Crypto Contactless Reader

User Guide

Address: Unit 7 Vitrage Technical Park, 27 Witney Road,
Poole, Dorset, BH17 0GL
Phone: +44 1202 666 700
Email: info@gemini2k.com

Version

Version	Description	Author	Date
1	Document created	S.Urumov su@gemini2k.com	04/05/2018
1.1	Layout updated	Julian Moskov jm@gemini2k.com	29/08/2018
1.2	Added mechanical specs, software integration, installation sections	Julian Moskov	26/11/2018
1.3	Storage instructions and battery details	Julian Moskov	3/12/2018
1.4	Operational management details added	Julian Moskov	7/01/2019
1.5	Label corrections	Julian Moskov	18/01/2019
1.6	Inspection guidance	Julian Moskov	21/01/2019
1.7	Label information updated	Julian Moskov	07/02/2019
1.8	Connector details added	Julian Moskov	26/02/2019
1.9	Overview added	Konstantin Chterev	12/03/2019
1.9.1	Tamper response updated	Stefko Urumov	27/03/2019

1. Overview

Crypto is an advanced payments module based on an NXP secure microcontroller running embedded Real Time OS.

Its EMV functionality - Entry Point, Kernels, Key Management and Configurations - is part of the reader's certified firmware. All other closed loop schemes like ITSO, Calypso etc. are executed on the host computer via a Pass-Through Mode, which is enabled by default. In fact, the host terminal is completely outside of the PCI PTS scope, which makes the PCI DSS and P2PE schemes easier to certify.

The design of the platform makes it lightweight and flexible, while providing high security and transaction speed. The reader incorporates a crypto engine and secure key storage as required by PCI PTS and is certified to PCI PTS POI v5.1.

The Crypto firmware consists of a Command Execution Engine, Firewall, Entry Point and EMV Kernels, Contactless and Contact Cards interfaces. Various I/O are available – UART, RS232, USB, SPI, LCD etc.

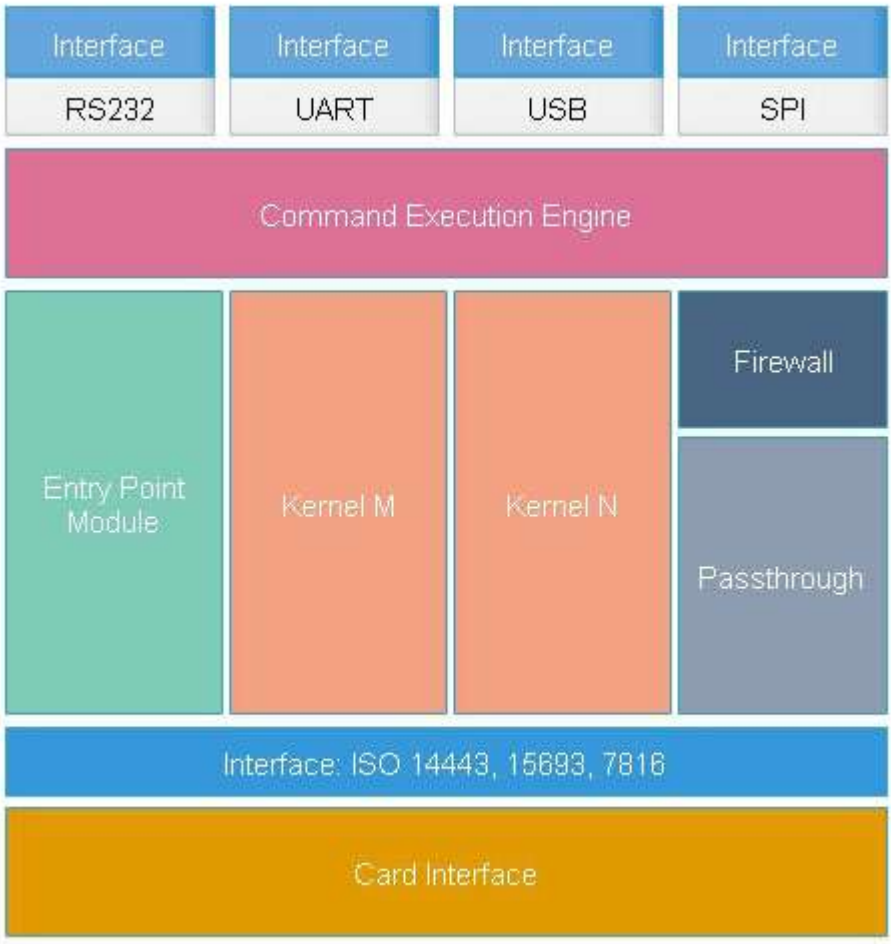
The main advantage of Crypto is the clear split between open and closed loop applications. Crypto does not allow arbitrary code to run in the firmware, thus simplifying the security requirements. The Firewall protects the cardholder data and the associated keys from unauthorised access by closed loop applications. As the host computer is usually a high-performance device (e.g. ARM 7/9, multicore, 1GHz and above), all non EMV applications that run on it benefit from the powerful processor, compared to an all-in-one reader.

