device.

All transactions are processed online, and the smart phone's network connectivity is used to access the Transaction Service. The connectivity can be via WiFi or GSM.

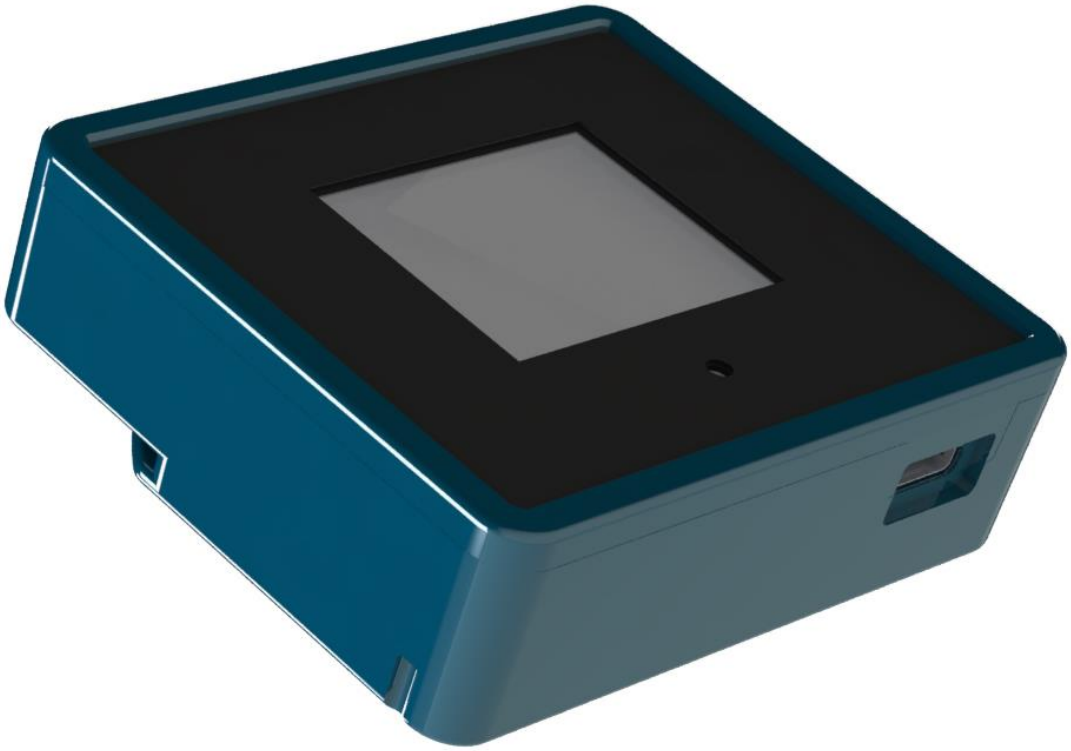

Figure 1: Payment Pebble® tCR2.1 P5.1.1.x with a magnetic swipe reader

Figure 2: Payment Pebble® tCR2.1 P5.2.1.x without a magnetic swipe reader

3.2. Product type

The tCR2.1 is a hand-held attended or an unattended device used to capture contact and contactless chip card and magnetic stripe card payments. The PIN is entered using a unique PIN entry method. There is no pin pad on the tCR2.1 itself, but rather the smart phone is used to input the PIN indirectly.

The account selection, amount, email address or mobile number are all entered on the smart phone and sent to the tCR2.1.

3.3. Product identification

The product name and the hardware version are engraved into the bottom of the unit. The device serial number and barcode are also located on the bottom of the unit. These labels must not be modified or covered.

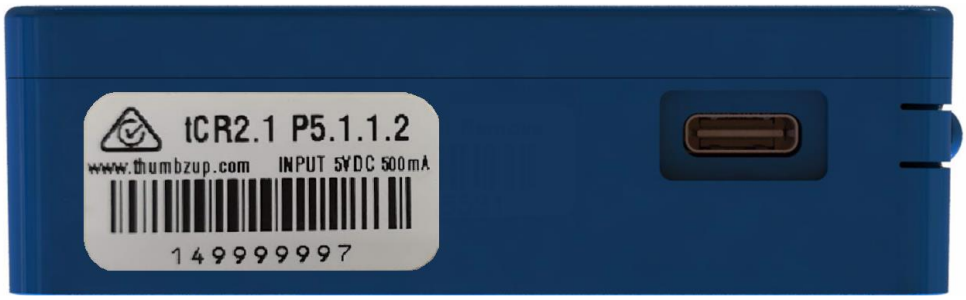

Figure 3: tCR2.1 image showing the hardware version

The hardware versions denote the following:

Hardware version	Magnetic stripe reader	BLE fitted
P5.1.1.1	Yes	No
P5.1.1.2	Yes	Yes
P5.2.1.1	No	No
P5.2.1.2	No	Yes

The software version is displayed when the device powers up. This information can also be obtained via an API call to the device. Note that the HW string in this display refers to the internal version of the Main PCB.

