MPOS-STD2 Hardware Reference Manual

Ref: RM25H08

Revision B

Maxim Integrated PROPRIETARY – CONFIDENTIALITY

Revision History

Rev A	2014-Sep-03	1st release
Rev B	2014-Oct-08	Added Bottom casing removal switch Added Installation section

Disclaimer

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realize that we may have missed a few things. If you find any information that is missing or appears in error, please contact us via www.maximintegrated.com/support. We appreciate your assistance in making this a better document.

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Maxim Integrated Office.

Maxim Integrated Technologies may only be used in life-support devices or systems with the express written approval of Maxim Integrated, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Table of Contents

List of Figures

References

[1] MAX32550 preliminary datasheet. DS25H01 Rev F. Feb 2014.

[2] PCI-PED PTS Security Requirements. V4.0.

[3] NIST Cryptographic Algorithms Validation Program (http://csrc.nist.gov/groups/STM/cavp/index.html)

[4] EMV2000 Specifications (www.emvco.com)

[5] EMV Integrated Circuit Card Specifications for payment systems, Book 1 - Application Independent ICC to Terminal Interface Requirements V4.2 Jun-2008 (http://www.emvco.com/specifications.aspx)

[6] ISO7816-1,2,3,4

[7] Implementation Conformance Statement Level 1 V2.1 Jan-2007 (http://www.emvco.com/specifications.aspx)

Glossary

EMV	Europay MasterCard Visa
FPC	Flexible Printed Circuit
I/O	Input / Output
ICS	Implementation Conformance Statement
IFM	Interface Module
LCD	Liquid Crystal Display
NVSRAM	Non-Voltile SRAM
PCB	Printed Circuit Board
PCB	Printed Circuit Board
PCI	Payment Card Industry
PET	polyethylene terephthalate
POI	Point Of Interaction
POS	Point Of Sale
PTS	Pin Transaction Security
RCP	Reader Communication Protocol
RFU	Reserved for Future Use
RISC	Reduce Instruction Set Computer
S/N	Serial Number
SRAM	Static Random Access Memory
TBD	To Be Defined
TFT	Thin Film Transistor
USB	Universal Serial Bus
IC	Integrated Circuit

1 Introduction

This document details the construction of the MPOS-STD2 terminal according to the PCI PTS security requirements 4.0.

2 Overview

The MPOS-SDT2 terminal is a mPOS. it works in association with a merchant terminal and an acquirer server.

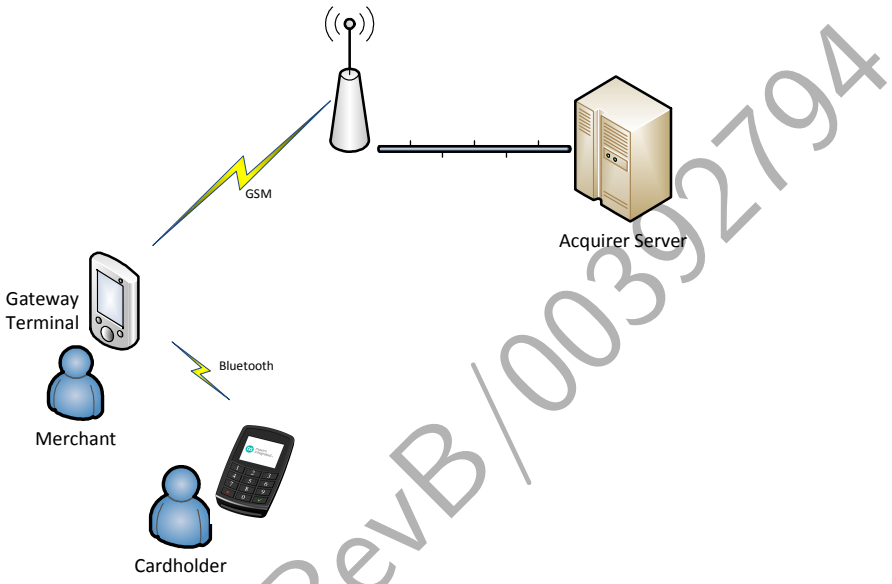


Figure 1: Payment Infrastructure

The merchant terminal provides means to run a dedicated application for merchants and to establish a communication link between the mPOS and the acquirer server. mPOS terminals normally can only access to a local network and merchant terminal can access to both local and global networks.

To perform a transaction, the merchant terminal sends data for initiating the transaction thanks to a dedicated application then the mPOS terminal deals with the acquirer server and with the cardholder; the merchant terminal acts at this stage as a gateway to allow the mPOS to reach the acquirer server.

The merchant terminal can be a smart phone, a tablet or a computer. It must be able to run an application to setup a transaction and to connect the acquirer server to the mPOS. The connection between the acquirer server and the merchant terminal can be established either over the air thanks to a mobile phone network or through internet. The connection between the merchant terminal and the mPOS is usually Bluetooth® while it can be via audio-jack or USB too.

The mPOS provides a secure environment for bank card acceptance. Generally speaking it is the cardholder interface and it performs subsets of the operations needed for completing a transaction to reduce the transaction duration. All transfers between the mobile POS and the server are done in an encrypted fashion meaning that the merchant terminal is not able to interpret any exchange between the mobile terminal and the server; the merchant terminal only sends a request for performing a transaction plus a context. The acquirer server runs software to achieve transaction in a secure room in the acquirer building.

3 Characteristics

MPOS-STD2 is a mPOS terminal running under FreeRTOS operating system.