Another advantage of Crypto is the dramatically reduced shut-down/power-on times. As there is no file system or OS services to support, the reader can be shutdown instantly at any point without corruption of keys, configurations, etc.

Crypto has capabilities for remote key management as well as remote firmware updates if necessary. The NFC front end is firmware upgradeable so new EMV Level 1 and 2 requirements can be fixed on the spot.

2. System Components

The interfaces and firmware modules that are included with the Crypto reader are outline below. Communication flows can be represented as vertical movement on the chart.



3. Specifications

Physical Specifications

Dimensions	70 x 75 x 20 mm (OEM module)
Weight Approx.	40 g (OEM module)
Status Indicators	Beeper 4 LED indicators 1 health-check LED

Contactless Smart Card Interface

Operating Frequency	13.56 MHz
Chipset	Kinetis K81
Communication Standards	NFC ISO/IEC 18092, ISO/IEC 14443 (Type A & B)
Card Reading Distance	Up to 70mm
Transmission Speed	Up to 848Kbps

Contact Interfaces

Card Slots	One SAM card slot, One MicroSD card slot

Connectivity

Host Interface	RS232, RS485 Serial UART, Slave SPI, USB CDC

Power Supply	5V DC, 7.5-12V DC, USB power supply
Current Consumption	350mA@5V

Security

PCI PTS v5.1 certified
Cryptography: DES/3DES, AES, RSA, SHA-1, SHA-256
Physical Security: Tamper protection

