Transaction Security

PCI PTS v4 evaluation report of the Maxim MPOS-STD2

UL Transaction Security (Melbourne) Prestudy report on compliance of the Maxim MPOS-STD2 to PCI PTS v4 requirements.

Make:	Maxim
Model:	MPOS-STD2
Reference Standard:	PCI PTS v4
Certification Body:	PCI Security Standards Council LLC
Evaluation Report No:	UL10244726
Authors:	D. McGregor
Report Type:	Prestudy

This Evaluation Report is Issued under the Authority of Andrew Jamieson, Security Laboratories Manager:

Issue Date: 24 November 2014	Version: v1411241700

UL Transaction Security (Melbourne)
842 High Street,
Kew East, VIC, 3021
Australia
Tel. +61 3 9846 2751
E-mail info@ul-ts.com
Website www.ul-ts.com

Copyright Notice

Version history

Version	Date	Author	Nature of amendment
1411141400	14th Nov 2014	D. McGregor	Initial draft
1411201534	20/11/2014	A Jamieson	Updated during internal review
1411241700	24/11/2014	D McGregor	Incorporate vendor feedback

Quality assurance

Version	Date	QA Reviewer
1411201534	20/11/2014	A Jamieson

Executive Summary

The Maxim MPOS-STD2 is a mobile POS device designed for handling card based payments. This device provides a 12 button keypad, ICCR, MSR, LCD, Bluetooth and contactless with USB and Bluetooth communications.

Picture of MPOS-STD2

UL Transaction Security was asked to perform a prestudy on the MPOS-STD2, focusing on the PCI PTS v4 hardware requirements. Under NDA, a sample device was provided for analysis, along with wiring schematics, PCB layouts and design documents.

This report presents our assessment against the relevant PCI PTS v4 requirements, with detailed analysis of each requirement, overview of architecture and methods and cost estimates of possible attacks.

The audience for this report is the designer, Maxim, and vendors utilising the design for their own products. This report is not designed to be submitted to PCI.

UL found that the hardware design of the MPOS-STD2 is compliant with PCI PTS v4 requirements, provided that suitable firmware and documentation is used.

Table of Contents

1 Introduction

1.1 Identification of Parts

1.1.1 Sponsor

Sponsor	Maxim Integrated
Contact name	Yann Loisel
Contact phone number	+33 442 981 532
Contact e-mail	yann.loisel@maximintegrated.com
Sponsor web-site	www.maximintegrated.com

1.1.2 Device identification

Company	Maxim
Model	MPOS-STD2

1.1.3 Device characteristics

Approval class	PED
PIN Entry Technology	Physical
Functions Provided	Display, ICCR, MSR, PIN Entry, SRED
Communications	USB, Bluetooth
Operating System	FreeRTOS (not tested in this prestudy)
Security Processor	MAX32550 (Cortex M3)

1.2 Associated Documentation

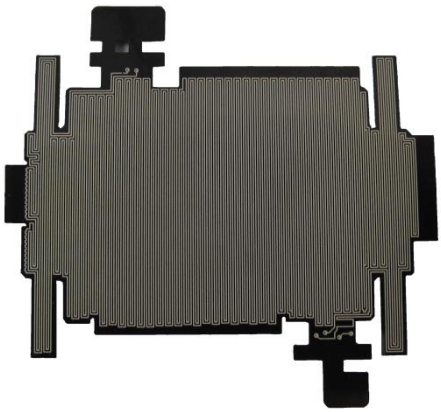
1.2.1 Documentation referenced for this evaluation

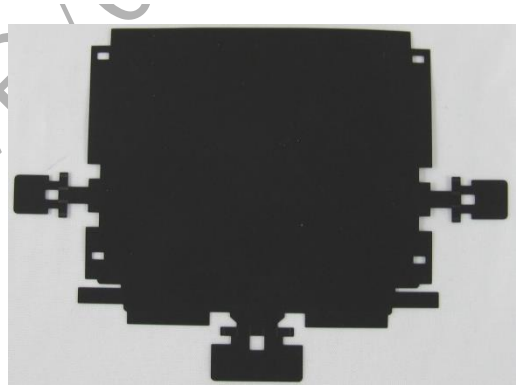
The following documents were referenced for this security evaluation:

Document Reference	Title, version and issue date
[PTS DTRs]	PCI PTS POI Modular Derived Test Requirements, v4 June 2013
[PTS FAQs]	PTS POI Security Requirements – Technical FAQs for use with Version 4 – July 2014
[PTS Guide]	PCI PTS Device Testing and Approval Program Guide, Version 1.3 - September 2013
MAX32550 Datasheet]	DS25H02RevA-max32550_datasheet
MAX32550 User Guide	UG25H05RevB-max32550_user_guide

1.2.2 Physical samples

The vendor provided a single physical sample as shown below. Unassembled meshes for the MSR and smart card circuits were also provided.





1.2.3 Documentation supplied by the device manufacturer

The following documents were supplied by the device manufacturer and were referenced during the evaluation:

Document Reference	Title, version and issue date
PCB Layouts [1]	PCB layout files for the main board and 2 flex foils
Schematics [2]	SC25H07RevB-mpos-std2_schematics.pdf
Hardware Design Guide [3]	RM25H08RevB-mpos-std2_hardware_reference_manual

1.2.4 Other references

Document Reference	Title, version and issue date
[ISO9564]	**International Standards Organisation.** *Banking PIN Management and Security*
[ISO11568]	**International Standards Organisation.** *Banking Key Management (Retail)*
[ANSI X9.52]	**American National Standards Institute.** *Triple DEA Modes Of Operation*
[ANXI X9.24]	**American National Standards Institute.** *Retail Financial Services Symmetric Key Management.*

1.3 Existing Test Evidence

Previously related testing	Title	Date
[ETR]	Prestudy of the MAX32550 against PCI PTS v4 (Not sighted)	Unknown

1.4 Conformance Statements

UL Transaction Security is not permitted to make conformance statements on behalf of PCI Security Standards Council LLC. This report is not designed to be submitted to PCI, but is for information of the chip vendor and terminal manufacturer.

2 Summary of verification of DTRs

2.1 Module 1 – Core Requirements

2.1.1 Core Physical Requirements

DTR	PCI requirement	UL finding
DTR A1	Tamper Detection Mechanisms	VERIFIED*
DTR A2	Independent Security Mechanisms	VERIFIED*
DTR A3	Robustness Under Changing Environmental and Operational Conditions	Should be OK*
DTR A4	Protection of Sensitive Functions or Information	VERIFIED*
DTR A5	Monitoring During PIN Entry	Should be OK*
DTR A6	Determining Keys Analysis	Should be OK*
DTR A7	Physical Security of Display prompts	Firmware dependent
DTR A8	Visual Observation Deterrents	VERIFIED*
DTR A9	Magnetic Stripe Reader	VERIFIED*
DTR A10	Component Protections against Removal	N/A
DTR A11	Audible Tones during PIN Entry	Not evaluated

2.1.2 Offline PIN Requirements

DTR	PCI requirement	UL finding
DTR D1	Penetration Protection	VERIFIED*
DTR D2	ICC Reader Slot Geometry	VERIFIED*
DTR D3	ICC Reader Construction (wires)	VERIFIED*

* These conclusions are based upon an assumption that a submitted device does not deviate from the provided hardware design in any way, and has compatible firmware, complete documentation and suitable lab testing has been performed.

3 Scope

3.1 Hardware

This prestudy report focuses on the hardware design of the MPOS-STD2 and its compliance with PCI PTS v4. Most of the A requirements, D requirements and the first two K requirements have been addressed.

The device provided for evaluation did not contain working software, therefore it was not possible to test or confirm some of the hardware related requirements. Assumptions have been made where appropriate and have been documented in this report.

Analysis of the MAX32550 has also not been attempted. The vendor has commissioned a separate prestudy into the processor, and this is expected to be available to the readers of this report.

The physical sample provided for this review was an early version. An additional tamper switch was added to the rear of the device to detect removal of the rear casing and battery. The vendor provided the design files for this change, but no physical sample was sighted by the evaluator.

3.2 Firmware

Firmware was out of scope of this review and does not form part of this report. Assumptions about firmware behaviour have been made where necessary to enable the hardware evaluation to be completed.

4 Module 1: Core Requirements

4.1 Core Physical Requirements

DTR A1 Tamper-Detection Mechanisms	Result:	VERIFIED*

The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, as defined in Appendix B.

Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours' attack time for exploitation.

Guidance

The objective of this section is to assess the device's ability to protect clear-text PINs and other sensitive data. Attack scenarios must be in support of the compromise of clear-text PINs and other sensitive data as noted in A1.

Requirement A6 focuses on determination of secret or private keys. This requirement focuses on tamper-detection and response mechanisms in place to prevent PIN disclosure.

"Immediate" is defined as fast enough to ensure erasure occurs before the tamper-detection mechanisms can be disabled using attack methods described in A1.

For those devices that do not contain secret information, device disablement may be used in lieu of "immediate erasure of all secret information."

"Secret information" consists of any private or secret cryptographic keys that the device relies on to maintain security characteristics governed by PCI requirements. If any of these keys are not zeroized, then other mechanisms must exist to disable the device, and these keys must be protected in accordance with Requirement A6.

Secret or private cryptographic keys that are never used to encrypt or decrypt data, or are not used for authentication, do not need to be considered secret data and therefore do not need to be erased—for example, where the device uses a chip set that automatically generates keys at initialization but the keys are not subsequently used by the device.

When designing an attack against the device as part of A1, replacement of casing parts like the front and rear case of the device shall be considered as part of the overall attack.

In addition to the specified minimum attack potential values, any feasible penetration attack against the device for the purpose of determining or modifying sensitive data must entail at least ten hours of exploitation time.

If switches are used as the primary protection for the area around a physical keypad area, then at least three blind, tamper switches must be implemented. The switches must be protected from attacks that use the application of adhesives or conductive liquids to disable the switches. The design must ensure that a minimum of three switches in the keypad area must be individually attacked to disable them. Note that these criteria are in addition to exploitation time and attack potential minimums and that the keypad in question is a physical keypad, not a touch screen.

If tamper grids are used as a primary mechanism, they meet the following:

- *Use a minimum of two layers of internal grids for protection.*
- *Vias of "upper grid" must be protected separately to vias of "lower grid" (for example, the two tamper grids must not be connected by vias that are accessible on both grid layers, or vias must be protected by other tamper mechanisms, such as switches).*
- *Minimum width / separation (of active traces) of 6 mil.*
- *Use "opposing" tamper-responsive traces routed side-by-side on each layer.*

Tester(s): D. McGregor

Vendor documentation (TA1.1 & TA1.2)

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts
- Schematics

Design overview (TA1.3)

The MPOS-STD2 is a handheld battery powered terminal designed to accept mobile payments. The terminal contains MSR and ICC readers, with a keypad and graphic LCD. Bluetooth* is used to communicate with the mobile phone or POS.

Note: At the time of writing, PCI does not accept the use of Bluetooth v4 Low Energy modules, and so any implementer of this reference design must ensure that either the module they use does not provide Bluetooth v4Low Energy functions, or confirm that PCI have updated their stance on this communications method.

Figure 1: Perspective view of the MPOS-STD2

Figure 2: Perspective view of the MPOS-STD2 without outer casing

The outer casing is constructed from two main plastic housings which are clipped together. The upper housing contains openings for the display lens and the keypad. The keypad is a separate plastic module which clips over the main PCB. A picture of the device without external casing is shown in Figure 2.

The MPOS-STD2 is a based around a single rigid main PCB. On the upper face of this board is the keypad and LCD.

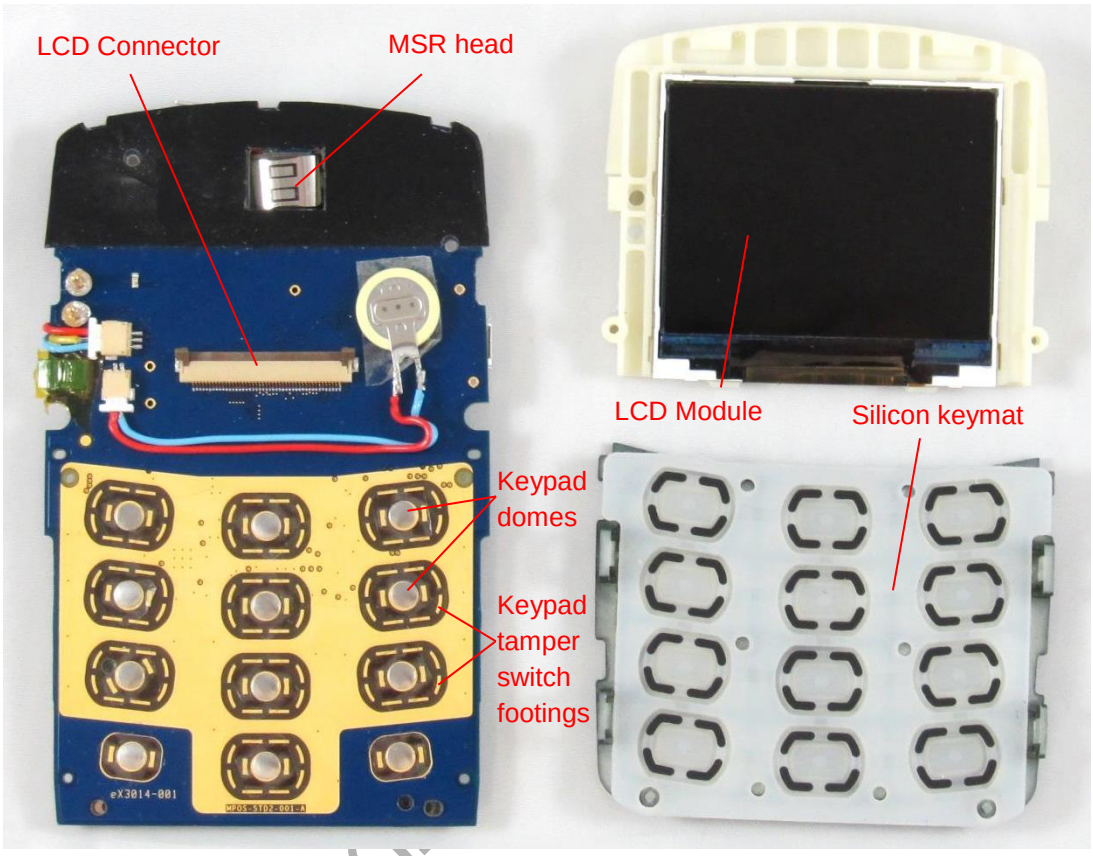


Figure 3: Upper face of main PCB, with keypad assembly (underside) and LCD module (topside)

The keypad module consists of 12 hard plastic keycaps which are attached to the silicon keymat. Pressing the keycaps transfers the pressure to the metal domes on the main board, which is monitored by the processor. A cell battery between the LCD and main board provides power to the security circuitry when the main battery is flat or disconnected.