Processor (secure microcontroller):

- 108MHz 32-bit ARM Cortex M3 core with MPU
- 256kbytes of SRAM
- 1Mbytes of Flash
- 4kbytes of OTP
- 8kbytes of encryptable NVSRAM

User Interface

- 320 x 240 dots graphic color TFT with backlight
- 12-key keypad

Magnetic Card Reader

- 2-tracks magnetic card reader

Smartcard Reader

- EMV 4.2 Level 1, ISO7816, 5V/3V/1.8V support, T=0 and T=1 protocols

Contactless Reader

- ISO14443 A & B, Felica and Mifare, EMV support

Connectivity

- USB full-speed
- Bluetooth 4.0

Optional storage memory

- 1 Mbytes external SPI flash (optional)

Environmental

- Operating temperature range from -10°C to 40°C
- Storage temperature range from -40°C to 85°C

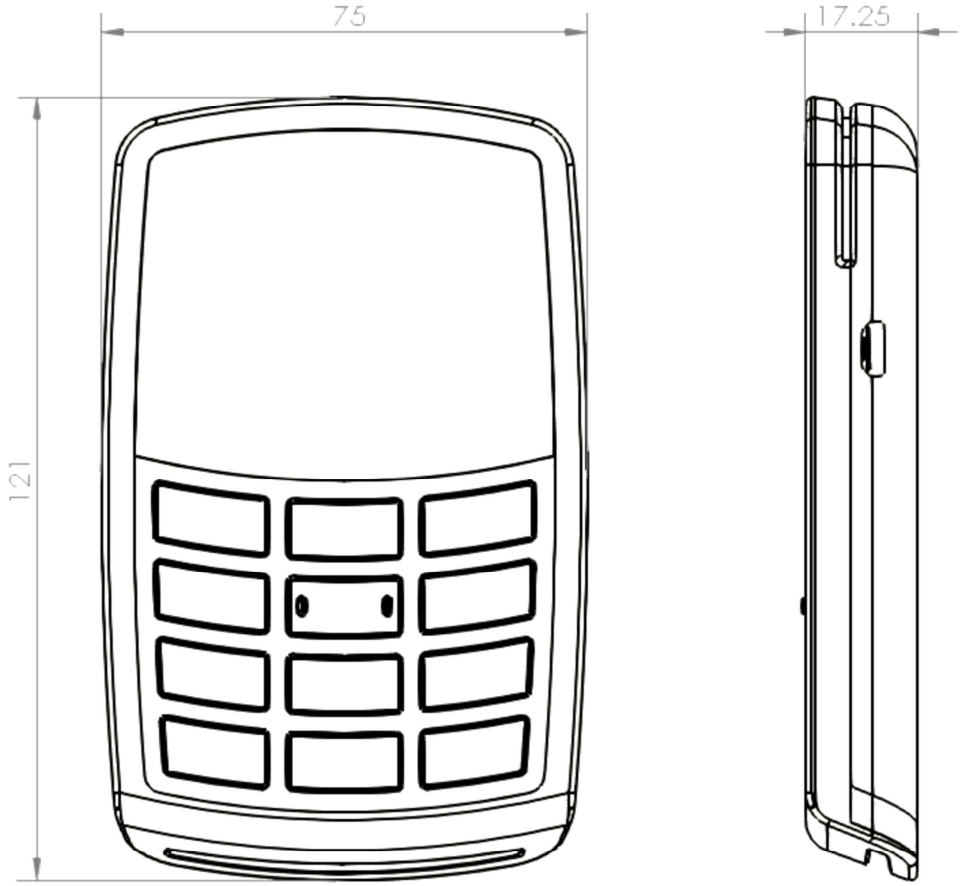
Power

- 3.7V 230mAh lithium-ion polymer battery
- 3V 160mAh lithium manganese dioxide battery

The secondary battery can be charged by USB. MPOS-STD2 can operate during charging.

Dimensions

- Length 121,5 mm x Width 75 mm x Thickness 17.25 mm



4 System Description

MPOS-STD2 terminal is based on the MAX32550 secure microcontroller which embeds the most of the interfaces of the terminal.

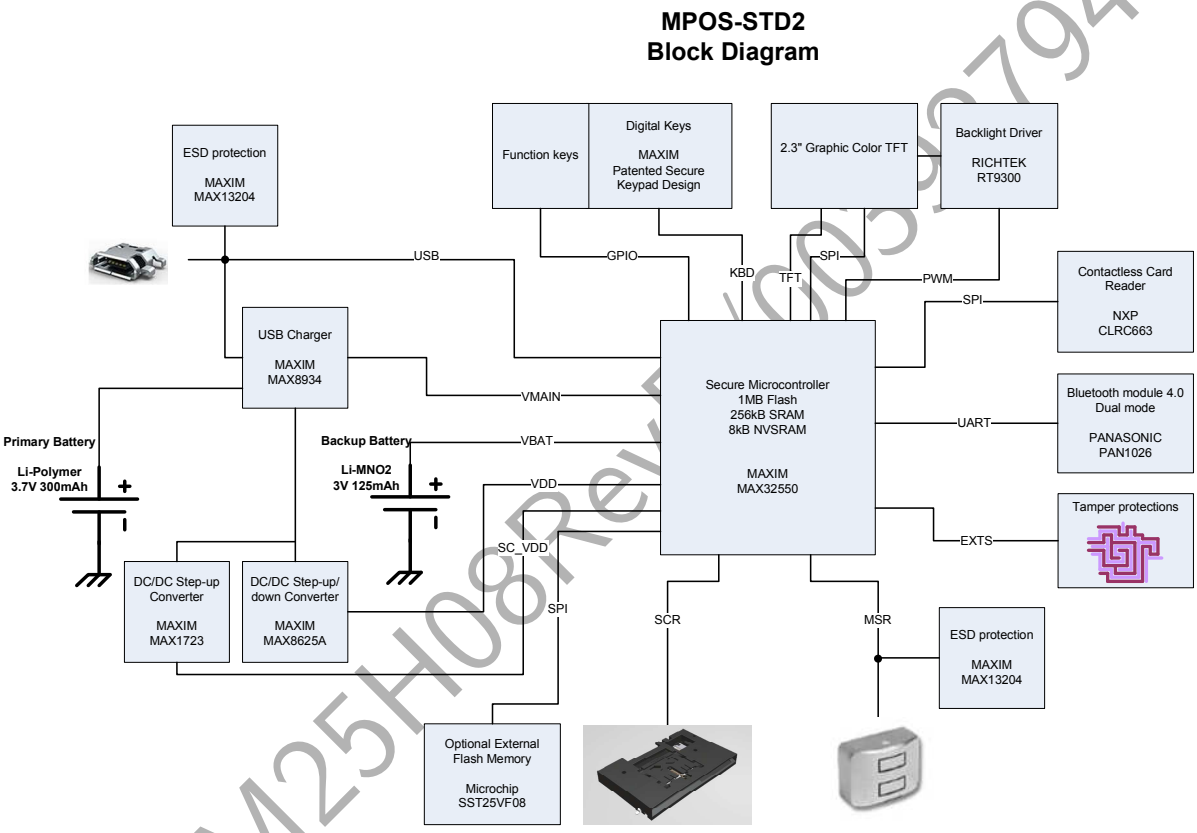


Figure 2: Block Diagram

4.1 Secure Microcontroller

The MAX32550 is a 32-bit ARM® Cortex™-M3 secure microcontroller running at 108MHz with embedded memories:

- 1Mbytes of internal flash memory
- 256kbytes of internal SRAM
- 8kbytes of NVSRAM

The 8kbytes of non volatile memory can be split in two areas, one in plain and the other secure by AES-256 encryption/decryption engine. The amount of memory for those areas is user configurable. In case of tampering the AES key protecting the secure area of the NVSRAM is instantaneously erased.

4.1.1 Security Monitor

The MAX32550 provides internal sensors for ensuring that the microcontroller runs in safe conditions and for protecting the terminal against tampering.

- Programmable temperature sensor
- Die shield
- Core and battery voltage sensor
- External Dynamic sensors

When the core voltage goes out of range, the microcontroller goes in reset state to avoid sensitive data leakage.

When one the other sensors triggers, the security mechanism instantly erases the AES key protecting the NVSRAM content.

The security monitors and the sensors are powered either by the main power rail or the backup power rail depending on power source availability.

The external dynamic sensors are powered by a true random generator making impossible to replay wire-mesh signals.

4.1.2 Secure Boot

The MAX32550 provides a secure boot ROM based on ECDSA algorithm. Data transfers and commands are signed to be verified by the MAX32550. Moreover the secure boot ROM is able to install and run applets allowing additional treatment on incoming data such as decryption.

4.1.3 JTAG

On production-grade MAX32550 secure microcontrollers, there is no ICE feature available by default in normal operating conditions. It is possible to have this mechanism available (e.g. for devices failure analysis) but the consequence is that the battery-backed AES-256 secret key is erased at each reset.

4.2 Power Supply

MPOS-STD2 power supply scheme is simple thanks to the MAX32550 embedded core voltage regulator and a set power supply pins allowing automatic power source selection in battery backed mode operation (i.e. to power the security mechanisms and NVSRAM).

The main power supply rail is 3.3V. It is generated by a step up/down DC/DC converter. It regulates power supply voltage coming from USB and the secondary battery through the battery charger.

A 5V power supply is available for smartcard class A support. Note that class A support is still mandatory for EMV compliance until 2015.

In case the secondary battery is empty and no power is available on USB, a primary battery can supply the security mechanisms and the NVSRAM of the MAX32550.

4.2.1 Power Management

In order to save power from the secondary battery, a MPOS-STD2 device goes in sleep mode when it is possible. A MPOS-STD2 device can be in the following power mode:

- Operating: the system runs normally
- Sleep: the main power supply is available but the system is frozen except the Bluetooth module which can wake-up the system on
- Power-off

Note that whatever the power mode, the security mechanisms of the device run and can instantaneously erase sensitive data on tamper detection.

The following flowchart shows power mode transition:

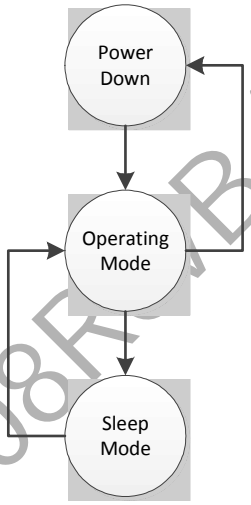


Figure 3: Power Mode Flowchart

The device power management is quite simple thanks to the MAX32550 electrical characteristics and the application needs.

To go in operating mode from the power off mode, the “Valid” key has to be pressed for two seconds.

To go in sleep mode, the device has to be set up for Bluetooth operation and the pairing procedure completed. Note that pairing parameters are saved and used for next run. Of course, they could be changed after if needed. When the device is connected by USB, Sleep mode is disabled but high power consumption interfaces are switched off (e.g. backlight, display…).

To go back from sleep can be achieved by two ways. The device gets a wake-up request by Bluetooth® or a user press the “Valid key” for one second.

Note that a Hardware reset can by generated by pressing the “Valid” and “Cancel” keys for a while. That will also put the system in operating mode.

4.3 Interfaces

This section describes electrical features of the MPOS-STD2 device interfaces.

4.3.1 Keypad

The MAX32550's keypad controller provides scan randomization features:

- Scan order is randomly set for each round
- Scan duration is randomly set for each scan pulse

The figure below shows how the controller works. In this case, the lines (Lx) are connected to the output of the controller and the column to the input. Depending on parameters draws at random for each round, the scan sequence can be completely different from the previous one.

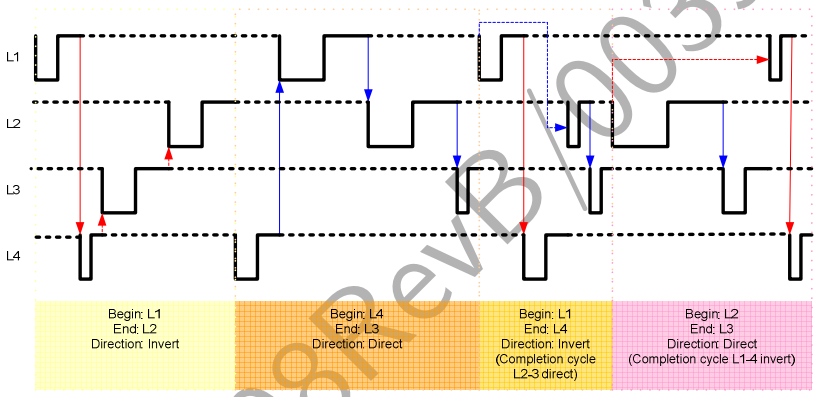


Figure 4: Keypad Controller Scanning

Randomization of matrix scan reduces key electromagnetic signature and synchronization of spying hardware.