EMV Certification

EMV Level 1
EMV Level 2 Visa and Mastercard
TQM Label

Application Interface

Supported APIs	G2K API Crypto Interface API

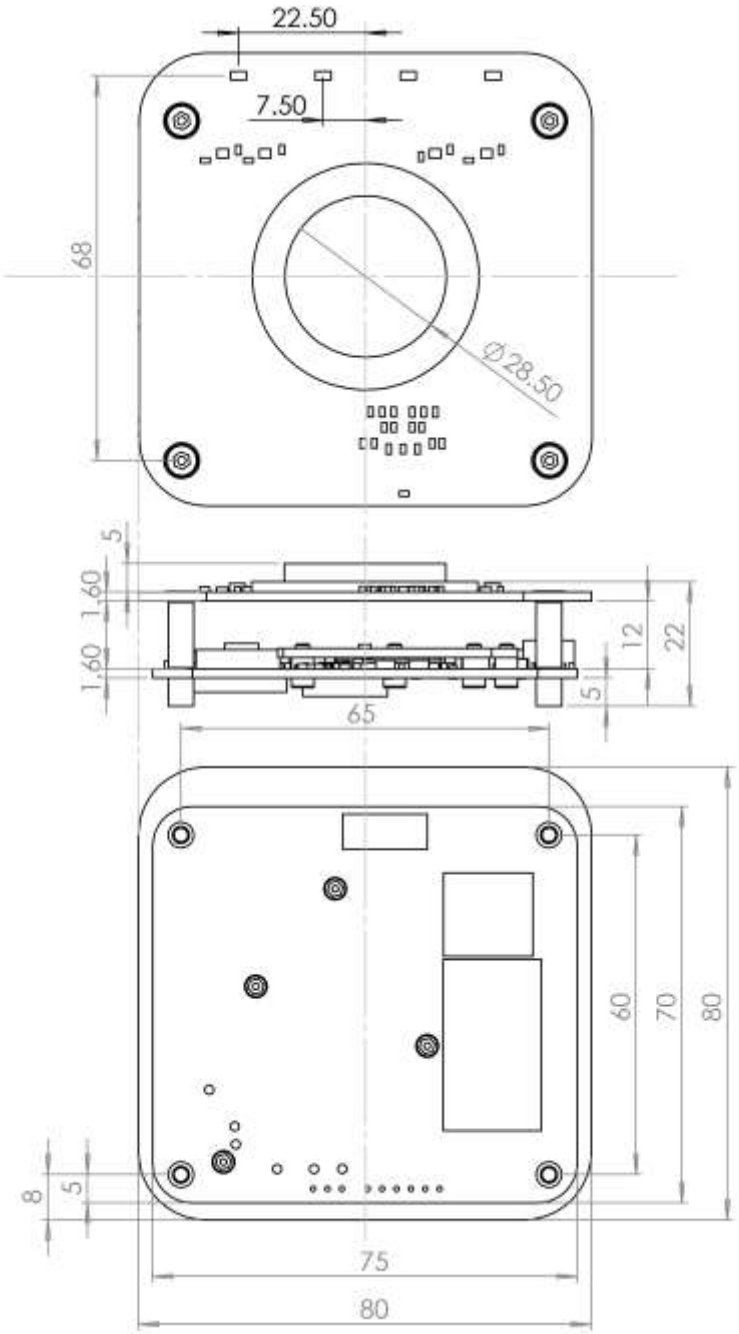
Operating Conditions

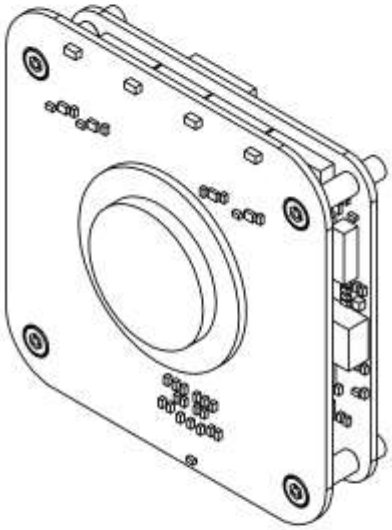
Operating Temperature	-20 to +80 °C
Non-Operating Temperature	-40 to +85 °C
Operating Humidity	0–95% non-condensing
MTBF	500,000 hours

1. Mechanical Specifications

The Crypto reader consist of two PCBs, a main board and an antenna board, held together with spacers. The assembly's dimensions are indicated below.

The NFC antenna plane button, measuring 28.5mm in diameter and 3mm in height, is positioned in the centre of the antenna to ensure correct fitting of the reader into a third-party enclosure. That enclosure therefore requires a 3mm thick non-metal front cover.