The main processor (MAX32550) is located on the rear of the main board, directly underneath the keypad. An ICC acceptor, MSR connector, Bluetooth module and USB connector are also present on the underside of the main board.

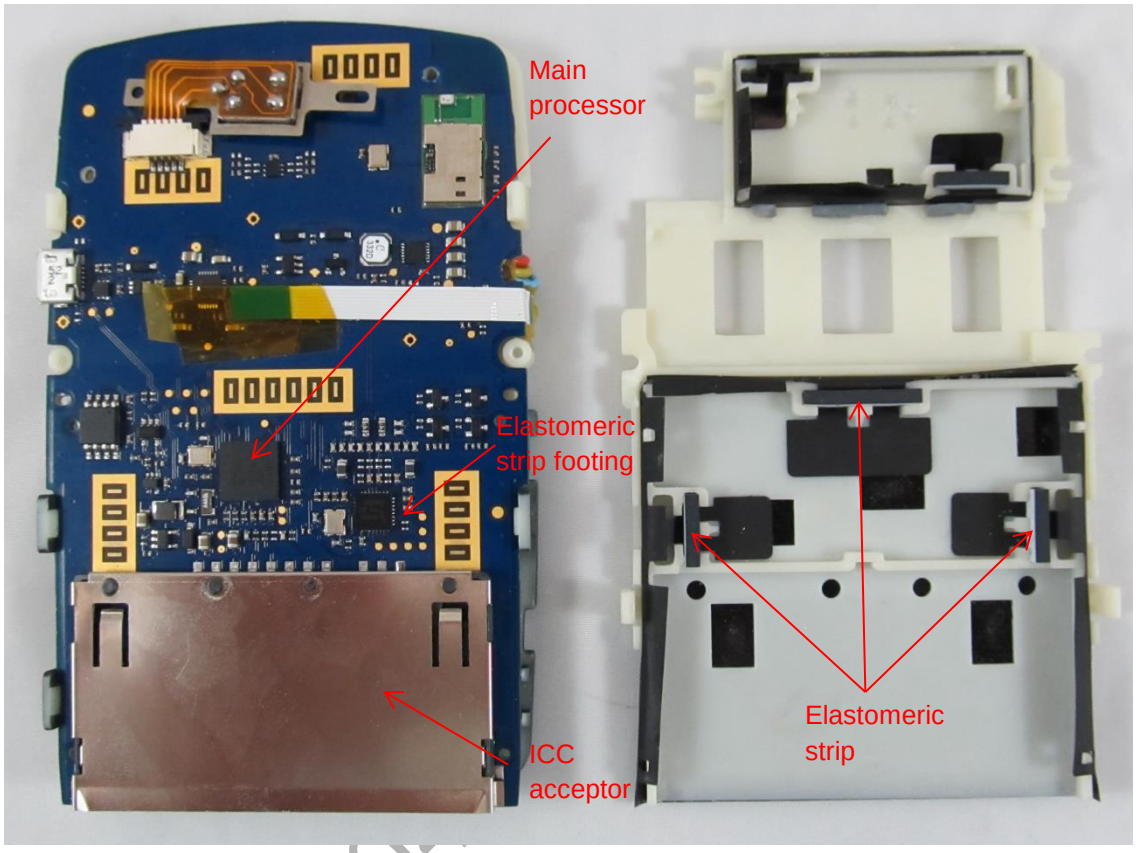


Figure 4: Lower face of main PCB(left) and plastic formers with flex meshes (right)

Protection against probing of the processor and other sensitive components is provided by flexible meshes covering two sections of the board.

A plastic outer casing encloses the main board and all components as shown below. No tamper mechanisms are used to detect removal of this casing.

Figure 5: Side view of MPOS-STD2 showing outer case housings

PIN entry mechanism (TA1.4)

Keypad buttons are constructed from a hard plastic keycap, which presses through a silicon keymat onto metal domes on the main board. Keycaps are inserted from the front of the device and protected against removal by being glued to the silicon keypad.

Each numeric key included an embedded tamper switch composed of plated footings on the main board, carbon on the silicon keymat depressed by the plastic frame surrounding the keys.

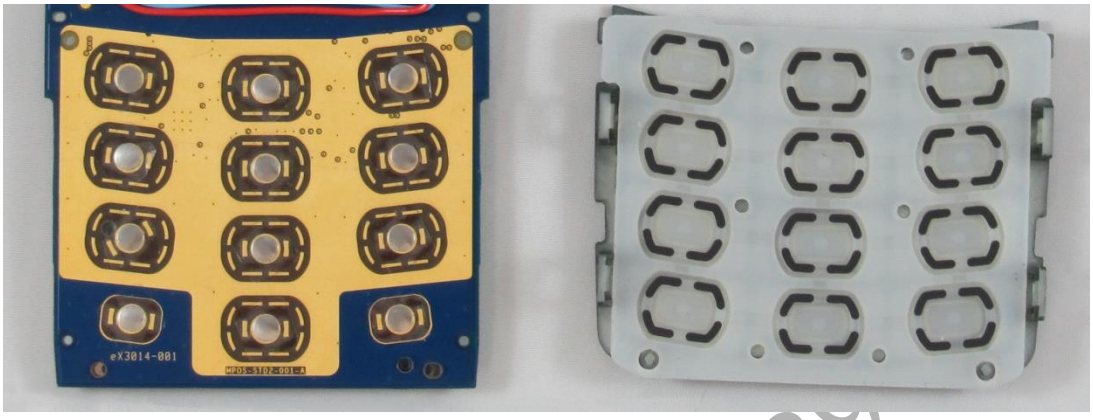


Figure 6: Keypad footings and underside of keypad assembly

Keypad path to processor (TA1.5 & TA1.6)

Review of the schematic showed the keypad footings are connected directly to the processor without any discrete circuitry. The processor is located on the underside of the main board, and the path between the keypad and processor is protected by the keypad tamper switches from the front, and the ICC mesh from the rear.

Traces connecting the row and column signals to the processor are routed exclusively in the PCBA board. Review of the PCB layout files confirmed that vias connect the footings to traces on layer 6. These traces, and some on layer 7, connect to the processor.

The MAX32550 includes a secure keypad controller which is used to drive and monitor the row and column signals of the keypad. The datasheet for the processor indicates it uses a randomised matrix scanning algorithm to complicate bugging of the keypad. No physical testing was performed during this prestudy. The use of randomised scanning is expected to add extra identification time and a more sophisticated bug.

Circuit Boards (TA1.7)

Circuit boards used in the device are tabled below.

PCB Designator	PCB Version	PCB Purpose	Sensitive Signals	Tamper-Detection Mechanisms
PCBA (8 layer board)	MPOS-STD2-0010B	Contains all active components	Keypad, ICC, MSR, Contactless	Mesh in layers 2 and 40 switches in keypad area 1 switch on rear
MSE Mesh		Protect MSR and cable	None	Two layers of mesh
Smartcard Security Film		Protect ICCR and processor	None	Two layers of mesh

PCBA (Main Board)

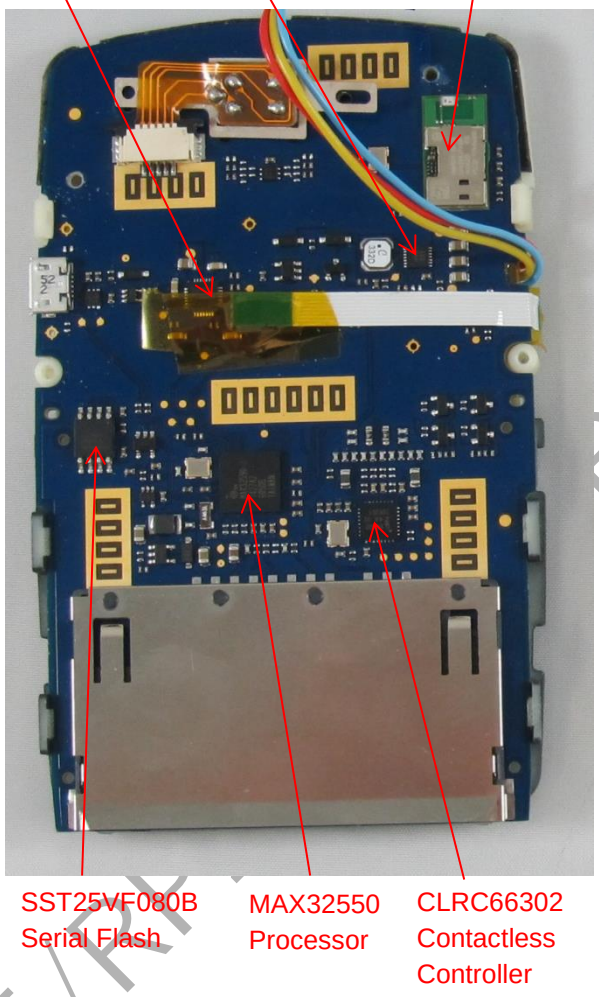


Figure 7: Lower face of PCBA board

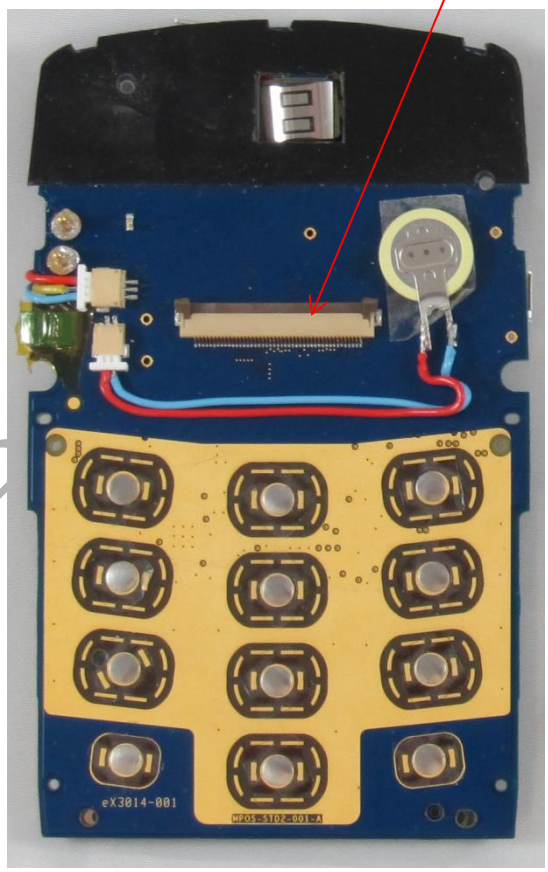


Figure 8: Upper face of PCBA board

MSE Mesh

The MSE mesh is used to protect the MSR head, cable, connector and filter components against probing from the rear and sides. The MSE mesh is composed of silver ink printed onto a black plastic sheet. Additional black plastic is adhered to the top and bottom to make the complete stack. The stack is then folded around a plastic former with elastomeric strips used to contact the footings on the main board and MSE mesh. Traces in the two mesh layers are run in perpendicular directions and shown in the pictures below.

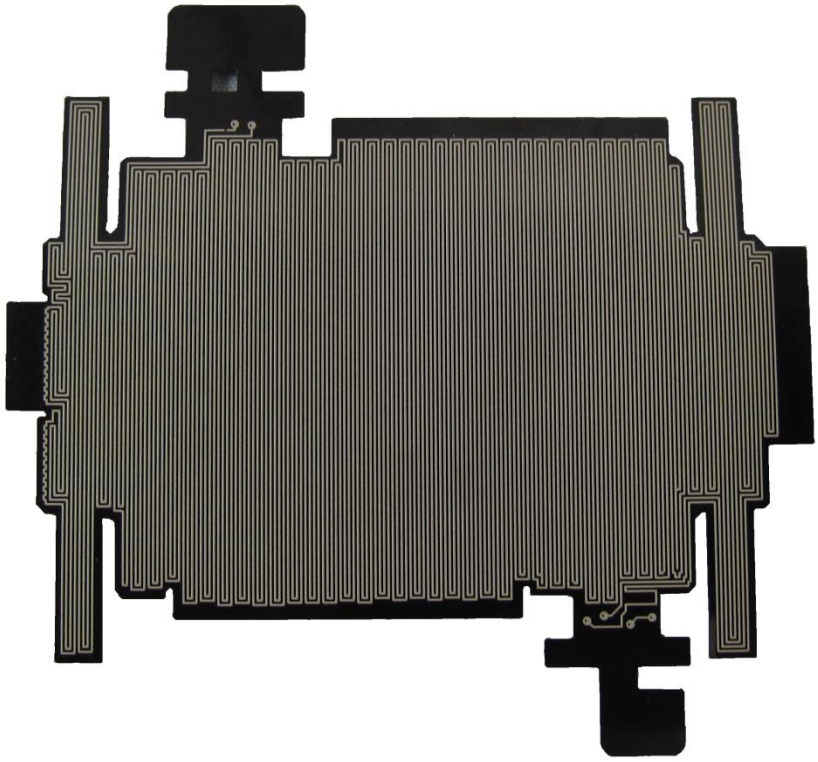


Figure 9: Underside view of MSR mesh (with outer plastic layer removed)

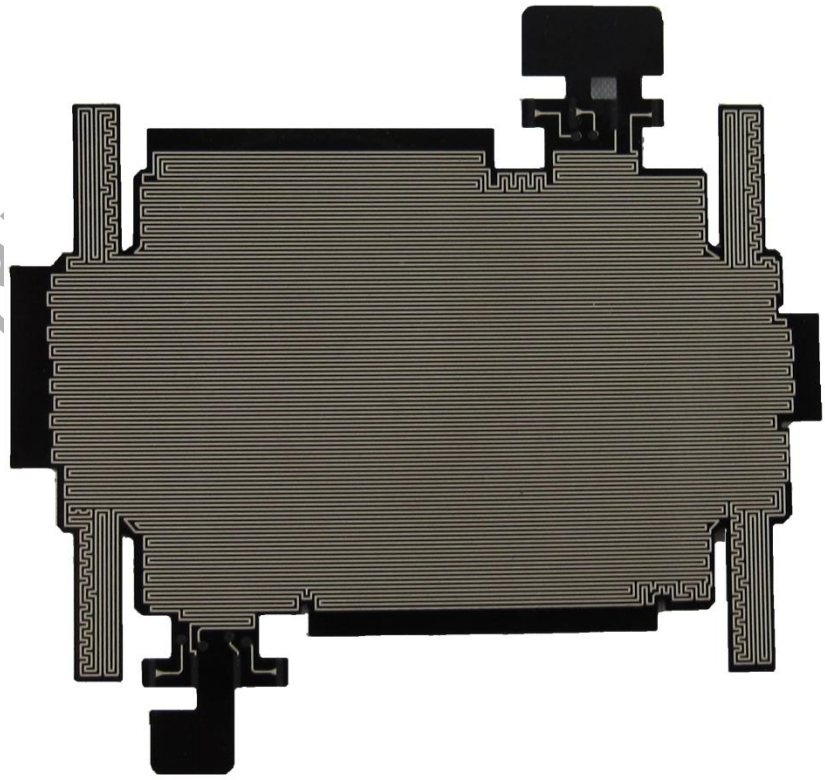


Figure 10: Topside view of MSR mesh (with outer plastic layer removed)

Smartcard Security Film

The smartcard security film is used to protect the ICC acceptor, security processor, contactless controller and other discrete circuitry. The flexible mesh is folded around a plastic former and placed against the lower face of the main board, providing protection against penetration through the rear or the sides of the device.