4.3.2 Smartcard Contact Reader

The MAX32550 provides a full smartcard reader interface including the analog front end. Then, the smartcard acceptor is directly connected to the secure microcontroller. The attack path for probing the smartcard I/O is very limited.

4.3.3 Magnetic stripe card Reader

The MAX32550 provides a 3-track F2F decoder. A magnetic head is directly connected to the secure microcontroller to provide the magnetic stripe card reader function.

4.3.4 Display

The MAX32550 embeds a TFT controller then it can directly control a display by providing RGB data signals, clocks and controls.

4.4 Connectivity

MPOS-STD2 device provides two communication links:

- Bluetooth
- USB

4.4.1 Bluetooth

The Bluetooth interface is based on a module from Panasonic.

The MAX32550 is interfaced with the module thanks to a serial link. UART RTS is used for waking up the system when it is in sleep mode.

4.4.2 USB

MPOS-STD2 can be interfaced with a USB host thanks to the USB CDC-ACM class driver. A USB full speed device interface is available on the MAX32550 secure microcontroller.

4.5 Optional Storage

An optional SPI NOR flash memory is installed allowing terminal to store logs outside the secure microcontroller. In case the terminal is out of order this memory could be accessed for post mortem analysis.

Note that memory could be also used for data and binary storage if needed. Depending on the sensitivity of the contents an appropriate protection scheme is required.

5 Implementation

5.1 Architecture

MPOS-STD2 device is built upon a single PCB. It is not designed for on the field maintenance then no door and removal facilities are provided. After system assembly, the front and rear case parts fit into each other to enclose the system. Hooks in both case parts keep the device closed.

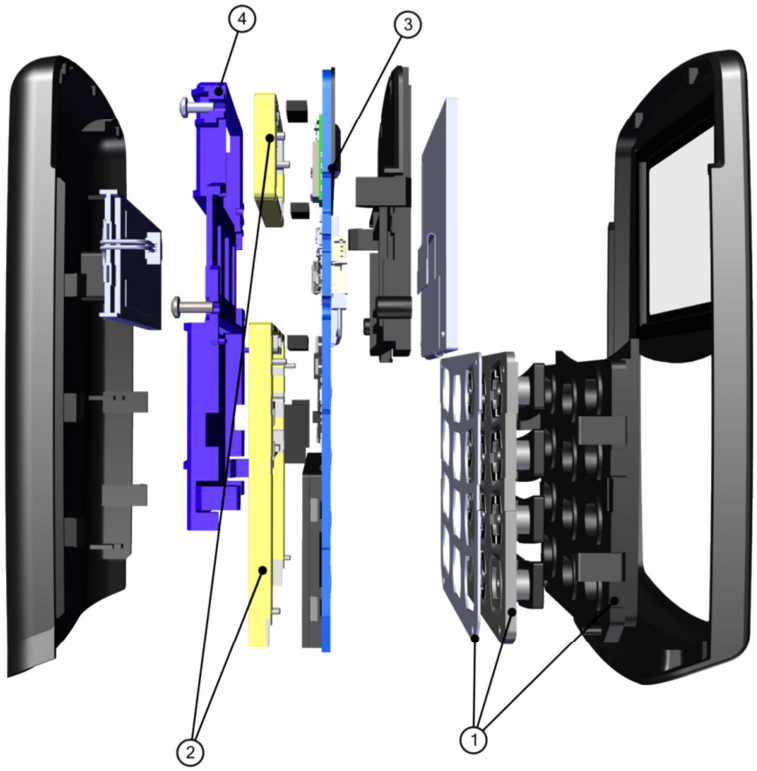


Figure 5: Keypad Controller Scanning

The exploded view above gives a general understanding of the assembly. The numbers identifies the mains parts and sub-assemblies:

1. Secure keypad sub-assembly
2. Secure enclosures protecting the system plus the smartcard acceptor and the magnetic head
3. PCB Assembly
4. Secure enclosure holder

5.2 Components

5.2.1 PCB

The PCB is eight layers and 1.6mm thick. The structure is the following:

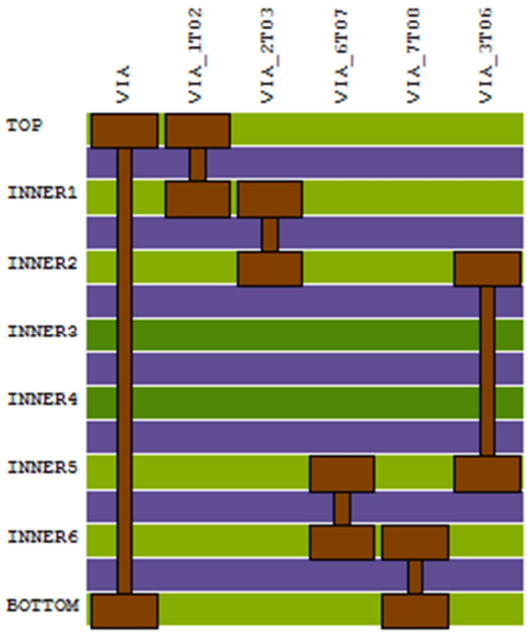


Figure 6: PCB Stack-Up

Vias:

- VIA:
  - Through all
  - Mechanical drilling
- VIA_1TO2, VIA_2TO3, VIA_6TO7, VIA_7TO8
  - Blind via
  - Laser drilling
- VIA_3TO6:
  - Buried via
  - Mechanical drilling

5.2.2 Meshes

PCB and secure enclosure meshes are designed according to the same design rules:

- 2-layers
- 150µm trace width and clearance

5.2.2.1 PCB

The PCB mesh covers the whole of the PCB area. It is laid out on INNER1 and INNER2 layers. It protects the system against physical intrusion coming from the top side.

Mesh layer connections are done using buried and blind vias. Vias connected to TOP, INNER1 and INNER2 layers are placed underneath keypad tamper switches to prevent from tampering.

5.2.2.2 Secure Enclosures

The secure enclosures consist on a FPC folded on a frame. The frame allows forming of the enclosure and contacts alignment with the board. A secure enclosure is put in contacts with the board thanks to elastomeric connectors. The secure enclosures protect the system against physical intrusion coming from the bottom side.