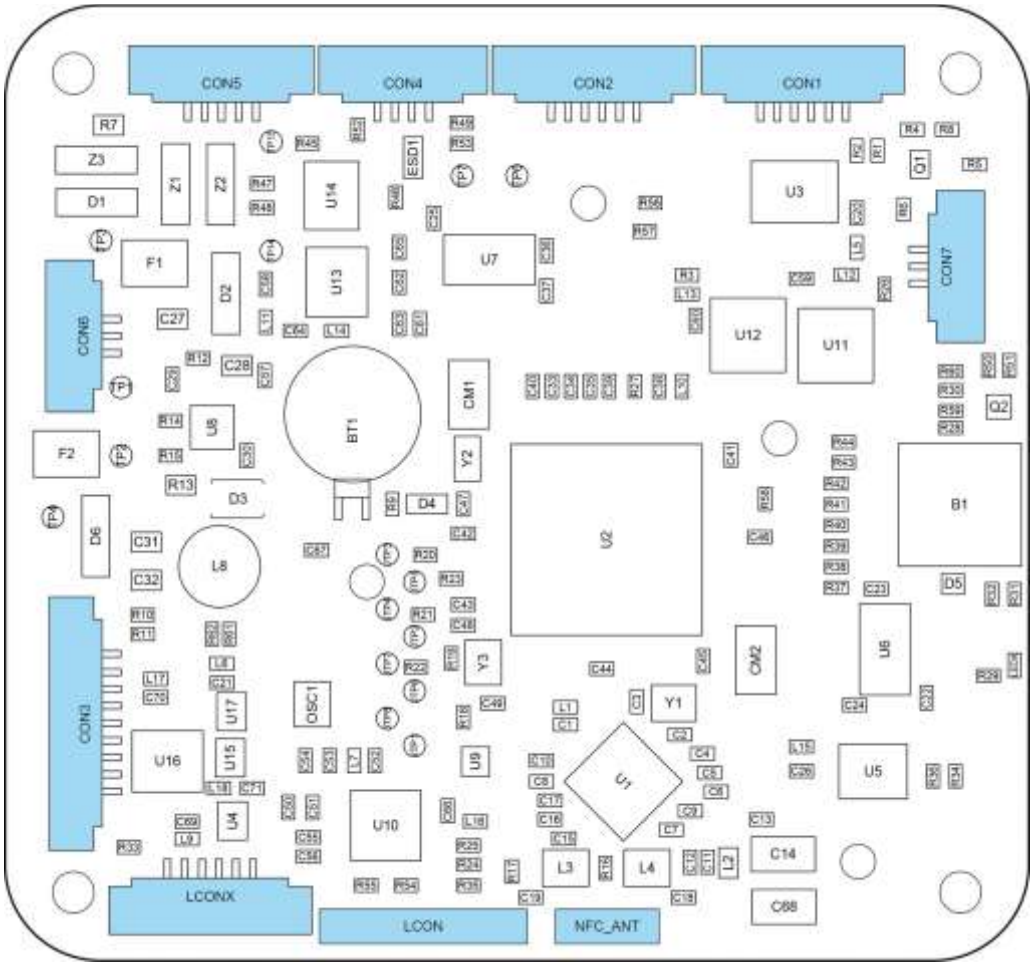




2. Connectors

The Crypto reader allows for 11 connectors to be placed, 10 on the top and 1 on the bottom side of the PCB. Not all are populated during manufacture, please contact us to state your requirements prior to ordering. The functionality and pinouts of the connectors are described below. Pin 1 is always the square pad on the board.

The top layer connector locations are highlighted in blue:



CON1

UART Logic levels (3.3V or 5V) host interface – Connector MOLEX-0532610671		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	B_RDR_INT	OUTPUT- Reader interrupt
3	UART_RTS	OUTPUT – RTS – Request To Send
4	UART_CTS	INPUT – CTS – Clear To Send
5	UART_DOUT	OUTPUT – Serial data out
6	UART_DIN	INPUT – Serial data in

CON2

SPI host interface – logic levels 3.3V or 5V – Connector MOLEX-0532610671		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	B_RDR_INT	OUTPUT- Reader interrupt
3	SLAVE_SPI_SCK	INPUT – SPI clock
4	SLAVE_SPI_DIN	INPUT – SPI slave data in
5	SLAVE_SPI_CS	INPUT – SPI slave chip select
6	SLAVE_SPI_DOUT	OUTPUT – SPI slave data out

CON3

LCD interface – logic levels 3.3V or 5V – Connector MOLEX-0532610871		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	LCD_SPI_CS	OUTPUT – SPI master chip select
3	LCD_SPI_SCK	OUTPUT – SPI master clock
4	LCD_SPI_DIN	INPUT –SPI master data in
5	LCD_SPI_DOUT	OUTPUT – SPI master data out
6	B_LCD_RESET	OUTPUT – reset signal to LCD
7	B_LCD_INT	INPUT – interrupt signal from LCD
8	LCD_POWER	Power supply to LCD – HW option 3.3V or 5V