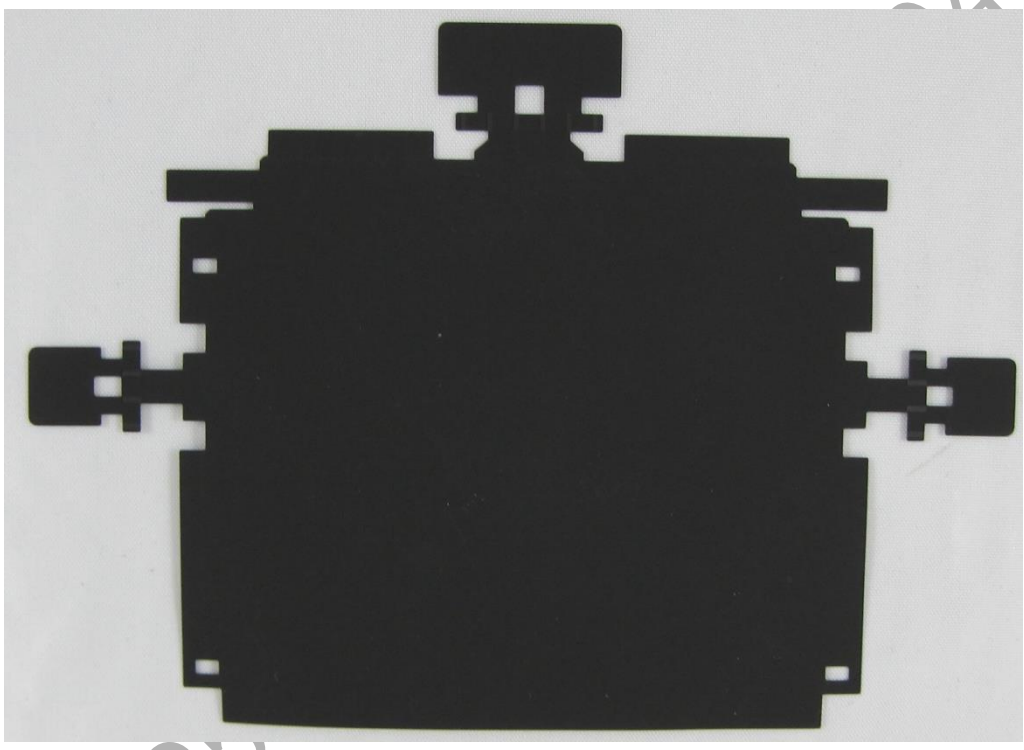


Figure 11: Topside view of smart card mesh

Protection of keypad signals (TA1.8 & TA1.9)

Signals between the keypad footings and security processor are located exclusively within the PCBA board. Attacks through the rear are prevented by meshes in the smartcard security film, which was confirmed to cover all keypad signal vias and traces. Access to keypad footings through the front would require disabling of the keypad area tamper switches. Vias are located underneath these footings. Meshes in layers 2 and 3 protect the keypad signals routed in the 6th and 7th layers.

Review of the schematic and PCB layout files confirmed that there are no passive components on the keypad path.

Tamper grids (TA1.10)

Tamper grids are present in the three printed circuits as tabled below.

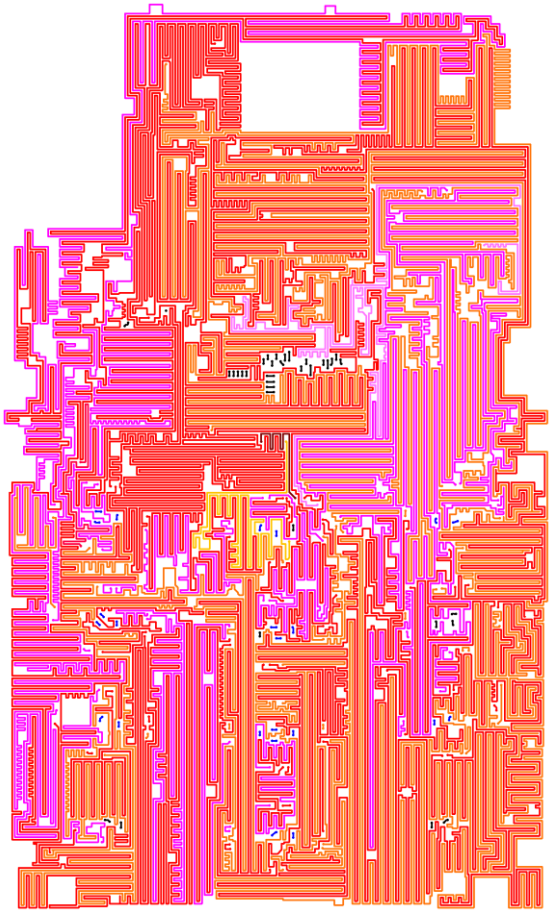
Tamper grid location	Physical implementation	Trace width	Trace spacing or distance between layers	Number of traces ^	Method of connection	Method of monitoring
PCBA Layer 2	Copper and FR4 rigid PCB	6 mil	6 mil	5 active	half blind vias	Dynamic (S0, S1, S2, S3, S4, S5)
PCBA Layer 3	Copper and FR4 rigid PCB	6 mil	6 mil	5 active	half blind vias	Dynamic (S0, S1, S2, S3, S4, S5)
MSE mesh layer 1	Silver trace and PET flex PCB	6 mil	6 mil	2 active	Pad for elastomeric strip	Dynamic (S0, S1)
MSE mesh layer 2	Silver trace and PET flex PCB	6 mil	6 mil	2 active	Pad for elastomeric strip	Dynamic (S2, S4)
Smartcard security film layer 1	Silver trace and PET flex PCB	6mil	6 mil	5 active	Pad for elastomeric strip	Dynamic (S0, S2, S3)
Smartcard security film layer 2	Silver trace and PET flex PCB	6 mil	6 mil	5 active	Pad for elastomeric strip	Dynamic (S4, S5)

^ Active traces are connected to the tamper detection circuitry, passive traces are connected to ground or power.

PCB layouts for the MSE mesh were examined, with colourised meshes provided below.

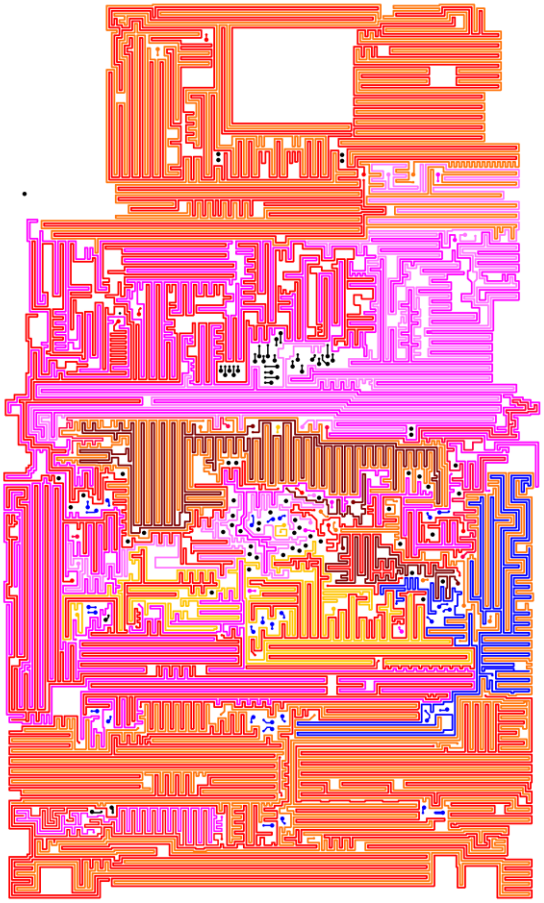
PCBA Meshes

The 8 layer main board, PCBA, contains meshes in layers 2 and 3. These meshes are routed across the entire board and provide protection against frontal penetration. These meshes are



2

Figure 12: Layer 2 mesh of PCBA board



3

Figure 13: Layer 3 mesh of PCBA board

MSR Mesh

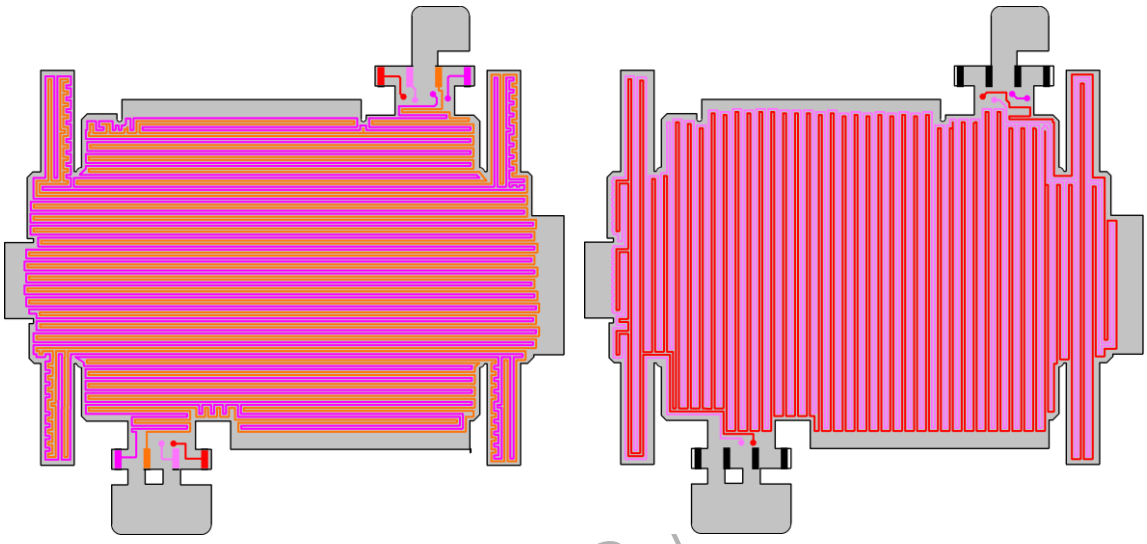


Figure 14: Colourised traces in the MSE mesh

A section of the plastic cover on this mesh was abraded to confirm that silver ink traces were present and consistent with the design files. Meshes on layer 1 and layer 2 are run in different directions, preventing any attack which cut along the length of the tamper mesh.

Smartcard Security Film

The smartcard security film contains two mesh layers. These layers use 6 mil conductive ink traces on plastic film. Mesh traces terminate on one of 14 carbon footings on the 3 tabs visible in the picture (right). These tabs are folded around the plastic former. When assembled the tabs are enclosed by the rest of the mesh.

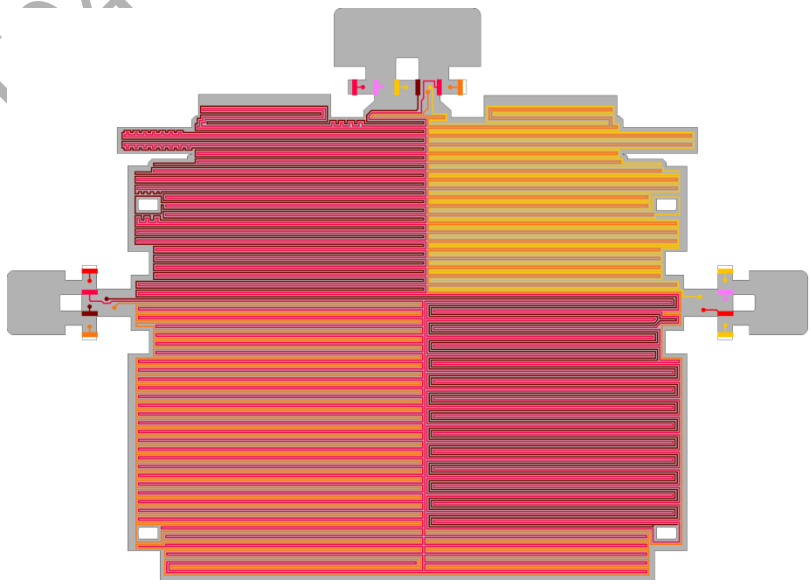


Figure 15: Colourised traces in the MSE mesh, layer 1

Traces in the two layers of mesh run in opposing directions, preventing the cutting of the mesh in the gaps between the traces.