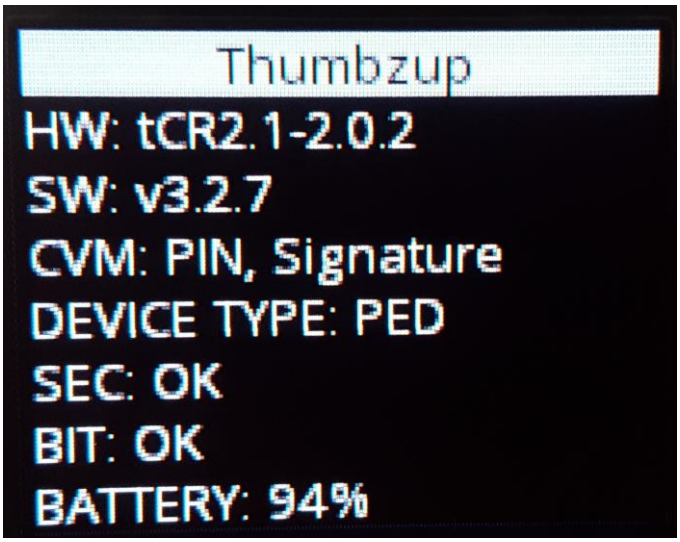

Figure 4: tCR2.1 Software Version

4. Installation and user guidance

4.1. Initial inspection

The merchant or acquirer must visually inspect the device for any sign of tampering when it is received. The merchant or acquirer should inspect the device for the following:

- Ensure that the hardware/firmware versions are consistent with section 3.3 above
- The tCR2.1 device is a sealed unit and is not designed to be opened. Check for evidence that the case has been opened. There is a label at the bottom of the unit that must not be damaged.
- There are no warning messages displayed on the display (see pictures above)
- There is no evidence of any unusual wires that have been connected to any parts of the device
- There are no unusual holes in the device
- There are no unexpected stickers attached to the device
- Once configured, ensure that the correct merchant name is displayed
- There is no shim or foreign objects in the chip card slot. The chip card slot has no joints and has no protruding objects. See picture below.
- There are no foreign objects in the slot for the magnetic stripe reader – see picture below
- These pictures indicate a normal device:

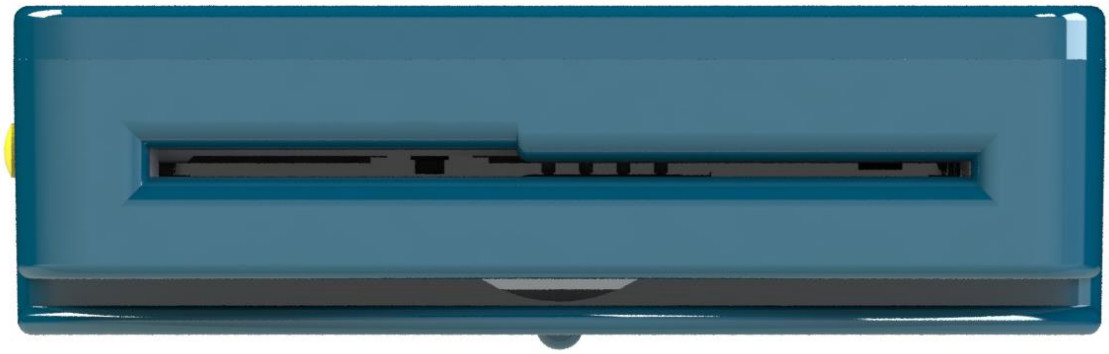

Figure 5: tCR2.1 chip card slot with Magnetic stripe reader

Figure 6: tCR2.1 chip card slot without Magnetic stripe reader

If any of these checks indicate a problem, the help desk must be contacted immediately, and the device must not be put into service and must be available for forensic investigations.

4.2. Guidelines

Ensure that the tCR2.1 is charged. A USB cable is supplied with the device to charge it on a PC, however, any mobile phone charger with a USB C connector can be used. The voltage should be 5V. A voltage exceeding 6V may damage your device.