The FPC is made of a PET film on which is designed a mesh on each side with conductive ink. Connections between the top and the bottom layers are placed in locations which are inside the secure enclosure after folding. Then there are not accessible.

In order to hide the mesh design on the top layer, an insulating black coating is added. On the bottom side an adhesive tape provides facilities for assembly the FPC on the frame and also prevents from disassembling.

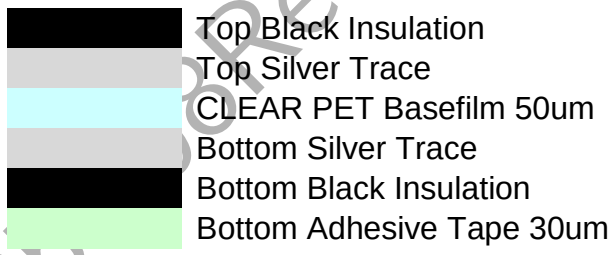


Figure 7: FPC Stack-Up

On the board side, meshes are connected to the tamper detectors, the dynamic sensors of the MAX32550, through elastomeric connector by a PCB landing pattern. Each contact is 0.5mm width and 2mm height. There are surrounded by a guard ring connected to GND. That is for preventing from conductive glue to shunt the tamper circuits

Figure 8: FPC mesh PCB landing pattern

5.2.3 Magnetic Stripe Reader

A secure enclosure is dedicated to magnetic head protection.

The mesh consists of wire-meshes interleaved, two per side.

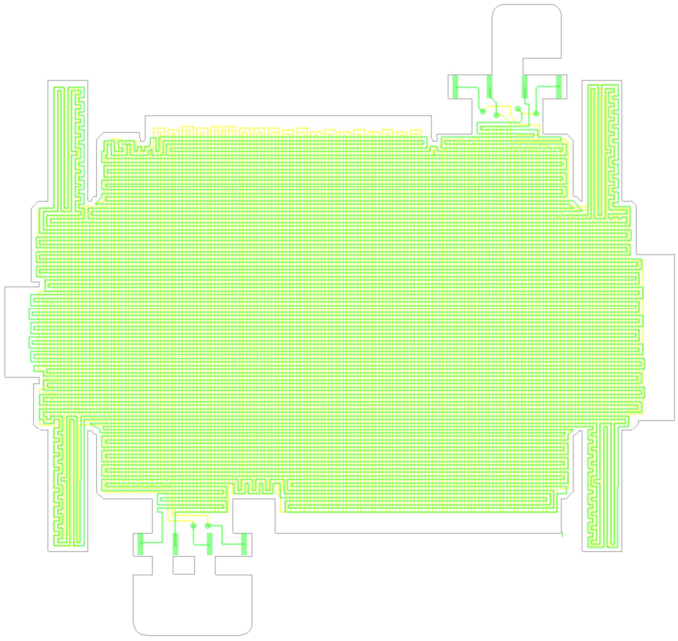


Figure 9: MSR FPC Mesh

One mesh layer is designed in horizontal direction and the other in vertical direction.

The figure below shows the magnetic head secure enclosure assembly.

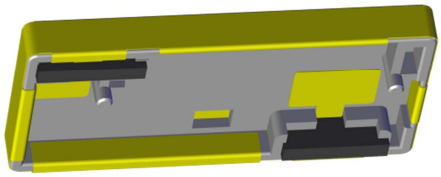


Figure 10: MSR Secure Enclosure

5.2.3.1 System

The system secure enclosure protects both the system and the smartcard connector. The microcontroller and other sensitive electronics are placed under the cover.

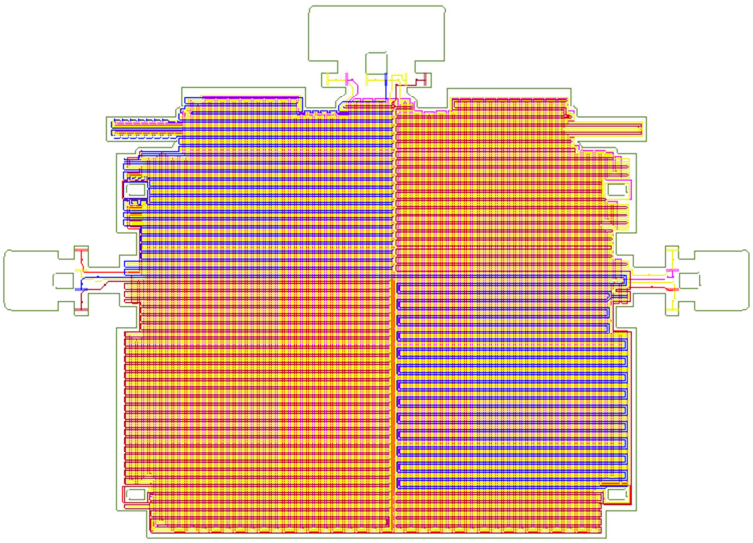


Figure 11: System FPC Mesh

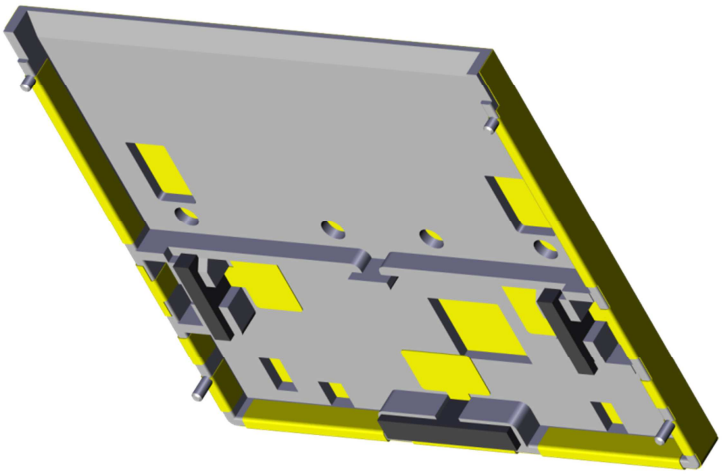


Figure 12: System Secure Enclosure

The system secure enclosure is designed in the same way than the one for the magnetic head but it is driven by five tamper circuits instead of four for the magnetic head and it is connected to the board thanks to three elastomeric connectors instead of two.