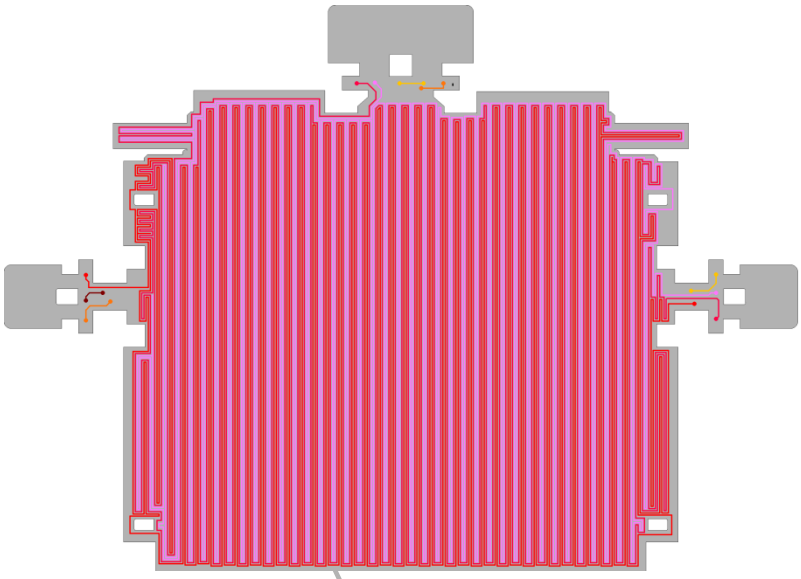


Figure 16: Colourised traces in the MSE mesh, layer 2

Tamper grid effectiveness (TA1.11)

Tamper grids in the MSE and smartcard security film use conductive ink on film technology. The evaluator has seen a number of similar meshes and has not found an effective method to bypass them.

The two layers of tamper mesh in the PCBA board use 6 mil copper traces on a fiberglass base. This is a common design and penetration through this mesh requires multiple hours of expert skill to bypass, which meets PCI PTS v4 requirements.

Tamper switches (TA1.12)

The MPOS-STD2 contains tamper switches around each numeric keypad button. This provides detection of key removal and front case removal.

Switch location	Number of switches used in that location	Physical implementation	Size of switch contacts	Conductive ink protections	Additional comments
Keypad area	40	Conductive footing with carbon pill	3mm x 0.8mm	Ground plane 2 mm from contacts	
Rear case	1	Mechanical micro switch		Located underneath battery	

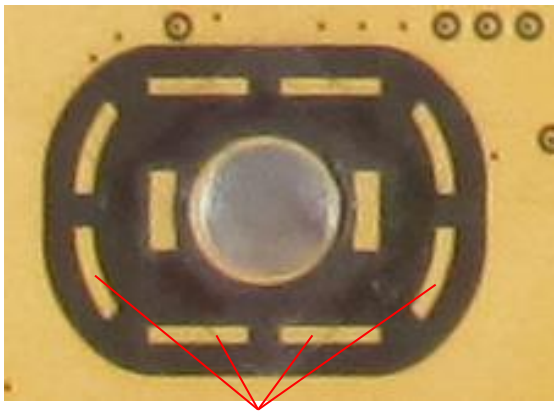


Figure 17: Keypad tamper switch footing

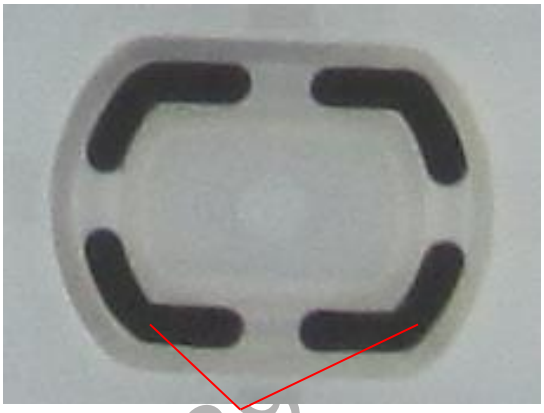


Figure 18: Keypad tamper switch pill

Pressure on the carbon pills is applied through the plastic frame surrounding the keypad buttons. This frame is clipped onto the PCBA board in four locations.

Tamper switch effectiveness (TA1.13)

The use of a plated ground plane and independent circuits on each pair of contacts protects against the use of conductive ink to disable the tamper switches. Gluing down all switches is difficult due to the limited access to the switches and the number of switches.

Any direct attack on the switches would have to be applied to all 40 switches, which is unlikely to be the most effective way to bug the keypad signals.

Removal of the rear casing is not detected by any tamper switches, however no keypad signals are accessible with only removing the rear casing.

Tamper monitoring (TA1.14)

The MAX32550 processor contains a module designed to energise and monitor tamper signals. Each of six output pins are randomly pulled high or low. If the processor does not read the same voltage on the related input pin a tamper signal is generated. Shorting of any tamper signal to a fixed voltage or to another tamper signal will be detected as an attempted tamper.

Tamper switches and meshes are connected in series to one of the six tamper circuits.

Volume encapsulation methods (TA1.15 & TA1.16)

No volume encapsulation methods are used.

Attachment or forming methods (TA1.17 & TA1.18)

The folded MSE mesh has elastomeric strip footings in two of the corners, leaving the other two corners potentially vulnerable to a bending attack. The MSR mesh is used to protect only magnetic stripe signals, and a costing has been provided in DTR A9.

Three elastomeric strips are used to detect separation of the mesh from the main board. These strips are located near the middle of the three sides, potentially allowing for the corners to be bent up. The mesh is folded around the internal plastic former, and testing found that it was not possible to unwrap the mesh from any of the corners. Cutting the former was found to be infeasible, as it is protected by the mesh at all points except near the ICC slot opening.

Accessing the former through the slot involves cutting through the metal casing of the acceptor and carefully cutting the plastic without damaging the flex.

Security processor and tamper circuitry (TA1.19)

The MPOS-STD2 uses a MAX32550 processor which contains the following security features.

- Six dynamic tamper detection sensors
- Temperature, die shield and battery voltage sensors
- True random number generator
- Secure battery backed key storage register
- Hardware cryptographic accelerators
- 1MB flash memory, 256KB system SRAM, 8KB NVSRAM and 4KB OTP memory
- Secure keypad controller
- Chain of trust boot process

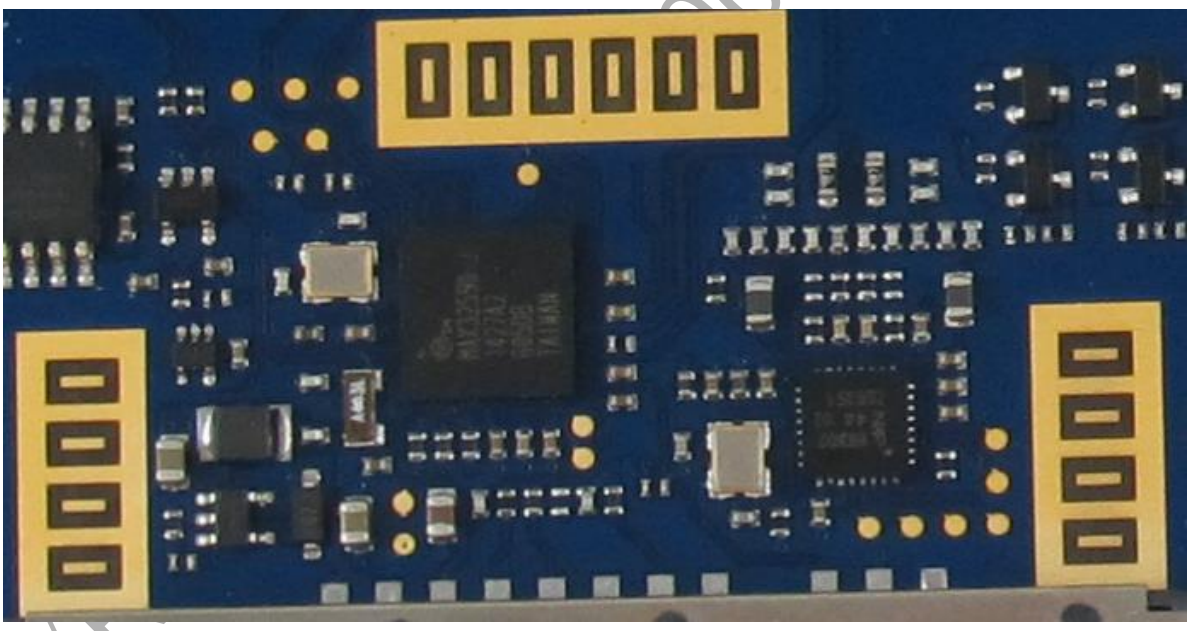


Figure 19: Underside of PCBA showing processor and other circuitry

Other security features (TA1.20)

The MPOS-STD2 relies upon the tamper switches and meshes to protect the keypad signals. No other security features are used.

Tamper circuit diagram (TA1.21)

The processor contains 6 pairs of tamper detection signals which are used to monitor all tamper meshes and switches in the device. The forty tamper switches in the keypad are connected to one of three signals as shown in the picture below.

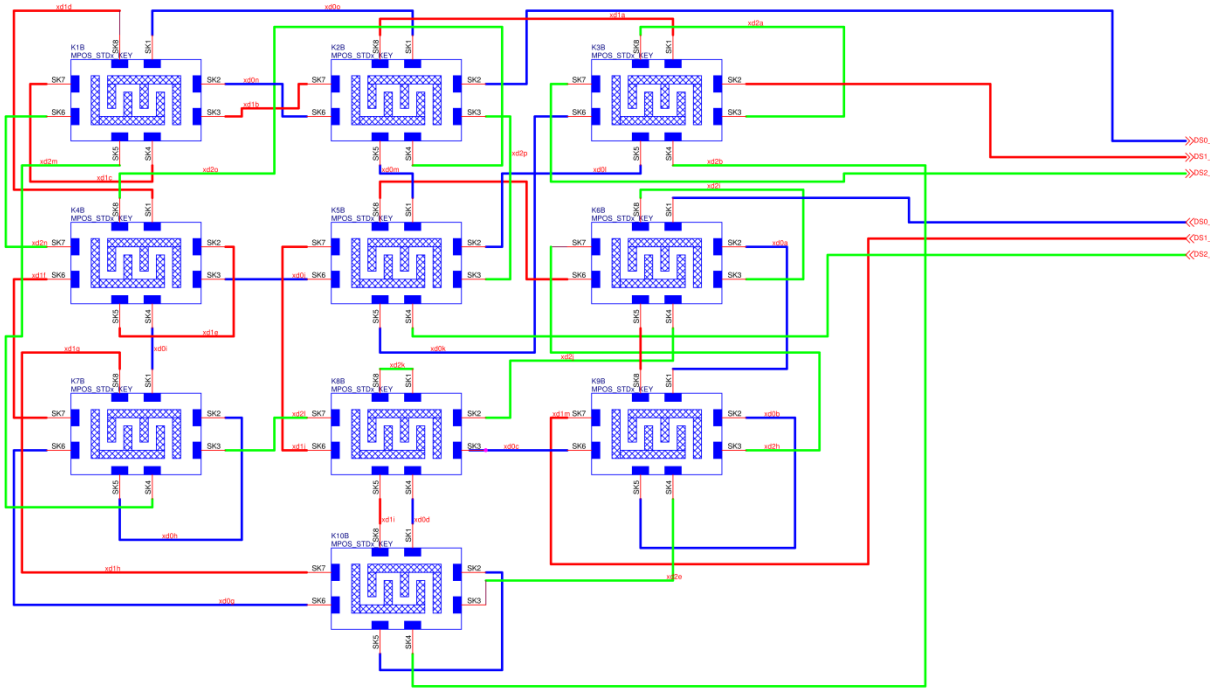
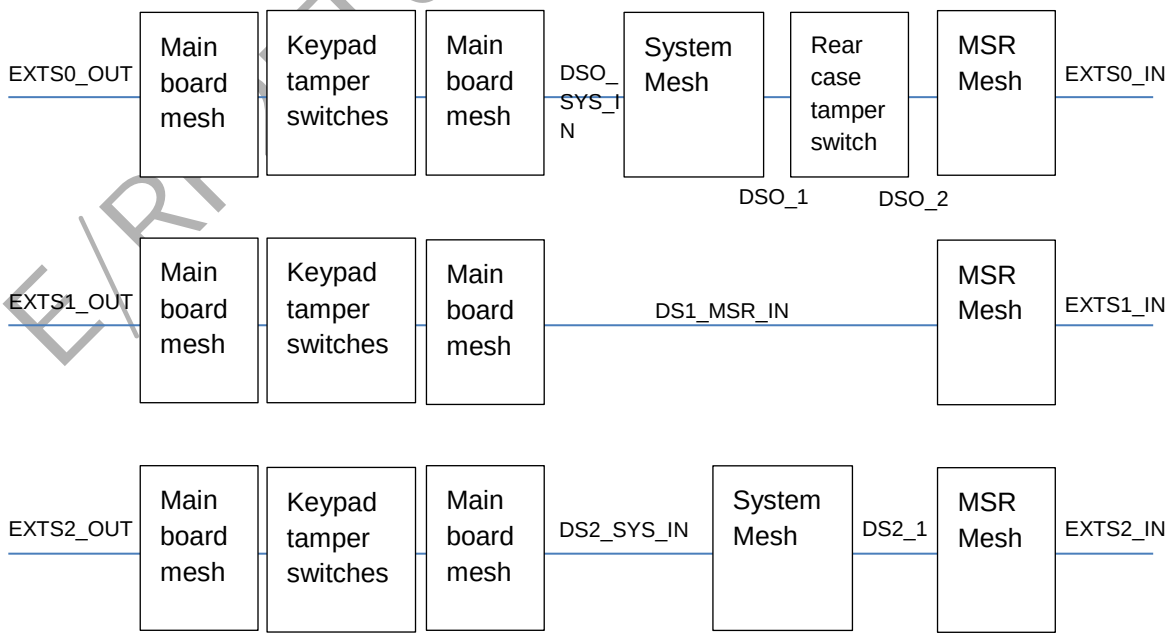


Figure 20: Circuit diagram of the keypad tamper switches

Meshes and other switches are connected as shown in the diagrams below. Review of these connections show that multiple circuits must be disabled for any attack direction. There are no easily accessible points which can be used to disable one or more meshes.