Should the battery go flat, a prompt will be displayed to contact your bank to return your tCR2.1 to reload the keys. To ensure continual service, keep the tCR2.1 charged.

4.3. Communications and security protocols

The device can be connected to a mobile phone via USB or by Bluetooth Low Energy. The USB connection is a USB type C connector.

The Bluetooth Low Energy interface can only be used with LE Security Mode 1 level 4. This mode is automatically set, and the user cannot change the settings.

4.4. Configuration

There are no configurations settings to be set by the user. The configuration of the device is controlled by the Transaction Service using cryptographic authentication.

4.5. Unattended installation

Where the device is used in an unattended mode, the device must be so installed that the chip card slot is in full view of the cardholder, so that any untoward obstructions or suspicious objects at the opening are detectable.

5. Operation and maintenance

5.1. Periodic inspection

The merchant or acquirer must visually inspect the device for any sign of tampering on a regular basis. Ideally these checks should be done before each transaction otherwise at least once each day of use.

The merchant or acquirer should inspect the device for the following:

- The tCR2.1 device is a sealed unit and is not designed to be opened. Check for evidence that the case has been opened. There is a label at the bottom of the unit that must not be damaged.
- There are no warning messages displayed on the display
- There is no evidence of any unusual wires that have been connected to any parts of the device
- There are no unusual holes in the device
- There are no unexpected stickers attached to the device
- There is no shim or foreign objects in the chip card slot. The chip card slot has no joints and has no protruding objects. See picture below.
- There are no foreign objects in the slot for the magnetic stripe reader – see picture below
- This picture indicates a normal device:

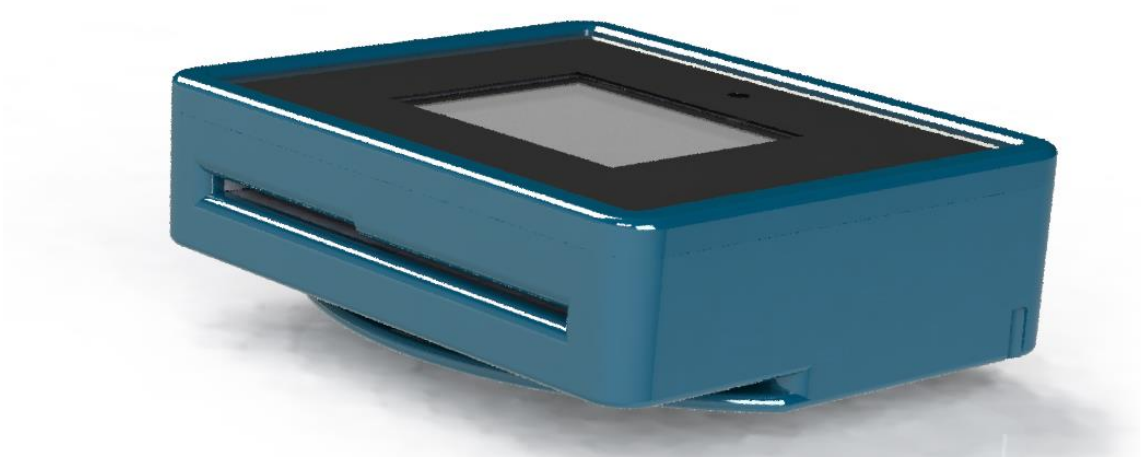

Figure 7: tCR2.1 chip card slot with magnetic stripe reader

If any of these checks indicate a problem, the help desk must be contacted immediately, and the device must be removed from service and be available for forensic investigations.

5.2. Self-test

During the booting process, a number of self-tests are performed to ensure that the device is behaving correctly. A device that has not run self-tests for 24 hours will reboot to run self-tests. The self-tests include:

- Firmware integrity
- Hardware security
- Crypto co-processor
- Random number generator
- Real time clock

After this, the firmware is authenticated. Only firmware that has been signed by thumbzup will be able to be executed.

5.3. Roles and Responsibilities

The device has no functionality that allows access to sensitive services based on roles. The Transaction Service manages such services using cryptographic authentication.

5.4. Tamper response

Should a device be tampered with, or if the device is opened, all keys are erased, and the device will not be able to process any transactions. A device that has been compromised will indicate the fault as shown below. The device must be returned to the acquirer for inspection.

