PMA959P-CB
08/11/2010

RDR CONTACTLESS READER

Reference manual

Headquarters, Europe

SpringCard
13 voie la Cardon
Parc Gutenberg
91120 Palaiseau
FRANCE

Phone : +33 (0) 164 53 20 10
Fax : +33 (0) 164 53 20 18

Americas

SpringCard
6161 El Cajon blvd
Suite B, PMB 437
San Diego, CA 92115
USA

Phone : +1 (713) 261 6746

www.springcard.com

DOCUMENT INFORMATION

Category : Manual
Group : K632-based readers
Reference : PMA959P
Version : CB
Status : Approved

Keywords :
RFID Scanner, K632, CSB4, Reader

Abstract :

pma959p-cb.doc
saved 08/11/10 - printed 08/11/10

REVISION HISTORY

Ver.	Date	Author	Valid. by Tech.	Valid. by Qual.	Approv. by	Remarks :
AA	16/02/09	JDA	JDA	LTX	JDA	Early draft, created as a copy of IWM-K632's reference manual Still a few paragraphs to be written
AB	09/11/09	LTX	LTX	LTX	ECL	Added "Special Mode" (firmware version ≥ 1.33)
CA	02/07/10	JDA				New chapter 2 "Getting started", a few precisions added here and there Added "Suspend" mode (firmware version ≥ 1.35)
CB	02/11/10	JDA				A few typo fixed, title "RDR-K632" changed to "RDR"

TABLE OF CONTENT

1. INTRODUCTION

This document provides detailed technical information for use of the **SpringCard** OEM contactless proximity card reader **RDR** firmware. This reader firmware can run in all devices based on the K632 hardware.

1.1. AUDIENCE

This manual is designed for use by application developers. It assumes that the reader has expert knowledge of computer development.

1.2. PRODUCT BRIEF

a. Abstract

SpringCard RDR are OEM proximity readers. They read serial number or data from any standard ISO/IEC 14443 contactless card, including popular NXP MIFARE and DESFire families, and also ISO/IEC 15693 vicinity tags used in RFID systems.

SpringCard RDR belong to the **SpringCard RFID Scanner** family, which means that most characteristics of the RDR products are shared with the RFID Scanner products (especially the configuration attributes and methods).

This makes it easier to use various products (for instance, a wall-mounted reader and an USB PC-connected reader) sharing a common configuration to read the same cards.

b. Typical applications

This reader is primarily dedicated to corporate access control, where a high level of security or versatility is needed, but can also be used in cash or vending machines.

c. Output modes

Depending on software configuration (stored in non-volatile memory) and on underlying hardware, the same reader firmware can be operated into 2 modes:

- Half-duplex serial mode (RS-485 typically),
- Full-duplex serial mode (RS-232 typically, or USB to serial bridge).

Actual capabilities and compliance to standards (RS-485, RS-232, RS-422, …) depend on the actual hardware, and are out of the scope of this document. Please refer to the datasheet of the product itself for details.

d. On the field configuration

SpringCard RDR is fully configurable on-the-field through secured Master Cards. Internal MD5, DES and 3-DES cryptographic algorithms are available for advanced security operations.

1.3. SUPPORT AND UPDATES

Interesting related materials (product datasheets, application notes, sample software, HOWTOs and FAQs…) are available at SpringCard's web site:

www.springcard.com

Updated versions of this document and others will be posted on this web site as soon as they are made available.

For technical support enquiries, please refer to SpringCard support page, on the web at address www.springcard.com/support .

1.4. SUPPORTED HARDWARE

You'll find any details regarding hardware and physical characteristics of each reader in the corresponding datasheet.

	Description	Hardware spec.	Integration manual
RDR-K632	K632 module with RDR firmware	PFL81TP	PNAE010
RDR-K632-TTL	K632 module plus antenna, TTL/CMOS interface, with RDR firmware	PFL9231	PNA9185
RDR-K632-232	K632 module with antenna, RS-232 interface, with RDR firmware	PFL9230	
CSB4.4U-RDR	CSB 4.4 USB with RDR firmware		
CSB4.4S-RDR	CSB 4.4 Serial with RDR firmware		

2. GETTING STARTED

2.1. INTERFACING RDR WITH YOUR TARGET SYSTEM

The **SpringCard K632** is a contactless/RFID reader. It will send its data over its serial line to a target system. This target could be a computer, an embedded micro-computer, or a low-end microcontroller. The simplicity of the communication protocol makes it possible to receive the contactless/RFID data with minimal constraints onto the target system.