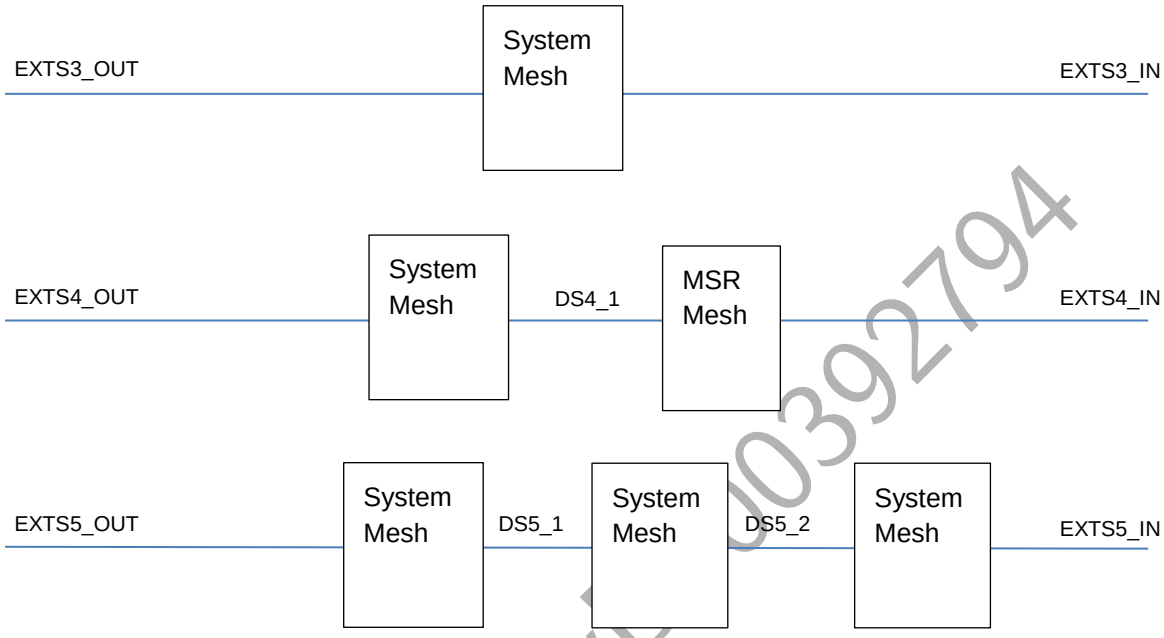


Figure 21: Block diagram of the meshes and switches connections to the processor

Protection of tamper signals (TA1.22)

Passive components

No passive components (resistors or capacitors) are connected to the tamper detection circuits.

Connectors

The only connectors used to carry tamper signals are the elastomeric strip footings connecting the main board to the flex meshes. These connectors were checked and found to be inside secure sections surrounded by two layers of tamper mesh.

Vias

The smartcard security film and keypad are located on opposite sides of the PCBA board, each providing protection against accessing signals and vias in the middle of the PCBA. Vias connecting the MSR mesh to the traces in the PCBA board are present on layers 2-8. Access to the layer2 vias is prevented by the LCD screen and layer1 (copper). Exposing and shorting these vias would only disable the MSR mesh.

Tamper response (TA1.23, TA1.24 & TA1.25)

Tamper response is handled by the hardware logic in the MAX32550 processor. If a tamper event is detected the processor clears the AES key register, records some details of the event and causes an interrupt (if powered on).

The AES key is used by the processor hardware to encrypt all information stored in the secure SRAM segment. Erasure of the AES key will cause all information in this segment to be unrecoverable.

No functional testing was performed during this prestudy, as details of the firmware were not provided. With suitable firmware the tamper response will meet PTS requirements.

External Overlay Attack (TA1.26)

An external overlay attack places a secondary keypad on top of the existing keypad, which records the button presses.

The keypad in the MPOS-STD2 is flush with the upper case housing. Adding an external overlay would change the visual design and be obvious as a change.

Internal Overlay Attack (TA1.27)

This attack inserts an overlay between the keypad buttons and the keypad footings.

Each numeric keypad button is surrounded by 4 tamper switches, which detect separation of the keypad frame from the main board. Insertion of an internal overlay would require disabling these 40 buttons (monitored with 3 dynamic signals).

Side Attack (TA1.28)

A side attack accesses keypad signals by penetrating through a side of the device.

Keypad signals connect the keypad footings to the processor through traces in the main PCB. No discrete components are connected to the keypad signals. Side penetration into the secure section is prevented by the meshes in the ICC cover, and even in access is gained there are no readily accessible components to probe.

Adding additional sensors into the silicon keymat was considered but discounted due to the difficulty of insertion, particularly for the central buttons (2,5 & 8).

An attack through the ICC is limited by the small slot height, but does not have any mesh protection. The lack of probable points also makes an attack through the ICC difficult.

Rear Attack (TA1.29)

A rear attack aims to penetrate through the device to access the keypad signals.

Access from the rear is protected by the smartcard security film mesh and MSR mesh. Even if the smartcard security film is disabled, keypad signals are still embedded in internal layers of the main board. A rear attack would be difficult requiring skills to bypass the flexible mesh and careful abrading of the main board to expose the keypad signals.

Frontal Attack (TA1.30)

A frontal attack penetrates through the front of the device to access sensitive keypad signals.

An attack through the front would damage the casing or key caps. Replacing the casing would require the disabling of the keypad area tamper switches. Keycaps are glued to the silicon keymat, which have carbon pills used as tamper switches. Attempts to pry the keycaps from the silicon mat were found to pull the carbon pills off the contacts, triggering a tamper event.

An attack which cuts away the keycaps, wires up a bug to the contacts and repairs the damage was considered the most feasible and is costed below.

There are no sensitive signals underneath the LCD, and an attack which removes the LCD was not found to be viable.

Attacks for Online PINs (TA1.31 & TA1.32)

A number of attacks for online PINs were considered, and a key removal attack found to be the most feasible. Details are provided below.

Attack "P1" for Online PINs

Identification stage of attack "P1"

1. Obtain a mechanical sample and disassemble and understand the tamper detection mechanisms and mechanical structure.
2. Devise a plan to expose the keypad footings and insert new switches. Limited free space in the casing will require the development of a custom bug.
3. Practice the attack on a functional sample

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Expert	Public	Standard	None	1 Mechanical	80 hours
2	Expert	Public	Standard	Standard		40 hours
3	Expert	Public	Standard	None	1 Functional without keys	20 hours

Exploitation stage of attack "P1"

1. Cut the rear casing and glue down the battery, which is holding the rear tamper switch shut. Remove the front casing, leaving the keypad plastic intact.
2. Carefully cut off the key cap from each of the keypad buttons. Insert either a microswitch or capacitive touch plate and thread wires out through the side of the keypad. This step requires expert skill as each button contains embedded tamper switches which must not be activated. Inserting additional switches into the keycaps is not easy, and any misstep will cause the obvious visual changes or a different feel to the keypad. Spare keycaps are glued back over the switches to make the keypad look unaltered.
3. Connect the wires to a bug located around the rear of the device. Reassemble with a spare rear casing and return to service.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Proficient	Public	Standard	None	1 Functional with keys	3 hours
2	Expert	Public	Standard	None		8 hours
3	Proficient	Public	Standard	Specialized		1 hour

Cost breakdown of attack "P1"

Identification Phase	Value	
Attack Time	5	≤ One hundred and sixty hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	3	One mechanical and one functional sample without keys
Equipment required	0	None (re-used during exploitation)
Specific Parts	1	Standard
Identification Total	**13.0**	

Exploitation Phase	Value	
Attack time	3	≤ Twenty four hours

Expertise	4	Expert
Knowledge	0	Public
Access Costs	4	Functional sample with working keys and software
Equipment required	1	Standard
Specific Parts	1	Standard
Exploitation Total	**13.0**	
Grand Total	**26.0**	

Attack "P2" for Online PINs (TA1.31-2)

Identification stage of attack "P2"

1. Obtain a mechanical sample and disassemble and understand the tamper detection mechanisms and mechanical structure.
2. Devise a plan to disable the keypad area tamper switches. Create an internal overlay which can be overlaid across the keypad area of the main PCB to monitor key presses.
3. Practice the attack on a functional sample.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Expert	Public	Standard	None	1 Mechanical	80 hours
2	Expert	Public	Standard	Standard		40 hours
3	Expert	Public	Standard	None	1 Functional without keys	20 hours

Exploitation stage of attack "P2"

1. Cut the rear casing and glue down the battery, which is holding the rear tamper switch shut. Remove the front casing, leaving the keypad plastic intact.
2. Carefully cut/drill through the keypad and expose 6 of the tamper switch footings. Attach wires between related pairs of footings to disable the tamper switches. The footings are 1mm x 3mm in size and attaching wires to these contacts without interrupting the tamper signal would require expert skill. Each contact is expected to take an hour to tap, requiring a total of 6 hours to complete this step.
3. With the tamper switches disabled, carefully cut and remove the keypad. Insert the custom overlay and replace the keypad with a spare part. Care must be taken not to dislodge any of the wires attached in step 2, otherwise the device will tamper and the attack failed.
4. Connect the overlay to a bug and wire the bug to the battery. Replace the front and rear casings and return to service.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Proficient	Public	Standard	None	1 Functional with keys	3 hours
2	Expert	Public	Standard	Standard		6 hours
3	Proficient	Public	Standard	None		2 hours
4	Proficient	Public	Standard	None		1 hour

Cost breakdown of attack "P2"

Identification Phase	**Value**	
Attack Time	5	≤ One hundred and sixty hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	3	One mechanical and one functional sample without keys
Equipment required	0	None (re-used during exploitation)
Specific Parts	1	Standard
Identification Total	**13.0**	

Exploitation Phase	**Value**	
Attack time	3	≤ Twenty four hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	4	Functional sample with working keys and software
Equipment required	1	Standard
Specific Parts	1	Standard
Exploitation Total	**13.0**	
Grand Total	**26.0**	

DTR A2 Independent Security Mechanisms	Result:	VERIFIED*
Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.		
Guidance *In general, techniques may include any combination of tamper-detection methods. Security mechanisms must not rely on insecure services or characteristics provided by the device such as (but not limited to) its power supply and unprotected wires. Tamper-evident labels and similar methods involving tamper evidence are not considered a security mechanism.* *This requirement does not imply the need for redundant security mechanisms, but rather separate mechanisms of a different nature.*		
Tester(s): D. McGregor		

Vendor documentation (TA2.1 & TA2.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Multiple security mechanisms (TA2.3 & TA2.4)

The MPOS-STD2 has the following security mechanisms

- 40 tamper switches in the keypad area
- A rear case removal switch
- 2 layer flexible meshes covering the ICC and MSR sections
- 2 layers of mesh in the main board
- 6 independent dynamic tamper monitoring circuits
- Temperature and voltage environmental sensors
- Die level tamper mesh

Attack vectors from every angle require the bypassing or disabling of at least 2 meshes or tamper switches.

Disassembly and review of the device was used to confirm that the protection mechanisms described by the vendor are present and were included in the assessment of DTR A1.

DTR A3 Robustness Under Changing Conditions	Result:	Should be OK*

The security of the device is not compromised by altering:

- ***Environmental conditions***
- ***Operational conditions***

(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)

Guidance

The vendor must either provide substantive data to support the security of the product functioning outside normal operating conditions, or show that the product uses sensors that will trigger a tamper response.

The objective is not to replicate the vendor testing, but instead it is to account for shortcomings within the vendor's testing of the implementation.

The tester may rely upon vendor testing as appropriate to fulfill the following test steps.

Tester(s): D. McGregor

Vendor documentation (TA3.1 & TA3.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Operational Environment (TA3.3)

No details of the intended operational environment were supplied for this prestudy.

Temperature ranges for tamper components (TA3.4)

The MPOS-STD2 uses a combination of tamper switches and tamper meshes to detect attempts to tamper with the device. Meshes and switches are connected serially to one of five circuits, which are directly connected to the security processor. No discrete components or other circuitry is used in the tamper detection mechanism.

Environmental Sensors (TA3.5 & TA3.6)

Processor temperature, battery voltage and core voltage sensors are embedded into the security processor. The data sheet for the processor shows that the tamper response mechanisms work correctly throughout the range of temperature and voltage conditions allowed by the sensors. Temperatures or voltages outside this range will cause the erasure of the secret keys in the battery backed memory.

Testing (TA3.7 & TA3.8)

Testing on the environmental sensors has/is being performed in a separate evaluation. No testing was performed on the MPOS-STD2 terminal. If the configuration of the processor is compatible with the chip testing then results would apply to the full device.

Attacks (TA3.9 & TA3.10)

Tamper switches, tamper meshes and the security processor will operate normally within the temperature and voltage ranges allowed by the environmental sensors. For details of the effectiveness of the environmental sensors see the chip evaluation report.

DTR A4 Protection of Sensitive Functions or Info	Result:	VERIFIED*
Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation, as defined in Appendix B.		
Guidance *Public keys used for functions that impact security requirements, such as firmware updates, display prompt control, or remote key distribution schemes must be protected against modification and substitution. Secret and private keys used for functions that impact security requirements must be protected against modification, substitution or disclosure.* *Protected area of the device is that area(s) within the boundaries of the tamper-detection and response mechanisms.* *The lab shall consider both voltage and EM glitch attacks. At a minimum, these should consider the core and battery input for the security processor.*		
Tester(s): D. McGregor		

Vendor documentation (TA4.1 & TA4.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Sensitive information stored in the device (TA4.3 & TA4.4)

The scope of this prestudy did not include the firmware, therefore the answers to this requirement are based upon details in the processor datasheet, the hardware reference manual and a typical software architecture.

Sensitive Information	Persistent Data		Temporary Data	
	Storage Area	Protection	Storage Area	Protection
Plaintext PINs	-	-	Internal SRAM	Processor package, ICC mesh
Passwords (if used)	Internal NVSRAM	Processor package, ICC mesh, encryption under secure AES key	Internal SRAM	Processor package, ICC mesh
Acquirer keys	Internal NVSRAM	Processor package, ICC mesh, encryption under secure AES key	Internal SRAM	Processor package, ICC mesh
Main Firmware	Internal flash	Processor package, ICC mesh, ECDSA signature	-	-
Boot ROM including public key	ROM	Processor package, ICC mesh, being in ROM	-	-

Debug or test functions for sensitive components (TA4.5, TA4.6 & TA4.7)

All plaintext information storage and processing is performed within the MAX32550 processor. The processor contains a boot ROM which supports loading of signed code through the serial or USB ports. The MPOS-STD2 has an external USB port, but no external serial ports. Documentation describing the Secure ROM was provided and briefly reviewed, the use of ECDSA with SHA-256 and curve P-256 is seen to meet the cryptographic requirements of PTS.

The processor contains a JTAG module, which is wired to a connector on the upper face of the main board. JTAG is typically used during development to debug code and investigate error conditions. The data sheet states that JTAG is permanently disabled on production versions of the processor. JTAG enabled processors must be specifically ordered from the vendor.

Application / firmware separation (TA4.9)

No details on the software design were provided during this prestudy.

Digital signatures (TA4.10)

Digital signatures are used as part of the self-test and for authenticating firmware updates. These signatures use the ECDSA, using SHA-256 and curve P-256. This is compliant with PCI PTS requirements. Review of the processor documentation shows that the signature verification code is part of the boot ROM, with the public key stored in the on-chip OTP memory.