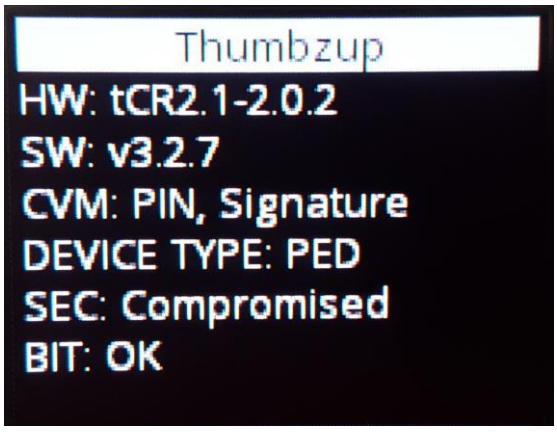

Figure 8: tCR2.1 with a tamper condition

5.5. Privacy shield

In attended mode, the size of the tCR2.1 with the smart phone is small that it encourages handheld use so that the user can shield the device with his own body. In unattended mode the device will be secured so that it cannot be removed.

The cardholder should be advised to shield the display of the tCR2.1 and the touch screen of the mobile phone or device so that no one can observe the PIN entry.

5.6. Firmware updates

Firmware can be automatically updated in the field without any user intervention. The activation for loading new firmware is done at the server. The firmware is provided in an encrypted form by the server. The key is provided encrypted under a key unique to that device. Once decrypted, the firmware signature is checked to authenticate the firmware and loaded into the device.

5.7. Device activation and deactivation

A tCR2.1 can be remotely suspended or deactivated at the Transaction Service. A suspended tCR2.1 cannot perform any transactions but can be reactivated again. The user must return the device to the acquirer.

If a tCR2.1 is disabled, all keys in the device are cleared. The user must return the device to the acquirer. The device can be repaired and reloaded in the trusted centre or can be destroyed. The acquirer must maintain an audited log of all devices and keep track of any devices that have been disabled or destroyed.

5.8. Battery charging

The device should be charged regularly. If the device is left uncharged for an extended period, the keys will be destroyed, and the device will not be usable.

5.9. Environmental conditions

The operating conditions for the device are between 0°C and 50°C and a humidity of 5% to 95%.

If a device is subjected to extreme temperatures (outside of -30°C and +110°C), or if the device is subjected to severe shocks, the keys will be destroyed, and the device will be disabled.

If a device is abused by incorrect voltages on the USB port, the voltages on the backup battery may be affected. If the voltage on the backup battery goes outside of the range 2.2V ±0.1V and 3.7V ±0.1V, the keys will be destroyed, and the device will be disabled.

6. Security

6.1. Security

The tCR2.1 has been built around a made-for-purpose secure processor that provides many layers of security to detect tampering of the device. Should it detect anything untoward, it self-destructs, deletes all sensitive data and becomes totally unusable.

The memory is embedded inside the secure processor and is encrypted with a unique key. Tampering with the device also scrambles this memory, so it's not possible to extract the current data in the memory or inject rogue programs.

Advanced cryptographic algorithms are used to protect the integrity of the tCR2.1. It is not possible to load any software into the tCR2.1 without the knowledge of the cryptographic keys used to protect the device.

The unique PIN entry method been designed to increase the security for mobile Point of Sale. There is no keyboard that can be attacked.

All messages between the tCR2.1 and the bank are encrypted. The smart phone is merely a carrier and cannot "see" what is inside any of the messages. The PIN is doubly encrypted and can only be checked by the bank that issued the card.

Every transaction is authorised immediately with the acquiring bank. No off-line transactions are allowed.

6.2. PIN entry

The tCR2.1 implements the thumbzup's unique patented secure PIN entry method that makes use of the insecure touch screen on the smart phone for the PIN entry, whilst keeping the PIN secret from the smart phone. The PIN entry method uses a secure mPOS device and allows the cardholder who knows the card PIN to make a visual association between the two devices whilst preventing the smart phone application from ever knowing the PIN.

When the PIN is to be entered, a map of the keypad is displayed on the secure screen of the tCR2.1 device. The layout of the keypad map shows the numeric keys in randomly reordered positions to ensure that the PIN will never be known to the smart phone. The cardholder enters a PIN by pressing the button on the smart phone screen that corresponds to the grid position of the numeral shown on the keypad map displayed on the secure screen of the tCR2.1 device.

It is important to note that the actual PIN digits are never entered via the smart phone software keypad; it only sends the representative coordinates for the keypad map that is displayed on the secure screen of the tCR2.1 device. This is only possible because the cardholder, who knows the PIN, is able to visually locate the PIN digit on the tCR2.1 device and locate its corresponding position on the grid on phone application.