The first step is to build the hardware interface to implement the serial communication line and, if needed the optional control signals.

Do not connect **RDR-K632** (module only) or **RDR-K632-TTL** (module with antenna featuring TTL interface) directly to an RS-232 communication port.

RX/TX are TTL-level digital pins.

Applying an inappropriate level to them may permanently damage the reader.

2.1.1. Interfacing RDR-K632-232 or RDR-K632-TTL

Please refer to document ref. PNA9185 for details.

The device could be interfaced through only 3 wires:

- Power (VCC),
- Ground (GND),
- *Module to host* communication line (TX).

Note that this minimal configuration does not allow any control from the host on the module;

- *Host to module* communication line (RX) makes it possible to configure the module through the serial line, and to change its runtime behaviour through short commands (see § 5.2.3).

3 more wires give advanced control on the module:

- The /SUSPEND pin makes it possible to put the **RDR** in "low frequency" lookup mode, or to disable totally the lookup. This reduces the overall power consumption of the device,
- The /RESET pin is necessary to reset the module's CPU,
- The /FLASH pin is necessary to upgrade the firmware.

2.1.2. Interfacing RDR-K632

Please refer to document ref. PNAE010 for details.

The K632 module needs an external antenna to operate.

The antenna has to be designed carefully, depending on your own specifications (size constraints, expected operating distance) but with limited flexibility due to the requirements of the ISO standards and the EMC regulations.

SpringCard has a strong experience in antenna design. Do not hesitate to contact us for consultancy.

2.1.3. Interfacing CSB4.4-RDR

The CSB4.4U (USB) and CSB4.4S (Serial) offer direct connection to a computer.

- **CSB4.4U-RDR**: download and install driver **SDD100** to make the device recognized as a **virtual communication port** other USB,
- **CSB4.4S-RDR**: the device's **RS-232 DB9 plug** allows immediate connection to the computer – no driver is needed.

2.2. CHECKING THE COMMUNICATION LINE

*In this paragraph, we assume that your RDR-K632 device has been connected to a computer. We use a "terminal emulation software" (**HyperTerminal** on Windows) to dialog with it. Adapt this to your actual target system.*

2.2.1. Communication settings

Out-of-factory communication settings are:

- baudrate = 38400bps,
- 8 data bits,
- 1 stop bit,
- no parity,
- no flow control.

NB: The baudrate could be changed by the mean of configuration attributes (§ 3.3.1). Set the baudrate to match the actual configuration of your device.

2.2.2. Startup prompt

Upon startup (power up or reset), the **RDR** firmware sends its version string:

```
SpringCard RDR-K632 1.35
```

NB: The string is followed by CR/LF. Upon power up, a dummy byte may be seen by the target before this string.

2.2.3. Retrieving firmware information

Send the command `info` (followed by CR/LF) to get more details on the firmware.

2.2.4. Testing the reading

When in out-of-factory configuration, **RDR** is free of any card acceptance template. To be easily testable and usable even without configuration, it will lookup for any supported card, and sends its ID (up to 8 bytes).

Present a supported card in front of the antenna, and see the transmitted stream.

NB: Once the card acceptance templates (see chapter 4) have been loaded in the reader, the reader will only transmit the ID or the data of the card(s) matching the template(s), according to the output format you've specified, so the behaviour may become very different than what is was when the device was in out-of-factory configuration.

2.3. CONFIGURING THE READER TO MATCH YOUR REQUIREMENTS

At this step, you may know configure the reader according to your own specification:

- Communication baudrate and output format,
- List of card to be looked-up for,
- ID or data to be retrieved from the card,
- Behaviour of the LED output lines, period of the lookup loop, etc.

The reader is fully configurable through configuration attributes (chapters 3 and 4).

The configuration attributes could be read and written either in the serial communication stream (chapter 6) or by the mean of a *Master Card* (chapter 7).

2.4. POWER-SAVING[1]

The **RDR** is not able to "see" the contactless cards coming in front of its antenna without establishing an RF field (to power the card, if some) and sending repeated discovery commands to see whether or not a card responds. This is the **polling** sequence.

The only way to reduce overall power consumption is to change the duty cycle, so the reader spends more time "doing nothing" that performing the polling sequence[2].

There are 4 configuration attributes that impacts the power requirement:

- Bit 7 of OPT (§ 3.2.1),
- POL.CFG, POL.FST and POL.SLO (§ 3.4.1).