Physical protections (TA4.11)

The MAX32550 includes enough flash, SRAM, NVSRAM and OTP memory to operate without any external memory buses. The MPOS-STD2 includes a serial flash chip which can be used to store information outside the processor. The serial flash chip is contained within the secure section surrounded by tamper meshes. Sensitive information such as keys should be encrypted before storing in this location.

Memory encryption (TA4.12 & TA4.8)

Memory encryption is used by the processor to protect the sensitive data stored in the on-chip NVSRAM. The datasheet states that AES-256 is used in ECB mode to transparently encrypt/decrypt all sensitive data. Memory relocation cannot be used as an attack vector in this design as the NVSRAM bus cannot be easily accessed.

Protection of sensitive information stored in the discrete flash is controlled by the firmware, which is outside the scope of this prestudy.

Attacks for Sensitive Information (TA4.13)

In a typical software design all sensitive information is stored within the security processor. Any attack to retrieve or modify this information would require expert skill, chip level equipment and sensitive information. A brief attack calculation is provided below.

Identification stage of attack "S1"

1. Obtain a development kit for the processor and depackage a chip.
2. Develop test software for the processor and then setup a micro probe or FIB to set/retrieve the sensitive information.
3. Obtain a mechanical sample and devise a plan to access the processor
4. Practice the attack on a functional sample.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Expert	Sensitive	Standard	Standard		8 hours
2	Expert	Public	Chip-level	None		40 hours
3	Expert	Public	Standard	None	1 Mechanical	80 hours
4	Expert	Public	Chip-level	None	1 Functional	40 hours

Exploitation stage of attack "S1"

1. Using a functional sample disable the rear case tamper and remove the rear casing
2. Bypass the tamper mesh protecting the processor
3. Depackage the processor and probe the sensitive information

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Expert	Public	Standard	None	1 Functional w/keys	2 hours
2	Expert	Public	Standard	None		8 hours
3	Expert	Public	Chip-level	Standard		40 hours

Cost breakdown of attack "S1"

Identification Phase	Value	
Attack Time	5.5	> One hundred and sixty hours
Expertise	4	Expert
Knowledge	3	Sensitive
Access Costs	3	One mechanical and one functional sample without keys
Equipment required	3.5	Chip-level attacks (shared)
Specific Parts	1	Standard
Identification Total	**20.0**	

Exploitation Phase	Value	
Attack time	4	≤ Eighty hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	4	Functional sample with working keys and software
Equipment required	3.5	Chip-level attacks
Specific Parts	0	None
Exploitation Total	**15.5**	
Grand Total	**35.5**	

DTR A5 Monitoring During PIN Entry	Result:	Should be OK*
There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring—even with the cooperation of the device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation, as defined in Appendix B.		
Guidance *For A5 monitoring sound refers to other audible sounds apart from the beep generated by the device when a key is pressed.* *Monitoring is to be done outside of the protected area of the device (in most cases: outside the PIN entry device).* *Methods such as video monitoring and shoulder surfing are addressed in A8.*		
Tester(s): D. McGregor		

Vendor documentation (TA5.1 & TA5.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

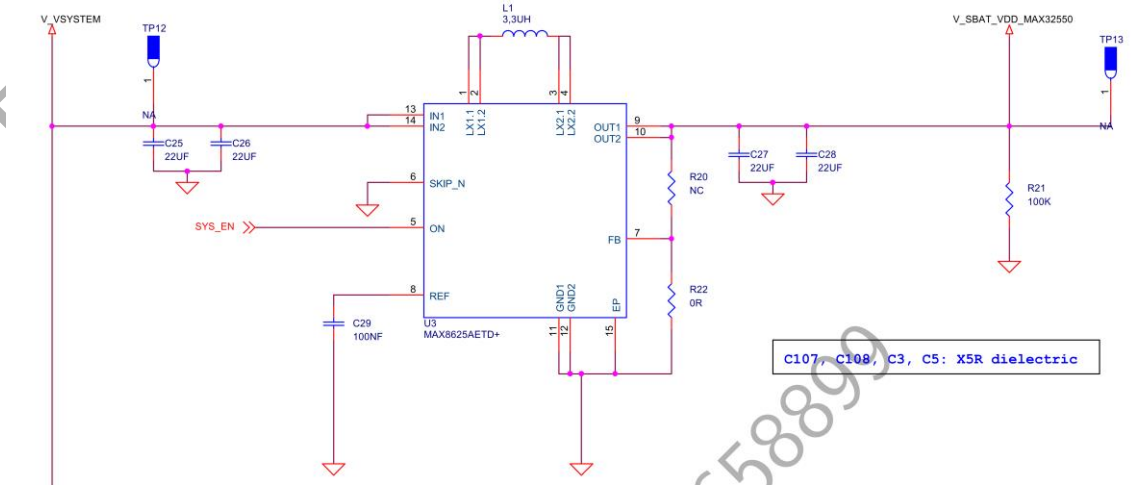
- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Power supply design (TA5.3)

The device is powered by a non-removable battery, with the USB port providing external power for charging the battery.

External power is passed through a MAX8625A step-up/down regulator before being used to power the processor and other circuitry.



The keypad is directly connected to port pins on the processor, which has a dedicated logic block designed for keypad scanning. This logic randomizes the scanning signals, complicating any power or EM emissions analysis.

Power leakage collection and analysis (TA5.4 & TA5.5)

The MPOS-STD2 supplied for evaluation did not have any firmware, therefore it was not possible to monitor power consumption during PIN entry. The use of an internal battery, switch mode regulator and low power scanning mechanism limits the leakage of keypad presses through the power consumption, and no problems are expected when this test is performed during a full evaluation.

EM emissions design (TA5.6)

The processor is located in the secure section, surrounded by tamper meshes. These meshes restrict the physical proximity to which a probe can be placed, and also help attenuate any EM emissions from the processor.

Traces connecting the keypad footings to the main processor are located in internal layers of the main board. EM emissions from these traces are attenuated by 2 layers of tamper mesh on all sides and the ground fill surrounding all keypad footings.

EM emissions collection and analysis (TA5.7 & TA5.8)

The low current in the monitoring circuits, randomized scanning algorithm and interference from other electronic components limit the EM emissions from the keypad. No testing was performed during this prestudy, however no leakage issues are expected due to the design of the device.

Mechanical sounds (TA5.9)

Numeric keys on the device are constructed with metal dome switches, which make a slight click when pressed. The low volume clicks are easily drowned out by any background noise, complicating any audio processing.

The evaluator held the keypad near his ear and pressed the different buttons on the keypad. Key clicks were all found to have a similar volume and tone, and no other characteristics were found which could enable PIN recovery.

Attacks for PINs through emissions (TA5.10)

No feasible attack vectors using emissions were found during this prestudy. Further testing would be performed during a full evaluation, however no issues are likely to be found.

DTR A6 Determining Keys Analysis	Result:	Should be OK*
Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation, as defined in Appendix B.		
Guidance *Keys resident in the device or its components means plaintext secret or private keys. If the encrypted keys are protected in accordance with the minimum key sizes and parameters for the key-encipherment algorithm(s) used as stipulated in Appendix D, they do not need to be considered.* *The vendor shall provide mechanisms to facilitate side-channel testing. These mechanisms shall include at least the following: an interface, the ability to vary data and keys, and the ability to set trigger points (for testing purposes only and not for production units).*		
Tester(s): D. McGregor		

Vendor documentation (TA6.1 & TA6.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Security processor (TA6.3)

The MPOS-STD2 uses the MAX32550 processor, which is designed for security sensitive applications such as payment terminals. This processor is soldered to the lower face of the main board, protected by tamper meshes in the main board and smartcard security film.

Cryptographic key storage and processing (TA6.4)

The MAX32550 processor contains the following memory and processing features.

- ARM Cortex M3 core
- 1MB Flash memory
- 256KB SRAM
- 8KB Self-encrypting NVSRAM
- 4KB User programmable OTP
- 256 bit Battery Backup AES Key Storage

A single plaintext key is stored in the AES key storage register, which is battery backed and erased upon detection of a tamper event. All other keys and sensitive data is stored in the NVSRAM, automatically encrypted under the AES key, and is therefore unrecoverable in the event of a tamper event.

All plaintext keys are processed in the ARM core, which is physically protected by the chip package and meshes in the surrounding tamper meshes.

No firmware was provided for this prestudy, but it is assumed that keys and other sensitive data is stored in the processor in the designated memory.

Security processor protections (TA6.5)

The MAX32550 processor has specific security design features. For details see the prestudy report on this processor.

Cryptographic operations and side channel (TA6.6 – TA6.9)

The processor contains cryptographic accelerators for AES, TDES, SHA and modular arithmetic. The use of these accelerators is controlled by the firmware which is out of scope of this prestudy. Side channel leakage of the accelerators is addressed in the chip prestudy.

Glitching (TA6.10)

The processor datasheet indicates a voltage glitch sensor is present. For testing and further information consult the chip prestudy.

Physical protection (TA6.11)

The processor datasheet indicates a die shield is present. For testing and further information consult the chip prestudy.

Published vulnerabilities in the security components (TA6.12)

The device uses the MAX32550 as the exclusive processing element. This requirement is addressed in the chip prestudy.

Plaintext keys in external memory (TA6.13)

The MAX32550 contains on-chip code and data memory and does not need external memory. Sensitive data stored in the external flash should be encrypted with a key stored in the internal memory.

Comparison to A4 (TA6.15)

DTR A4 included a chip level attack to retrieve sensitive information. This attack exceeded the 35 point minimum for this requirement.

Attacks for Cryptographic Keys (TA6.14)

Physical probing of cryptographic keys was considered in A4 and found to meet the minimum difficulty level. Vulnerability to side channel and glitch attacks will depend upon the firmware and chip details, which are outside the scope of this prestudy.

DTR A7 Physical Security of Display Prompts	Result:	Firmware dependent*
The unauthorized alteration of prompts for non-PIN data entry into the PIN entry keypad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation, as defined in Appendix B.		
Guidance *A7 is applicable to a device that contains a display and may output non-PIN data.* *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit. B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer. E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *"Non-PIN data" refers to numeric data other than the PIN that is entered via the keypad.* *Audio prompts must be considered if applicable.*		
Tester(s): D. McGregor		

Vendor documentation (TA7.1 & TA7.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with the physical samples.

Non-PIN data handling (TA7.3)

Software for the MPOS-STD2 was not provided for this prestudy. It is assumed that the software may allow for non-PIN keypad output, therefore this requirement is in scope.

Control of the display (TA7.4)

The LCD is located underneath the upper casing. A lens is glued to the top of the upper casing. Testing confirmed it was feasible to remove this lens without damaging or tampering the device.

The MPOS-STD2 contains a 50mm x 35mm graphic color TFT display. The display is connected to the main board with a flexible ribbon cable sandwiched between the display and main board.

Figure 22: Top view of device with lens removed

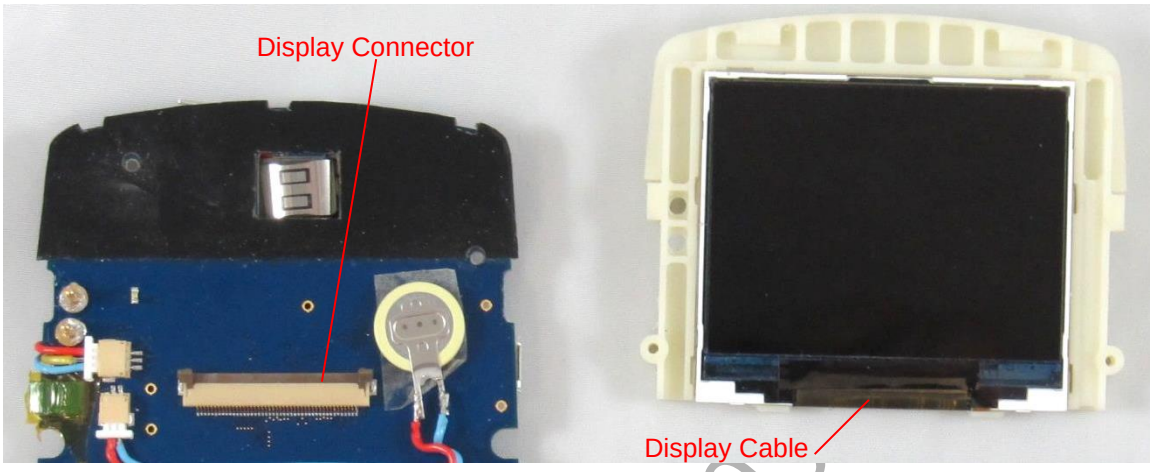


Figure 23: Top view of main board and display assembly.

Protection Mechanisms (TA7.5)

The device does not contain any specific protection mechanisms for the LCD and cable. The LCD is enclosed by the lens, upper casing and main board. Penetration through the rear to the LCD is prevented by the MSR mesh.

The cable between the LCD and main board is routed in the narrow gap between the LCD and main board.

Prompt storage (TA7.6)

The processor contains internal memory which is used for code and data storage. This internal memory is physically protected and cannot be easily modified. The device includes discrete flash memory which is also within the secure section surrounded by tamper meshes.

Attacks for Changing Prompts (TA7.7)

A number of attacks for changing prompts were considered as follows

Rear attack

A rear attack would require the disabling of the either the MSR foil or removal of the battery. The meshes in the foil and the tamper switch under the battery complicate any attack through the rear.

Side attack

Probing the cable could be achieved through the side of the device, however it is complicated by the narrow gap and the large number of signals which have to be tapped. A complete attack would have to locate a space to insert a bug and to repair the casing damage.

Frontal attack

The most feasible attack is to remove the lens and cut the upper casing surrounding the LCD. The LCD could then be removed through the front and the cable disconnected. A custom bug could then be inserted into the cable and the LCD and lens replaced.

This attack is unlikely to meet the 18 point minimum score for this requirement. For this device to pass PTS the firmware must not allow for the output of non PIN data.