CON4

USB interface – reader is USB device – Connector MOLEX-0532610471		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	USB+	USB Data+
3	USB-	USB Data-
4	VCC +5V	5V Power supply from USB host

CON5

RS232 host interface – Connector MOLEX-0532610571		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	RS232_RX/RS485B	RS232 RX data (input) or RS485-B
3	RS232_TX/RS485A	RS232 TX data (output) or RS485-A
4	RS232_CTS	RS232 CTS (input)
5	RS232_RTS	RS232 RTS (output)

CON6

Power supply 7.5V to 15V DC – Connector MOLEX-0532610371		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	Power input	+5.0VDC regulated
3	Power input	+7.5VDC ÷ +15VDC

CON7

Audio output – Connector MOLEX-0532610371		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	Audio output	Audio PWM signal – amplitude is HW option 0.5÷3.0V DC
3	External battery	3V external/auxiliary battery input

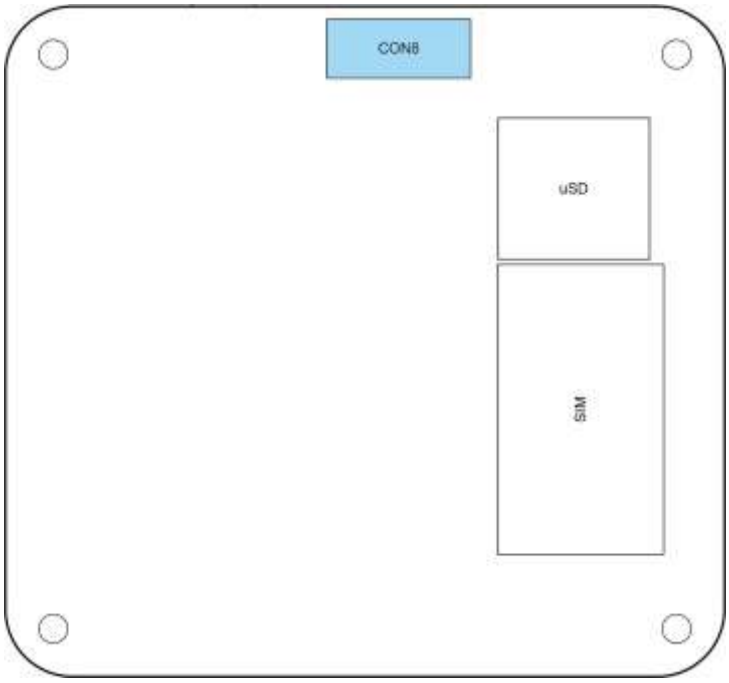
LCON/LCONX

LEDs control connector – Connector MOLEX-0532610671		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	LED1	3.3V digital output
3	LED2	3.3V digital output
4	LED3	3.3V digital output
5	LED4	3.3V digital output
6	+5V	+5V power supply to LED block

NFC_ANT

NFC frontend antenna connector		
Pin #	**Pin name**	**Function**
1	TX1	Transmitter output
2	GND	Ground
3	TX2	Transmitter output

The bottom layer connector location is highlighted in blue:



CON8

Multi-function connector – Amphenol FCI91900		
Pin #	**Pin name**	**Function**
1	GND	Ground
2	LED1	3.3V digital output
3	LED2	3.3V digital output
4	LED3	3.3V digital output
5	LED4	3.3V digital output
6	+5V	+5V power supply input
7	GND	Ground
8	LCD_SPI_CS	OUTPUT – SPI master chip select
9	LCD_SPI_SCK	OUTPUT – SPI master clock
10	LCD_SPI_DIN	INPUT –SPI master data in
11	LCD_SPI_DOUT	OUTPUT – SPI master data out
12	UART_DIN	INPUT – Serial data in- Logic levels (3.3V or 5V) host interface
13	UART_DOUT	OUTPUT – Serial data out- Logic levels (3.3V or 5V) host interface
14	GND	Ground
15	GND	Ground
16	+5V	+5V power supply input
17	+5V	+5V power supply input
18	GND	Ground
19	External battery	3V external/auxiliary battery input
20	+12V	+12V power supply input
21	+12V	+12V power supply input