2.4.1. User experience drawback

As a consequence of changing the duty cycle of the polling sequence, the reactivity of the reader is decreased: the user has to keep his card in front of the antenna until the polling sequence finds the card, so if the sequence runs, say, every 2 seconds, he may wait up to 2 seconds before observing any reaction from the system.

2.4.2. Role of the /SUSPEND pin

When the /SUSPEND pin is enabled in POL.CFG and is at LOW level, the reader does the following:

- It switches of all its LEDs,
- It stops listening on the serial line,
- If POL.SLO is non-zero, the interval between the polling sequences is set to POL.SLO ; if POL.SLO=0, the polling is halted until /SUSPEND is back to HIGH level.

When the /SUSPEND pin is back to HIGH level, the polling sequence is resumed within 15ms, then the interval is set to POL.FST again.

[1] Only for firmware version ≥ 1.35

[2] The duration of the polling sequence itself is mandated by the standards or the specification of the cards being looked up for. The more protocols are to be handled, the more time it will last, so the more energy it will needs. Specifying the Card Acceptance Templates efficiently to "see" only the card you do really need is the first step to reduce overall power consumption.

3. CONFIGURATION ATTRIBUTES

There are two groups of configuration attributes:

- Product specific Global Configuration Attributes,
- Card Acceptance Templates.

The Card Acceptance Templates are common to all products in the **SpringCard RFID Scanner family**, and are exposed in detail in the next chapter.

In this chapter, we'll introduce configuration tags and detail the **RDR**'s specific configuration attributes.

3.1. PRINCIPLES

a. Configuration tags

Each configuration attribute is recognized by its "tag" and its length. The tag is a one-byte value, which uniquely identifies the attribute.

The list of available tags, and their meaning, is the purpose of this chapter and the next one.

Unless specified, each configuration attribute is exactly one byte (8 bits) long.

b. Non-volatile memory endurance

RDR configuration attributes are stored in reader's non-volatile memory (flash). They can be changed up to 100 times.

Changing any configuration attribute more than 100 times may permanently damage your **RDR** reader.

3.2. GLOBAL CONFIGURATION ATTRIBUTES

3.2.1. General options

Name	Tag	Description	Size
OPT	$_h$60	General options. See table **a** below.	1

a. General options bits

Bit	Value	Meaning
7	0	Normal mode
	1	Power saving mode[3]
6	0	Shutdown RF field when idle
	1	Shutdown RF field only when no card detected[4]
5 – 4		***Anti-collision model :***
	00	Process every card one after the other
	01	*RFU*
	10	When 2 cards are in the field, process the 1st and ignore the 2nd
	11	When 2 cards are in the field, ignore both
3 – 2		***Master Card :***
	00	Master Cards are disabled[5]
	01	Master Cards are enabled at power up
	10	*RFU*
	11	Master Cards are enabled all the time
1 – 0		***Output interface***[6] ***:***
	00	serial duplex (RS-TTL, RS-232, USB …) reader
	01	serial half-duplex (RS-485) reader
	10	*RFU*
	11	*RFU*

Default value: $_b$00001101

(Master Cards are enabled all the time, RS-485)

[3] When this value is selected, the card detection loop runs only every 250ms. In the meantime, RC chipset is OFF to reduce average power consumption. Do not choose this mode if you need fast operation at the gates, since it will increase transaction time at least by 250ms.

[4] This is required if strict anti-collision (bits 5-4 = $_b$10 or $_b$11) is needed.

[5] Configuration settings can only be altered through serial link

[6] Actual RS-232, RS-422, RS-TTL or USB compliance depends on external/optional hardware.

3.2.2. Delays and repeat options

Name	Tag	Description	Min	Max
ODL	$_h$61	Min. delay between 2 consecutive outputs (0.1s).	0	100
RDL	$_h$62	Min. delay between 2 consecutive identical outputs (0.1s). A value of 255 means that the card must be removed from the field –and re-inserted into– before being read again.	0	100

Default value: ODL = 5 (1ms) RDL = 20 (2s)