DTR A8 Visual Observation Deterrents	Result:	VERIFIED*
The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.		
Guidance *Some markets may require Option A.1.1 or A1.2 of Appendix A or a stricter criterion.* *The vendor shall provide a privacy shield providing protections as described in Appendix A of this document. Alternatively, the vendor may use less restrictive privacy-shield criteria provided that the vendor supplies rules and guidance as to how the visual observation is to be deterred by the environment in which the device is installed. These rules shall be binding for the organization placing the device into the environment—for example, the acquirer or merchant. If the vendor gives rules for an external physical privacy shield, the vendor shall provide a demo/sample with the appropriate dimensions. The user (acquirer or merchant) instructions provided by the vendor shall clearly state that the acquirer or merchant must either meet the implementation criteria or deploy devices meeting the criteria defined in Appendix A, Section A1.1 or A1.2.* *If the means to deter visual observation are not an integral part of the PIN entry device, the vendor shall specify by appropriate means (for example, drawings and description) how the visual observation is deterred by the structure or piece of equipment housing the device. These specifications shall be binding for the vendor.*		
Tester(s): D. McGregor		

Vendor documentation (TA8.1 & TA8.2)

No vendor questionnaire or other relevant vendor documentation was provided for this prestudy.

Wireless characteristics (TA8.4)

The MPOS-STD2 is powered by an internal lithium battery, and contains a Bluetooth communications module.

Handheld documentation (TA8.5 & TA8.6)

No relevant documentation was supplied.

Privacy shield (TA8.7)

The device is not provided with a privacy shield, and has no attachment points.

Mounting (TA8.8)

The rear case of the device is formed from a smooth plastic part. No screw points or other mounting fixtures are provided.

Device characteristics (TA8.9)

Dimension	Device Measurement	Maximum for classification as handheld
The width at the ‘5’ key	7.5cm	7.6cm
The height at the ‘5’ key	1.9cm	
The sum of the width and height at the ‘5’ key	9.4cm	10.2cm
The keypad length, from the bottom of the ‘0’ key to the top of the ‘2’ key	4.5cm	10.2cm
The weight of the POI	130grams + battery	500grams

The characteristics of the MPOS-STD2 meet the definition of a handheld device.

Handheld classification (TA8.10)

The form factor, wireless operation and vendor instruction are all consistent with a classification as a hand held device.

Privacy Shield (TA8.11)

The device is designed to be handheld, and no privacy shield is provided nor required.

Operating Environment (TA8.12)

The device is designed to be handheld, and no operating environment guidance is provided nor required.

DTR A9 Magnetic-Stripe Reader	Result:	VERIFIED*

It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation, as defined in Appendix B.

Guidance

Skimming is the unauthorized capture and transfer of payment data to another source, for fraudulent purposes.

Countermeasures include, for instance, active detection of skimmers, active disturbance of the skimming process. The protection of the reader may consist of resistance of the device cabinet/the reader enclosure against manipulation.

Skimming attacks to recover payment card data may occur via either the attachment of external devices or attacking other areas (hardware or software) of the device. Both must be considered for this requirement.

Access to the inside of the device for routine maintenance (for example, replenishing paper) shall not allow access to clear-text account data, for example, by making cabling which transmits the data physically inaccessible to routine maintenance personnel or encrypting the sensitive card data transmitted internally within the device between components.

Tester(s): D. McGregor

Vendor documentation (TA9.1 & TA9.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts
- Schematics

These documents were found to be consistent with the physical samples.

Magnetic stripe data overview (TA9.3)

The MPOS-STD2 includes a magnetic stripe reader within the casing of the device. The device does not accept magnetic stripe data from external sources.

Magnetic stripe reader location and operation (TA9.4)

Magnetic stripe cards are swiped through a channel at the top end of the device. An MSR head is inserted from behind the main board, with the magnetic reader facing the display.
An FPC cable is soldered to the rear of the MSR head, and terminates in a connector on the underside of the main board. The rear of the MSR head, FPC and connector are covered by a flexible circuit with embedded tamper mesh.

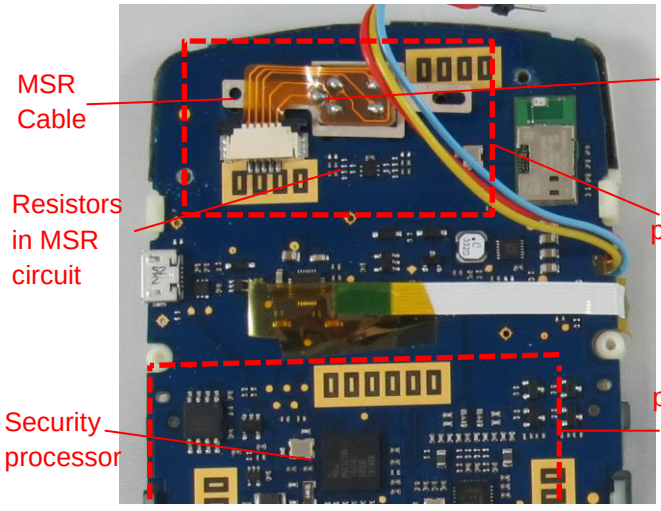


Figure 24: Underside of main board with rear case and MSR mesh removed

Path from MSR head to security processor (TA9.5)

Magnetic stripe data is present on the traces between the MSR head and security processor. The first segment of this path is from the head to the connector, which is physically protected by the MSR flexible mesh and main board mesh.

The second segment is from the connector to the discrete resistors and ESD protector chip. These traces and components are located in the secure section as the MSR head.

The final segment from the intermediate components to the security processor is through traces on layer 4 of the main board.

Logical protections (TA9.6)

Physical mechanisms are used to protect MSR data, no logical protections are used.

Physical protections (TA9.7)

Protection to the traces carrying MSR data is provided by the MSR mesh, ICC mesh and main board mesh. Details on these meshes have been addressed in DTR A1.

The MSR mesh and ICC mesh are both constructed from two layer film printed with conductive ink. The Main board has meshes on layer 3 and 5, which provides a single layer of 6mil mesh from the front or rear.

Secondary read head (TA9.8)

The read head is located in a hole in the main board, protruding 2mm above the board. A 1mm plastic guide surrounds the read head and prevents payment cards rubbing against the PCB. Adding a secondary read head would require making a hole in this board, or an extremely thin read head (~1mm).

Attacks for MSR data (TA9.9)

A number of attacks were considered during the evaluation as listed below

- Bugging the read head
- Tapping the signals on the path
- Accessing the components handling MSR data
- Insertion of a secondary read head.

The most feasible attack found was to access the trace carrying the data between the two secure sections. This attack is costed below.

Identification stage of attack "M1"

1. Obtain a mechanical sample and disassemble to understand the protection mechanisms and paths of the MSR data.
2. Devise a plan to attack the device and recover MSR data.
3. Practice on a functional sample.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Proficient	Public	Standard	None	1 Mechanical	8 hours
2	Proficient	Public	Standard	None		20 hours
3	Proficient	Public	Standard	Standard	1 Functional without keys	10 hours

Exploitation stage of attack "M1"

1. Obtain a functional sample and cut an access hole in the rear casing. Carefully probe and disable the tamper switch located under the battery. Remove the rear casing and battery.
2. Carefully abrade through the battery holder and main board to expose the MSR signals in layer 4 of the main board. Connect wires to these traces and wire up to a F2F decoder and bug.
3. Store the small bug in a space in the rear of the device. Replace the rear casing and return to service.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Proficient	Public	Standard	None	1 Functional with keys	1 hour
2	Proficient	Public	Standard	Standard		3 hours
3	Proficient	Public	Standard	Standard		½ hour

Cost breakdown of attack "M1"

Identification Phase	Value	
Attack Time	3.5	≤ Forty hours
Expertise	1.5	Proficient
Knowledge	0	Public
Access Costs	3	One mechanical and one functional sample without keys
Equipment required	0	None (re-used during exploitation)
Specific Parts	1	Standard
Identification Total	**9.0**	

Exploitation Phase	Value	
Attack time	2	≤ Eight hours
Expertise	1.5	Proficient
Knowledge	0	Public
Access Costs	4	Functional sample with working keys and software
Equipment required	1	Standard
Specific Parts	1	Standard
Exploitation Total	**9.5**	
Grand Total	**18.5**	

DTR A10 Component Protections against Removal	Result:	N/A

Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation, as defined in Appendix B.

Guidance

The objective of this requirement is to assess the device's ability to protect the component against removal from its frame or the cabinet. This protections aims against component device overlays or chained ICC readers; it also aims at complicating attacks against the component wherein it is taken away by attackers in order to perform subsequent attack steps under controlled conditions.

Installation or removal of the device requires an authorized process. An authorized installation must provide traceability and accountability (what happened, when, and who did it).

If all components are integrated into a single tamper envelope, then removal detection at the component level is not necessary and removal detection will be addressed in the Integration section for the final form factor, for example, AFD.

Protection against removal may be implemented as detection of removal and procedures for authorized installation or re-installation. The procedures must:

- *Use dual-control techniques;*
- *Provide accountability and traceability including logging of user IDs, date and time stamp, and actions performed;*
- *Prevent replay of authorization data; and*
- *Cause the device to not process PIN data until authorized to do so.*

Tester(s): D. McGregor

Vendor documentation (TA10.1, TA10.2 & TA10.3)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts
- Schematics

These documents were found to be consistent with the physical samples.

Unattended classification (TA10.5 & TA10.6)

The vendor has designed the device to be used handheld, which is consistent with the finding in DTR A8. A handheld device is always attended, and no removal sensors are required or provided.

DTR A11 Audible Tones During PIN Entry	Result:	Not evaluated
If the PIN entry is accompanied by audible tones, then the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.		
Tester(s): D. McGregor		

Vendor documentation (TA11.1 & TA11.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts
- Schematics

These documents were found to be consistent with the physical samples.

Design (TA11.3)

Review of the schematics did not show any buzzer, speaker or other audible tone generator.

Testing (TA11.4)

No software was provided during this evaluation therefore no analysis could be done of any feedback mechanisms.

4.2 Offline PIN Requirements

DTR D1 Penetration Protection	Result:	VERIFIED*
It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, as defined in Appendix B, nor is it possible for both an ICC card and any other foreign object to reside within the card-insertion slot. ***Note: All attacks shall include a minimum of ten hours attack time for Exploitation.***		
Guidance *The card reader may consist of areas of different protection levels, for example, the areas of the ICC card interface itself, and the area holding retracted cards.* *In addition to the specified minimum attack potential values, any feasible penetration attack against the ICCR for the purpose of determining or modifying sensitive data must entail at least ten hours of exploitation time.* *The ICC reader may be equipped with mechanical and/or optical mechanisms to meet this requirement when used in conjunction with the implementation guidance.* *Implementation guidance is provided to facilitate detection of shim devices by the entities (for example, merchants) deploying these devices.* *A PIN-disclosing bug shall be prevented from being inserted into the device through the card slot. The volume of space accessible via the card slot that could be utilized by an attacker can vary with the geometry of the space and attack methods. For this reason, the requirement does not prohibit a specific volume. Rather, the feasibility of effective bug placement is to be considered when assessing D1 compliance. Examples of these considerations are:* • *Contact points must be present for the bug to connect to;* • *The bug and wires must not obstruct normal operation;* • *The placement of the bug must not cause tamper evidence that would be noticed by a typical cardholder.* *Space accessible via the IC card slot large enough to conceal a PIN-disclosing bug is not allowed. There must not be space accessible via the card slot large enough to conceal an IC card chip and small battery.*		
Tester(s): D. McGregor		

Vendor documentation (TD1.1 & TD1.2)

No vendor questionnaire was provided for this prestudy.

Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts
- Schematics

These documents were found to be consistent with the physical samples.

Protection mechanisms (TD1.3)

Protection of the ICC reader and I/O signal is provided by the ICC mesh and keypad. Examination of the device confirmed that these protection mechanisms exist.

Implementation guidance (TD1.4)

No security policy was provided for this prestudy, during a complete evaluation the security policy must at a minimum contain guidance for a merchant or operator to periodically check the slot for bugs.

Slot dimensions (TD1.5)

Space for an ICC bug is limited by the slot size is the upper housing and the internal spaces within the ICC acceptor.

Dimensions of the slot were made and tabled below.

IC slot width	54mm
IC slot height (in the embossing area)	1.2mm
IC slot height (in the non-embossing area)	1.2mm
IC slot height (in the acceptor)	1.8mm
IC slot depth	54mm

The acceptor is constructed from a 1mm plastic base, covered with a sheet steel top. No significant spaces exist within the acceptor.

Slot enlargement (TD1.6)

The ICC acceptor is surrounded by the flexible mesh which is held against the main board by a plastic cover. Forcing the mesh up would release the pressure on the side elastomeric strips, triggering a tamper event. The acceptor is constructed from 1 mm thick plastic and 0.2mm steel, which do not allow much space for slot enlargement.

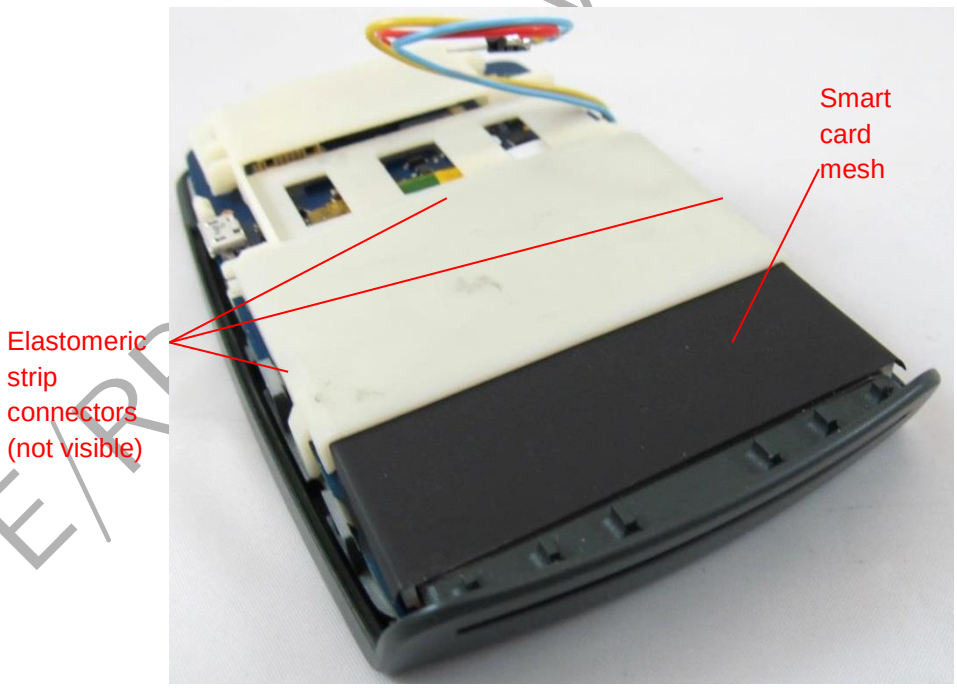


Figure 25: Underside view with rear casing and battery removed.