In the image below, it is shown how the cardholder will be instructed to enter the card's PIN via the text prompt "Enter PIN" that is shown at the top of the secure screen, with the keypad layout mask below the instruction. A ghost/disconnected keypad without numeric legends is provided on the smart phone. The cardholder should be advised to shield the display of the tCR2.1 and the touch screen of the mobile phone so that no one can observe the PIN entry.

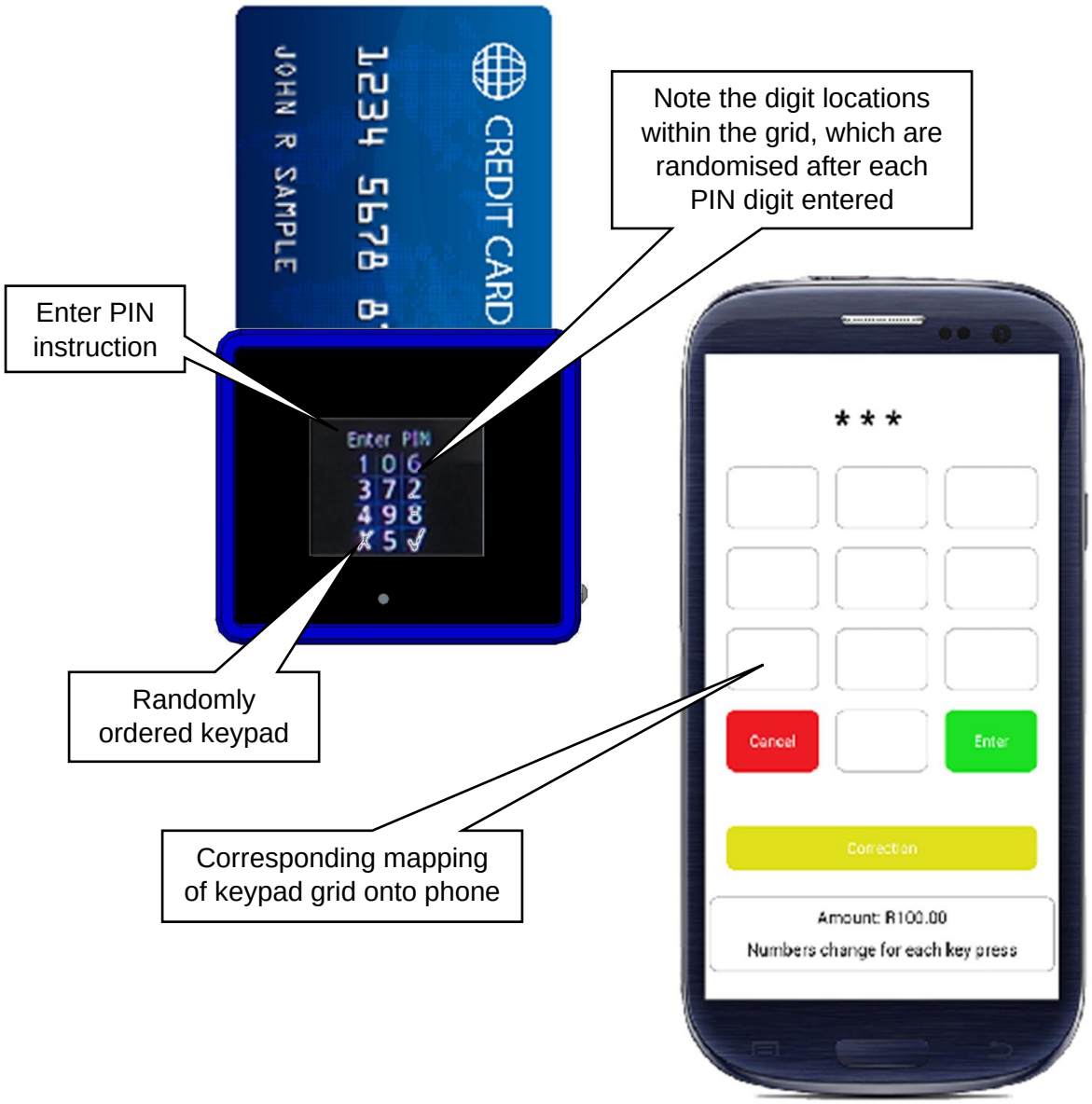

Figure 9: Secure PIN entry method

As soon as the cardholder starts entering the card's PIN, the "Enter PIN" instruction will be replaced by a non-significant character (*) representing each digit of the PIN that is being entered by the cardholder.