3. Product Delivery & Acceptance

Due to the security features of the reader, recipients are asked to observe the following delivery acceptance guidelines:

1. The origin address on courier paperwork should be Gemini 2000 Ltd, Unit 7 Vitrage Technical Park, 27 Witney Road, Poole, BH17 0GL, United Kingdom, or a KIF address agreed beforehand. Device accountability transfer is achieved when the receiving party signs the courier acknowledgement of goods received.

2. Inspect integrity of the parcel prior to opening and presence of 2 void stickers on top and bottom.

3. Read and keep Delivery Note and Certificate of Authenticity.

4. Ensure individual readers are in anti-static bags that are sealed and not tampered or compromised in any way. See section **Determining Authenticity** below.

5. Check all readers' serial numbers against a list provided separately via email or letter.

4. Reader Storage

The following storage measures are recommended for both short-term and long-term storage:

1. Store readers in sealed anti-static bags.

2. Label and quarantine tampered readers and other returns and store separately until shipping to Gemini 2000 Ltd. Use our RMA form for all returns.

3. Keep Crypto readers in locked storage with access provided only to personnel that requires it.

Keep Crypto readers in locked storage with access provided only to personnel that requires it.

Battery for Long-Term Storage

The on-board backup battery on the Crypto reader lasts up to 7 days. Running out of power will cause a tamper event and disable certain reader functionality. For prolong storage, therefore, ensure that readers remain powered.

A larger battery, for example 3V 1000mAh, connected at CON7 would provide years' worth of power.

4. Installation

Determining Authenticity

Ensure that all instructions listed in the **Product Delivery and Acceptance** section above have been followed. This procedure represents a secure mechanism for catching tampered products.

The reader should be checked for any signs of tampering that may have occurred. Those include:

- Ground boards, scratches.
- Thermal damage.
- Hanging wires.
- Foreign objects between the two boards.
- Missing labels.

Identification Labels

The UID of the Crypto reader (QR-code) and its configuration are noted on labels on the antenna and the main boards.

Firmware version

Obtained via software commands. **Format:** e.e.e-s.s.s-xxx

Where:

- Positions 1-3-5 of variable (e.e.e) - EMV related version number, currently 0.7.1
- Positions 7-9-11 of variable (s.s.s) – Security related version
- Positions 13,14, 15 (xxx) - A counter which reflects the non-EMV and non-Security related updates. Any change in xxx does not require re-certification.

FW version example: v0.7.1-1.0.0-012

Hardware version

Indicated on label. **Format:** v2.0-x-yyyy-ff-rr-k-a-p

x – Host interface, one of:

- R – for RS232 host interface
- U- for UART host interface
- C – for USB/CDC host interface
- 4 - RS485
- S – SPI slave – RFU (not yet implemented)

yyyy – Hexadecimal bitmap – connector mask – the corresponding bit is set if the connector is fitted on board

Connector	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
CON1																X
CON2															X	
CON3														X		
CON4													X			
CON5												X				
CON6											X					
CON7										X						
CON8									X							
LCON								X								
LCONX							X									
CM1						X										
CM2					X											
uSD				X												
SIM			X													

ff – QSPI Flash size

- First letter is one of
  - 0: no QSPI FLASH fitted
  - 1: one QSPI chip fitted
  - 2: two QSPI chips fitted
- Second letter is the memory size of FLASH chip in Mbytes

Ex: 14 – One flash chip, 4MB

rr – FRAM size in Mbit

k – KB host functionality present (0 or 1)

a – antenna LEDs - can be one of:

- T - no LEDs fitted
- G – LEDs fitted

p - Power supply

- 5 - 5v
- 9 - 9-12V or 5V

Installation

The Crypto reader is an OEM device. For a successful integration, the following requirements must be complied with:

The interface type and connectors used – the reader should be ordered with the correct type of interface (USB or RS-232 – TTL or RS levels) and the correct type of connectors (wire-to-board or board-to-board) for integration with the host.