5.2.4 Keypad

The keypad design is based on the secure keypad patented by Maxim Integrated.

Each key is surrounded by four blind switches. They are connected to two three dynamic sensors allowing tamper detection.

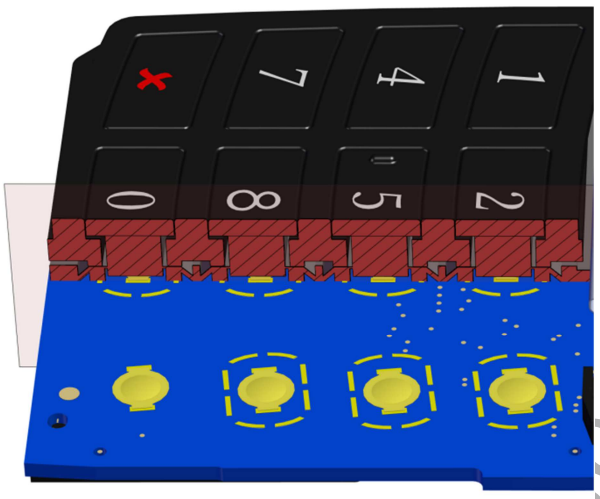


Figure 13: Keypad Assembly

User keys consist of a dome switch. They are powered with the scan by the keypad controller. When a dome is pressed, the scan signal is transmitted to the associated keypad input.

Tamper switches consist of a silicone key mate with four contacts per keys which closes fours tamper circuits per key (eight contacts) on the board. When the silicone key mate is maintained pressed, near the keys, the tamper switches are closed. The figure below shows a bottom view the silicone key mate and a top view of the board.

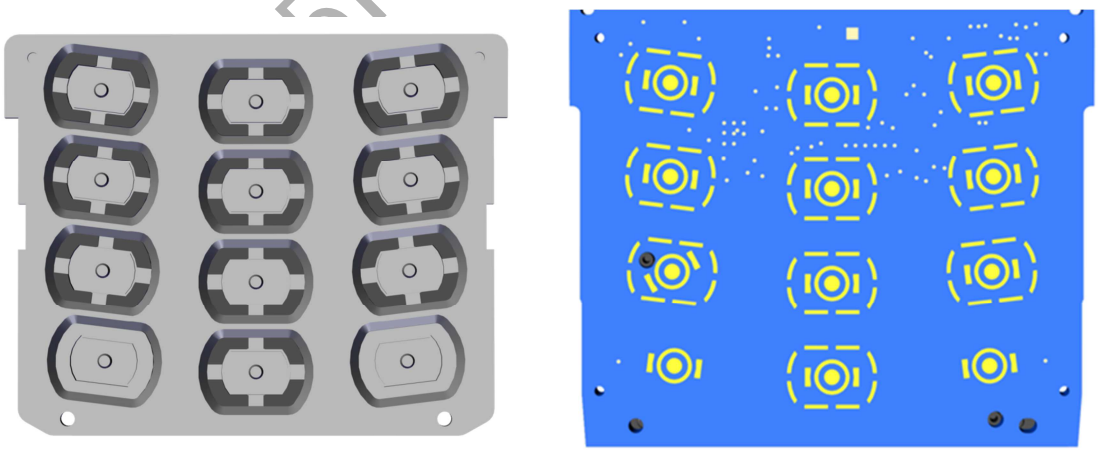


Figure 14: Keypad Tamper Switches

To ensure that releasing of the silicone key mate (1b) will open the tamper switches, a spacer (1c) is placed in between the silicone key mate and the board.

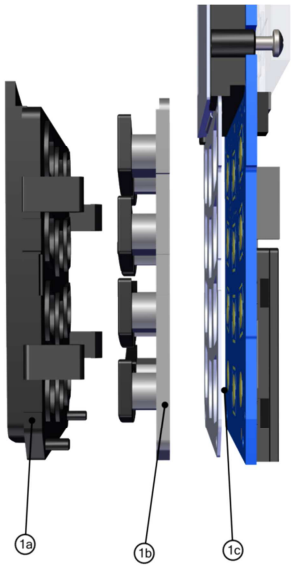


Figure 15: Keypad Assembly Exploded View

To keep the assembly in place, a grid comes on top of the silicone key mate and hooks the board. Finally, key caps are glued on top of the silicone key mate. They provides look and feel and links the silicone key mate to the grid.

5.2.5 Bottom Casing Removal Detection

A micro switch is placed on the bottom side of the PCB for early detection of tampering by removing the bottom casing. The switch is covered by a silicone cap in order to fill the gap between the switch and the secondary battery and compensate mechanical tolerance.

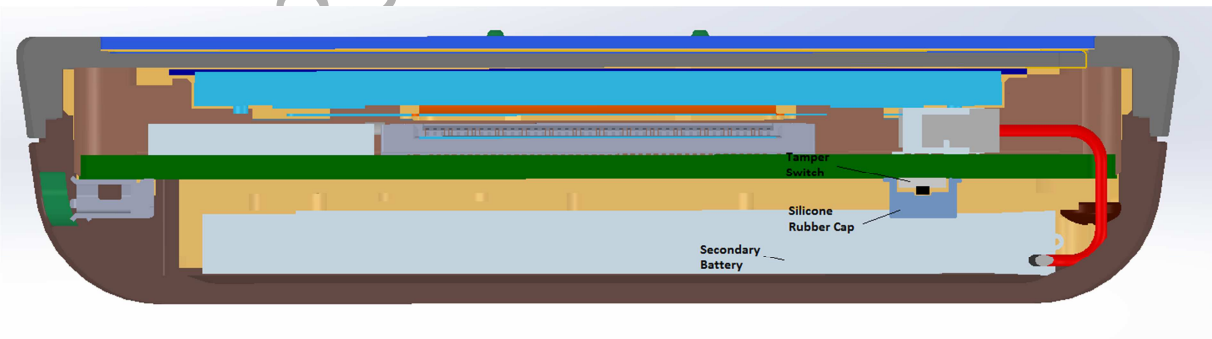


Figure 16: Bottom Casing Removal Switch

When the casing is closed the battery is pushed inside the compartment then press on the switch to closed the tamper detection circuit.