Two card test (TD1.7)

The tester attempted to insert two unembossed cards into the slot. The slot height prevented the insertion of two cards.

ICC acceptor and location (TD1.8 & TD1.9)

The ICC acceptor is located at the cardholder end of the main board as shown below. The acceptor is a C&K Components CCM01-Mk5-2523.

Figure 26: ICC slot

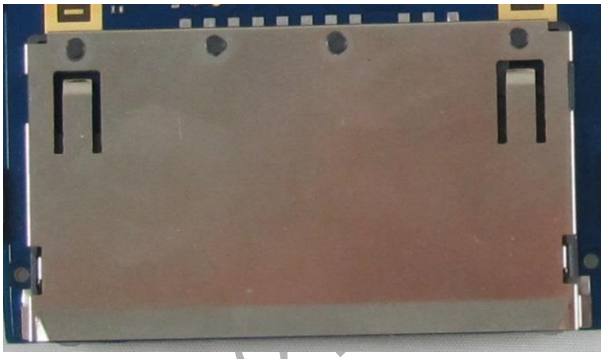


Figure 27: ICC acceptor

Active bug detection (TD1.10)

The device does not include any active bug detection mechanisms. Documentation for periodic manual checking of the slot is assessed in TD1.4.

Spaces within the acceptor (TD1.11)

A picture of the acceptor was provided in Figure 27, which shows the metal covering the top of the acceptor. The bottom of the acceptor is made from 1mm plastic. The largest space in this plastic is found to be 3mm x 5mm x 1mm, which is smaller than the maximum space in the requirements of 10mm x 10mm x 5mm.

Path between ICC reader and security processor (TD1.12 & TD1.13)

Pictures showing the path of the I/O signals and involved components are shown below

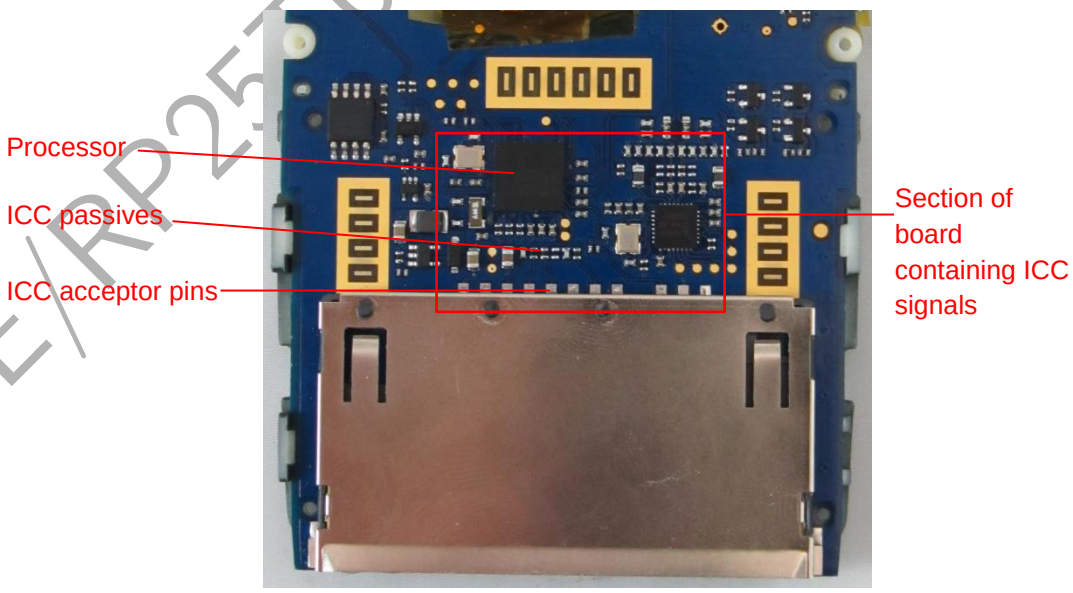


Figure 28: View of the Path from ICC acceptor to security processor

I/O signals are routed through layers 6 and 7 of the main board, within the area bounded by the rectangle in Figure 28.

Tamper detection mechanisms protecting the path (TD1.14 & TD1.17)

The path of the I/O signal was confirmed to be full contained within the secure section as described in DTR A1. This section is surrounded by tamper meshes in the main board (layer 2&3) and ICC flex (layers 1 &2).

Probing of any ICC related signals and components without disabling the tamper detection mechanisms were found to be infeasible from any angle except through the slot.

Unprotected I/O signals (TD1.15)

Review of the vias, components and traces which handle I/O data confirmed that they are protected by the tamper detection mechanisms described above and in DTR A1.

Passive resistors and capacitors attached to the I/O line are located on bottom face of the PCBA board. The other end of the capacitor was confirmed to be soldered to the ground plane which surrounds all components on the bottom layer. No method to access and disconnect the grounded end of the capacitor was found.

Tamper meshes (TD1.16)

ICC I/O signals are protected by meshes in the main board and smart card security flex. For details on these meshes refer to DTR A1.

Tamper response (TD1.18)

Mechanisms protecting the I/O signal are connected to the same tamper response circuitry as used for keypad signals. For details on the tamper response see TA1.23 - TA.25

Attack "I1" for Offline PINs (TD1.19)

Identification stage of attack "I1"

1. Disassemble a mechanical sample to understand the devices design and tamper detection mechanisms. Significant time is estimated to reverse engineer the mesh layouts and circuit diagrams.
2. Devise a plan to tap the ICC signal and customise a bug to record the ICC signals.
3. Practice the attack on a functional sample.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Expert	Public	Standard	None	1 Mechanical	40 hours
2	Expert	Public	Standard	Standard		40 hours
3	Expert	Public	Standard	None	1 Functional	20 hours

Exploitation stage of attack "I1"

1. Obtain a functional sample with keys and make a hole in the rear casing. Use ink or glue to disable the tamper switch under the battery and remove the rear casing.
2. Abrade through the plastic former and expose the traces in the smart card mesh. Disable and repeat on the second layer of traces. Disabling 6mil tamper meshes in a flex circuit is difficult, and 8 hours of expert skill is estimated.
3. Create a hole in the disabled flex mesh and probe the I/O signal from the smart card. Wire up to a bug and replace the rear casing.

Step	Expertise	Knowledge	Equipment	Parts	Samples	Time
1	Proficient	Public	Standard	None	1 Functional with keys	1 hour
2	Expert	Public	Standard	Standard		8 hours
3	Proficient	Public	Standard	None		1 hour

Cost breakdown of attack "I1"

Identification Phase	Value	
Attack Time	5	≤ One hundred and sixty hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	3	One mechanical and one functional sample without keys
Equipment required	0	None (re-used during exploitation)
Specific Parts	1	Standard
Identification Total	**13.0**	

Exploitation Phase	Value	
Attack time	3	≤ Twenty four hours
Expertise	4	Expert
Knowledge	0	Public
Access Costs	4	Functional sample with working keys and software
Equipment required	1	Standard
Specific Parts	1	Standard
Exploitation Total	**13.0**	
Grand Total	**26.0**	

DTR D2 ICC Reader Slot Visibility	Result:	VERIFIED*
The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.		
Tester(s): D. McGregor		

Vendor documentation (TD2.1)

No vendor questionnaire was provided for this prestudy.

Customers view of IC card reader slot (TD2.2 &TD2.3)

Customers would be handed the device to insert their IC card into. The ICC slot is formed at the end near the '0' key as shown in the picture below. The slot is clearly viewable to the cardholder, and any suspicious objects at the opening would be detectable.

Figure 29

DTR D3 ICC Reader Construction (Wires)	Result:	VERIFIED*
The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.		
Tester(s): D. McGregor		

Vendor documentation (TD3.1)

No vendor questionnaire was provided for this prestudy.

Construction of IC card slot (TD3.2 & TD3.3)

The IC card reader slot is formed in the upper casing half. The part line between the upper and lower casing halves is on the sides and bottom of the device (not visible in the picture below).

A wire emerging from the ICC slot would be exposed for approximately 5mm, which can be easily observed by the cardholder.

Figure 30: End view of slot

Add-on parts (TD3.4)

There are no removable parts which could be used to hide a bug.

Internal construction (TD3.4)

The ICC acceptor is located immediately behind the slot in the upper plastic housing as shown in the picture on the right.

No significant gaps are present which may allow for the threading of a wire between the acceptor and slot into the internal space within the device. In addition there are no unprotected openings (SAM bay etc) which could be used to hide a bug.

Figure 31: View of slot with rear casing removed

Conclusion (TD3.5)

Wires exiting from the slot in the upper plastic housing are likely to be highly visible to a cardholder. Pushing a wire between the slot and acceptor to a bug is difficult due to the narrow gap and the lack of an accessible storage place for the bug.

Removal of the rear casing would allow for the routing of a wire between the slot and acceptor, however a tamper switch near the battery prevents this. It is possible to remove the upper case housing without triggering a tamper event, however the largest available space is only 2mm x 2mm x 15mm which is not of sufficient size to store a bug.

5 Module 4: Secure Reading and Exchange of Data

5.1 Account Data Protection Requirements

DTR K1 Account Data Processing	**Result:**	**VERIFIED***
All account data is either encrypted immediately upon entry or entered in clear-text into the device and processed within the secure controller of the device.		
Guidance *The objective of this requirement is to ensure that all account data is handled in a secure manner. The requirement allows for the encryption of account data directly at the read head or for account data to be submitted to the device in clear-text form. This data is then communicated to a secure controller where it is processed.* *The term "processed" is used as a generic term, which includes but is not limited to account-data encryption and the selective disclosure of clear-text account data by the secure controller to authenticated applications (per K15.1).*		
Tester(s): D. McGregor		

Vendor documentation (TK1.1 & TK1.2)

No vendor questionnaire was provided for this prestudy. Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with physical sample provided.

Account Data Entry and Protection Mechanisms (TK1.3)

Documentation review, physical examination and testing were used to determine all paths taken by account data. These, together with the protection methods have been tabulated below.

Account data path	**Protection Method**
MSR to security processor	Tamper meshes and switches
Contact ICC reader to security processor	Tamper meshes
Contactless ICC controller to security processor	Tamper meshes
Keypad to security processor	Tamper meshes and switches

DTR K1.1 Account Data Protection	Result:	VERIFIED*
The device protects all account data upon entry (consistent with A9 for magnetic-stripe data and D1 for chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation. ***Note that MSRs and ICCRs must meet the attack potentials stipulated in DTRs A9 and D1 respectively.***		
Guidance *All methods of card-data entry supported by the device must be assessed. This includes both contactless and any manual PAN-entry modes that are natively supported by the SRED firmware. The path for contactless data must be secured to 16 points from the point of digitization of this data.* *All methods of access to the card data should be considered, including emanations (except for contactless).*		
Tester(s): D. McGregor		

Vendor documentation (TK1.1.1 & TK1.1.3)

No vendor questionnaire was provided for this prestudy. Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with physical sample provided.

Related core requirements (TK1.1.2)

The MPOS-STD2 contains a manual PAN entry keypad, magnetic stripe reader and an ICC reader. Security of the keypad, readers and paths to the security processor has been addressed earlier in this report. For details see DTR A1 (keypad), DTR A9 (MSR) and DTR D1 (ICCR).

Protection mechanisms (TK1.1.4)

The MPOS-STD2 supports contactless cards. An antenna surrounds the LCD which is connected to digitizer located in the secure section. The NXP CLRC663 chip is connected to the main processor with a serial peripheral interface (SPI) bus.

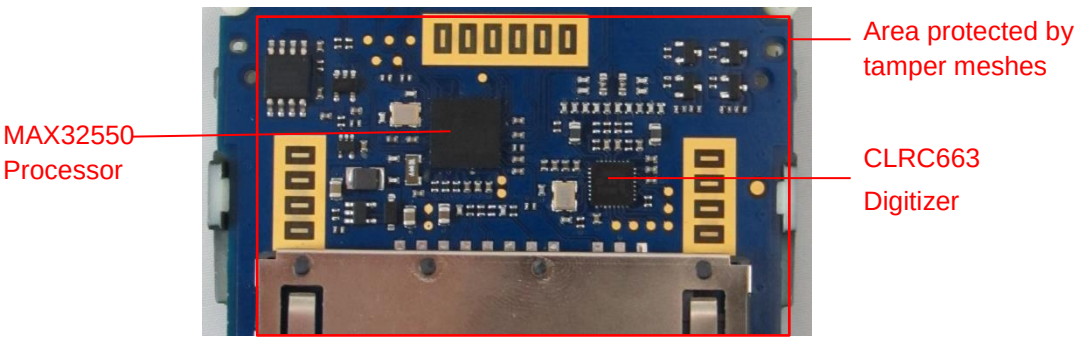


Figure 32: Lower face of main board showing main processor and contactless controller

Tamper meshes in the main board and smart card security film surrounded the processor, digitizer and interconnect traces.

Attack scenario (TK1.1.5)

Attacks to recover manual PANs, magnetic stripe data and ICC information have been addressed in DTR A1, A8 and D1 earlier in this report. Digital contactless information is processed exclusively within the secure section protected by tamper meshes. Disabling or bypassing these meshes was considered in DTR A1/D1 and found to exceed 26 points of difficulty.

DTR K1.2 Independent Security Mechanisms	Result:	VERIFIED*
Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.		
Guidance *In general, techniques may include any combination of tamper-detection methods. Security mechanisms must not rely on insecure services or characteristics provided by the device such as (but not limited to) its power supply and unprotected wires. Tamper-evident labels and similar methods involving tamper evidence are not considered a security mechanism.* *This requirement does not imply the need for redundant security mechanisms, but rather separate mechanisms of a different nature.*		
Tester(s): D. McGregor		

Vendor documentation (TK1.2.1 & TK1.2.2)

No vendor questionnaire was provided for this prestudy. Supporting documentation used during the evaluation of this requirement is listed below.

- PCB Layouts [1]
- Schematics [2]
- Hardware Design Guide [3]

These documents were found to be consistent with physical sample provided.

Independent Security Mechanisms (TK1.2.3 & TK1.2.4)

Account data is protected by the same mechanisms used to protect PIN data, therefore this requirement has been addressed in DTR A2. For further details refer to DTR A2 earlier in this report.