Power supply – 5V or 12V power supply. External battery for the tamper protection is optional.

Mechanically secured reader – the reader should be mounted with 4 screws on the back.

NFC – no metal objects, for example metal housing parts, should be within 2cm of the reader antenna.

Thermals – the reader should not be near warm parts (like power supply, for example), because high temperatures can set of the tamper protection.

The reader should not be disassembled during installation, as the tamper protection could be set off by accident.

Environmental Conditions

Power supplies - 12V ± 10% or 5V ± 10%. Never use 12V and 5V power supply at the same time. There is an optional battery input (3V) in order to keep the battery for the tamper protection fully charged.

Working and storage temperature -20°C to +80°C.

5. Software Integration

Communication

Crypto communicates with the host via serial interface – RS232 or UART logic levels, or via USB CDC. The host sends commands and the reader returns result code and data. The host always talks first. The reader does not send data to host if not instructed to. The communication with the host is carried by proprietary Block Framing Protocol. Gemini 2000 Ltd provides G2K API library which implements this protocol and takes care of the low-level communication layer.

API

Crypto implements a set of commands identified by a command code. Each command takes a number of parameters and returns a result code. Some commands return data as requested.

All commands are accessible via G2K API. An additional library – Crypto Interface library – is provided which facilitates the invocation of commands necessary to perform EMV Contactless payment transactions. For more detailed description of the library refer to **Crypto Interface Library User Manual**.

For detailed software development documentation refer to **Gemini 2000 API4.0 Reference Guide** and **Crypto Developer Guide.**

6. Operation, Repair and Maintenance

Periodic Inspection

The device should be visually inspected on a regular basis (recommended annually) to ensure that no foreign objects have been attached to the device. Check for signs of physical tampering including, but not limited to drilling, grinding, broken tamper meshes and thermal damage. Note the inspection date on an attached label or a spreadsheet.

Further, all errors returned by Crypto should be recorded and analysed to ensure that no tamper event has occurred.

Tamper Mechanisms and Response

The Crypto has tamper meshes for physical protection and mechanisms to detect extreme temperatures, voltages and glitch attempts. If any of those mechanisms are triggered, the reader will delete all of the important keys and become inoperable. If a tamper event has occurred, the reader will restart itself and beep with two long beeps and three short beeps then it beeps periodically. In the event of a suspected tamper, contact Gemini 2000 Ltd immediately.

Self-Test

The Crypto does a self-test to determine the authenticity of the loaded firmware using an HMAC-SHA256. The test is executed at every power up and periodically every 24 hours. If the test fails, the content of the FLASH memory is erased.

Repair

All repairs should be done by Gemini 2000 Ltd in the authorised facility in Poole, Dorset. No repairs should be carried out outside of these premises. Any products that require repairs should be shipped to us with a completed RMA form. This is available at www.gemini2k.com/RMA

Decommissioning

To decommission a Crypto reader, make sure you follow all steps below:

1. Power down the reader.
2. Detach auxiliary battery from the reader.
3. Detach the antenna to gain access to the on-board battery.
4. At this stage most probably the reader is in a tampered state.
5. Using conductive material, (e.g. tweezers, wire) momentarily short circuit the battery.
6. All secure data, e.g. keys, is lost, the reader is in non-functional state and cannot be used for account data handling.
7. You can return the decommissioned reader to Gemini 2000 Ltd for safe disposal. Use RMA form at www.gemini2k.com/RMA

Loss or Theft

A misplaced Crypto reader poses a serious security threat. Whether a board is lost or suspected stolen, the customer should immediately alert:

- Gemini 2000 Ltd
- The scheme's Payment Service Provider
- Any other partners that are involved in the payment process

Providing the UID of the reader, if possible, will help identify if the device is in use and the PSP can stop accepting communications from it.

Copyright