The tamper switch is powered by an external dynamic sensor of the MAX32550.

The micro switch footprint includes a guard ring made of copper without solder resist coating and connected to the ground plane. It prevents from attack using conductive glue.

The silicone rubber cap also helps to avoid gluing of the tamper switch because of the silicone characteristics: soft and hard to glue.

5.3 Installation

This section describes how are built the tamper protections of the device.

Sensitive electronics are placed underneath the secure enclosures.

Sensitive signals are enclosed between two two-layer meshes. One is designed in the PCB and the other is provided by the secure enclosures. The PCB provides protection against tampering coming from the top side and the secure enclosures from the bottom side of the device.

On the figure below it can be identified three main areas:

- Magnetic stripe reader
- Power supplies
- System: microcontroller, contactless card reader…

Both the magnetic stripe reader and the system are covered by a secure enclosure. Power supplies are not protected because of DPA and SPA resistance of the MAX32550 and because of the placement of bypass capacitors which are close to the secure microcontroller and underneath the system secure enclosure.

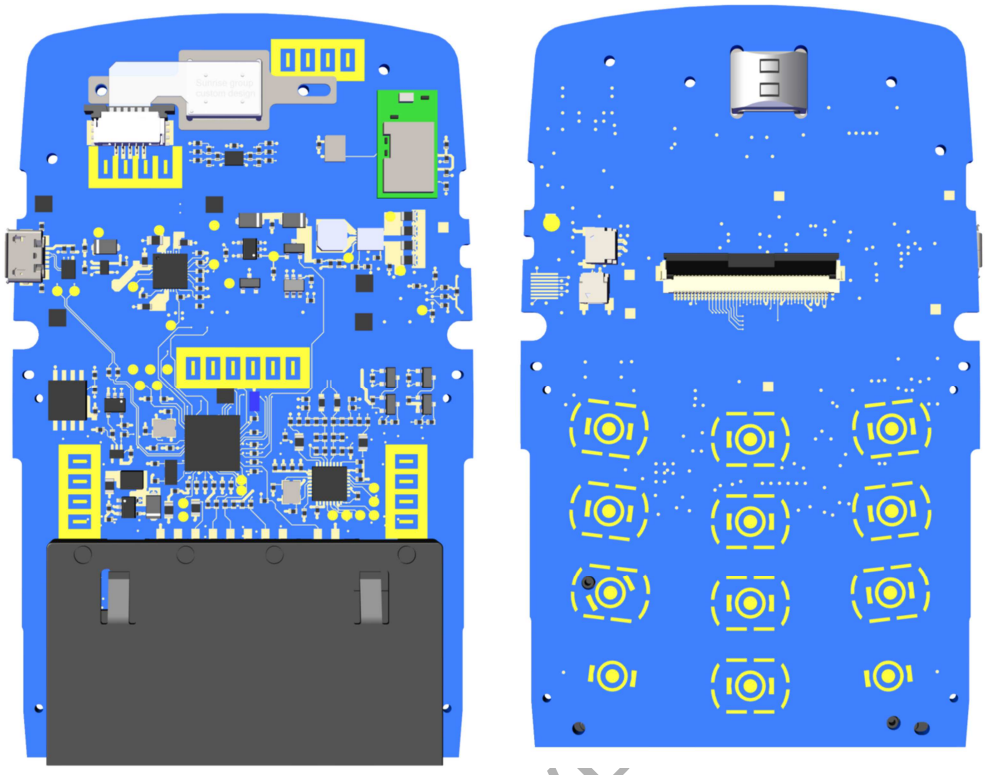


Figure 17: Device Installation Overview

PCB is designed with the following layer usage:

- TOP : Keypad
- INNER1 : Mesh
- INNER2 : Mesh
- INNER3 : Power plan (GND), magnetic head traces
- INNER4 : Power
- INNER5 : Signals, keypad matrix
- INNER6 : Signals
- BOTTOM : Signals

The Device's tamper protections are connected to the MAX32550 external dynamic sensors. The figure below shows the wire-meshes connection scheme.