A new random keypad map is generated after each digit has been entered or when the Correction button has been pressed. The entered PIN is treated securely according to PCI requirements.

Even if an observer has knowledge of the keypad map, the PIN entry will be no less secure than a conventional pin pad where the positions of the keys are known.

The cardholder must not enter a PIN onto a keymap that has not been scrambled. The smart phone is not a secure device.

6.3. Communications

The tCR2.1 is connected to a smart phone via USB or Bluetooth Low Energy. The co-processor in the tCR2.1 receives the messages and forwards them to the secure processor via a serial link.

The messages need to conform to the API. All messages are checked before they are processed.

6.4. Software Management

The signing of the firmware is under dual control, and is only done when the following processes have been completed:

- Firmware has been tested
- All firmware has been logged into a software repository that tracks all changes and modifications
- An official build has been made and numbered
- Firmware has been audited according to the Software development practices for secure devices [2]

An API is defined with a suite of commands are used to interface with the tCR2.1. Checks are made on the commands to block any invalid commands or parameters.

7. Key Management

During the booting process, ECC P-256 is used to authenticate the firmware before it runs.

During initialisation, the 2048-bit RSA secret key and 521 EC secret key are generated by the tCR2.1 and signed by the server. This process takes place in a secure zone with access control, video cameras and audited processes to comply with the PCI requirements.

When the tCR2.1 is configured for use, the Merchant code needs to be entered. The DUKPT PIN encryption keys are securely loaded into the device by the Transaction Service using the device's 2048-bit RSA key. The Terminal Master Key is loaded under a session key generated using ECDH and Ephemeral EC keys that are exchanged. The parameters, EMV parameters merchant data are loaded using secure messages based on AES256 and SHA-2 base HMACs. Once this is complete, the tCR2.1 can be used to accept payments. There are no manual configuration settings to be applied.

For transactions, the PIN is encrypted using the DUKPT PIN key. The messages are authenticated using the DUKPT MAC keys and TDES encrypted using the DUKPT encryption keys.

Each time the tCR2.1 connects to the Transaction Service, the Transaction Service checks that the tCR2.1 is registered and that the keys are in sync. Keys will be updated or rolled as required.

There is no manual loading of keys.

7.1. List of keys in tCR2.1

The following keys are stored in the tCR2.1:

Key name	Purpose usage	Algo-rithm	Size (bits)	Storage
CA PK	CA public key for certificate verification	RSA	2048	Secure unit
Product PK	Public key for product certificate verification	RSA	2048	Secure unit
Acquirer PK	Public key for acquirer certificate verification	RSA	2048	Secure unit
Acquirer HSM PK	Public key for acquirer HSM certificate verification	RSA	2048	Secure unit
Storage Master Key (SMK)	Protects other keys	AES	256	Secure encrypted memory
Terminal RSA Key	Private and public key	RSA	2048	Encrypted under SMK
Terminal EC Key	Private and public key	EC	521	Encrypted under SMK
Terminal Master key (TMK)	Used to generate signing and encryption keys for Transaction Service messages	AES	256	Encrypted under SMK
DUKPT keys	Encrypt PIN, sign and encrypt transaction message requests and responses	TDES AES	112 128	Encrypted under SMK

Table 1: tCR2.1 Software Version

7.2. Firmware application program interfaces (APIs)

The tCR2.1 has a well-defined API interface to control the flow of a transaction. Any deviation will return an error and cancel the transaction. A sensitive and secret information is not directly available via this API. All sensitive data is transmitted encrypted and is sent to the Transaction Service where it is decrypted. Each message also authenticated so that they cannot be modified.

8. Reference documents

[1] Payment Card Industry (PCI) - PIN Transaction Security (PTS) - Point of Interaction (POI) - Modular Security Requirements - Version 5.1 dated March 2018.

[2] thumbzup WD-THB-17135 Software development practices for secure devices - Version 1.2 dated 5 June 2018.

9. Glossary

Term	Description
AES	Advanced Encryption Standard – symmetric key algorithm
API	Application program Interface
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction
EC	Elliptic Curve – public key cryptosystem
EMV	Europay, MasterCard and Visa
mPOS	Mobile Point of Sale
PCI	Payment Card Industry
PK	Public Key
POI	Point of Interaction
RSA	Rivest, Schimir and Adleman – public key cryptosystem
TDES	Triple DES