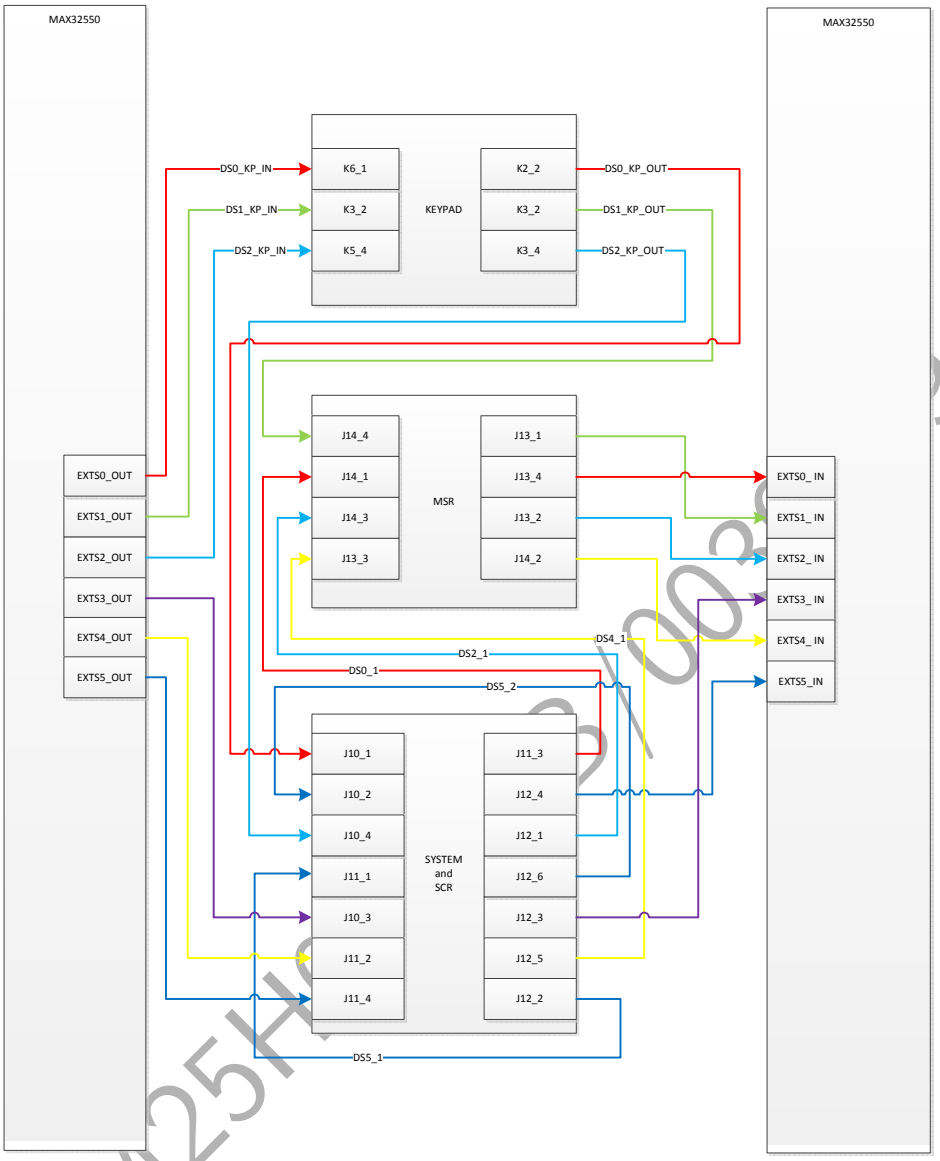


Figure 18: Wire-Meshes Connection Scheme

5.3.1 Display

Because transfers are performed in encrypted form, there is no way for getting benefit of attacking the display. This interface is out of the protected domain of the terminal.

5.3.2 Keypad

The keypad tamper protection is ensured by:

- The keypad tamper switch grid
- The two-layer mesh on the inner layer 1 and 2 of the PCB
- The System secure enclosure

The system secure enclosure prevents the keypad matrix signals from any physical access from the bottom side of the device. It covers the whole of the keypad area including the microcontroller.

The two-layer mesh in the PCB prevents from physical access from the top side to the keypad matrix.

The keypad tamper grid prevents from keypad disassembly avoiding installation of hardware for logging key entries. The tamper grid switches are surrounded by a ground plane without solder resist coating which acts as guard ring to prevent from attacks using conductive glue.

The vias used for the keypad matrix connection are located underneath the keypad tamper switches to benefit of their tamper protection. The vias used for mesh connection are placed in the same way.

Dome switch noise is muffled by the silicone mat covering the keypad. It makes harder key pressing identification by noise analysis.

5.3.3 Smartcard

The smartcard reader is fully integrated in the secure microcontroller. The smartcard I/O signal trace is connected to the smartcard acceptor through a RC filter. The RC filter allows signal adjustment to meet EMV electrical requirements if needed.

The smartcard reader protection is ensured by:

- The System secure enclosure
- The two-layer mesh on the inner layer 1 and 2 of the PCB
- The bottom casing removal switch

The whole of the reader is place underneath the system secure enclosure including the smartcard acceptor. It prevents from tampering coming from the bottom side of the device. The two-layer mesh also covers the whole of the smartcard reader area then prevents from tampering coming from the top.

In addition the smartcard acceptor pins are placed on the back side, far from the entrance.

A guard ring is installed front of the smartcard I/O contact and underneath the smartcard acceptor. It prevents from inserting a needle under the smartcard acceptor to reach the I/O pin.

The removal bottom casing switch placed underneath the secondary battery helps to protect against tampering consisting of installing hardware inside the casing.

The smartcard reader bezel is designed in order to avoid insertion of two cards stacked. Because of the smartcard thickness tolerance, the bezel has a specific shape leaving higher space at embossing location.

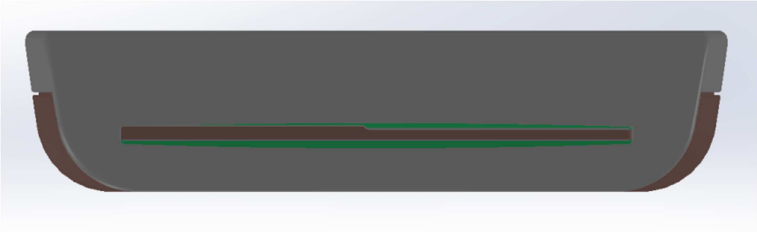


Figure 19: Smartcard Reader Bezel

The smartcard reader bezel is placed in the top casing to avoid having any seal usable for hiding wires coming out from smartcard reader.

5.3.4 Magnetic Stripe Card Reader

The magnetic stripe reader is made of the secure microcontroller plus a magnetic head.

The magnetic stripe reader protection is ensured by:

- The system secure enclosure
- The magnetic stripe reader enclosure
- The two-layer mesh on the inner layer 1 and 2 of the PCB
- The mesh on the inner layer 6
- The bottom casing removal switch

The secure microcontroller is placed underneath the system secure enclosure and benefits of the two-layer PCB mesh protection on the opposite side. The magnetic head is placed underneath the magnetic stripe reader secure enclosure and benefits of the two-layer PCB mesh as well. Then the both parts of the reader are protected against tampering from the top and bottom sides.

The head is connected to the MAX32550's magnetic stripe reader controller by four traces. They are routed on the INNER3 layer which is underneath the two-layer PCB mesh. Thus they are protected against tampering coming from the top side of the device. A dedicated mesh covers the magnetic stripe signal traces on the INNER6 layer. In addition the bottom casing removal switch helps for early detection of tampering.

The device design does not allow installation of magnetic stripe head beside the regular one. The secure enclosure covers a large part of the device at the magnetic head level leaving not enough space for installing an additional magnetic head.

5.3.5 Contactless Card Reader

The contactless card reader is made of a dedicated controller which is interfaced by SPI to the secure microcontroller. Both are placed underneath the system secure enclosure and benefits of the protection of the two-layer PCB mesh on the opposite side. Only the antenna is not out of this area.

The contactless card reader protection is ensured by:

- The system secure enclosure
- The two-layer mesh on the inner layer 1 and 2 of the PCB

The SPI bus interfacing the contactless reader IC and the MAX32550 are dedicated and not accessible from outside the secure enclosure.