3.2.3. LED control options

Name	Tag	Description	Size
CLD	$_h$63	LEDs control. See table **a** below.	1

a. LEDs control bits

Bit	Value	Meaning
7	0 1	Short LED sequences (3 seconds) Long LED sequences (10 seconds)
6	0	*RFU (set to 0)*
5	0 1	When idle, red LED blinks slowly (“heart beat” sequence) When idle, red LED is off
4	0 1	Green LED stays OFF Green LED blinks when a valid card has been processed
3	0 1	Red LED stays OFF Red LED blinks when an unsupported card has been processed
2	0 1	Green LED stays OFF Green LED blinks as soon as a card is seen in the field
1 – 0	11	*RFU (set to 11)*

Default value: $_b$00001111

3.3. OUTPUT MODE

3.3.1. Serial configuration

Name	Tag	Description	Size
SER	$_h$67	Serial configuration bits. See table **a** below.	1

a. Serial configuration bits

Bit	Value	Meaning
7	0	No STX / ETX frame markers
	1	Use STX and ETX as frame markers
6 – 5	00	No BEL / TAB / CR/LF frame markers
	01	Use CR/LF only
	10	Use BEL and CR/LF as frame markers
	11	Use TAB and CR/LF as frame markers
4 – 3		**Serial Repeat**
	00	No repeat
	01	Repeat 4 times with timeout of 100ms
	10	Repeat 4 times with timeout of 250ms
	11	Repeat 9 times with timeout of 250ms
2 – 0		**Baudrate**
	000	1200bps
	001	2400bps
	010	4800bps
	011	9600bps
	100	19200bps
	101	38400bps
	110	*RFU*
	111	115200bps

Default value: $_b$11000101

The baudrate parameter is common to USB, RS-232 and RS-485 interfaces.

Even if it is allowed, do not set baudrate to 115200bps when working with RS-485 interface, as the hardware and the characteristics of the bus aren't able to support it.

b. Serial frame format

Serial frames are always transmitted using ASCII representation of binary values.

For example, data '00 7A 12 6C 59 F4 04' (hexadecimal notation) is transmitted as string "007A126C59F404".

c. Serial frame markers

Bits 7-5 drive the start of frame / end of frame markers.

See chapter 5 for details on using the reader in Serial mode.

3.3.2. RS-485 mode

Name	Tag	Description	Size
SHD	$_h$68	RS-485 configuration bits. See table **a** below.	1

a. RS-485 configuration bits

Bit	Value	Meaning
7 – 4		*RFU*
3 – 0	0000	Addressing disabled (single device on bus)
	0001 to 1110	Address = $_h$01 ($_d$1) to address = $_h$0E ($_d$14)
	1111	*RFU*

Default value: $_b$00000000

3.3.3. Prefix and postfix

Name	Tag	Description	Size
BEF	$_h$A2	Prefix string. See paragraph **a** below.	Var.
AFT	$_h$A3	Postfix string. See paragraph **a** below.	Var.

a. Prefix and postfix format

BEF defines the character string do be sent *before* the actual data.

Default value for DEF: empty *(no prefix)*

AFT defines the character string do be sent *after* the actual data.

Default value for KBD: empty *(no postfix)*

If a non-null ASCII value is specified for either DEF or AFT (either a single character or a string, up to 8 characters), it will be transmitted respectively before of after the actual data (and between the frame markers defined according to 3.3.1.c, if some).

Please refer to the ASCII table for the list of values[7].

3.3.4. Keep-alive

When the reader is running in serial mode (RS-232 or RS-485), it may send keep-alive frames periodically to the target host.

This allows the host to make sure the reader is still connected.

[7] http://www.asciitable.com/

Name	Tag	Description	Size
KAL	$_h$69	Keep-alive configuration. See table **a** below.	1

Default value: $_h$00

a. Keep-alive configuration bits

Bit	Value	Meaning
7 – 4	0000	*RFU (set to 0000)*
3 – 0	0000 0001 to 1111	Keep-alive disabled Delay between 2 keep-alive frames. Minimum = $_h$1 (1s) to maximum = $_h$F (15s)

3.3.5. Specific output configurations

Name	Tag	Description	Size
SPE	$_h$6A	Specific output configuration bits. See table **a** below.	1

a. Specific output configuration bits

Bit	Value	Meaning
7 – 0	0 1 -255	Normal serial communication *RFU*

Default value: $_b$00000000

3.4. OTHERS

3.4.1. PIN code

Name	Tag	Description	Size
PIN	$_h$6F	PIN code to access reader's console.	2

Default value: empty *(no pin-code)*

Use this tag to define a 4 digits PIN code to protect access to reader's console.

The 2-byte value must store 4 valid BCD digits, or the reserved value $_h$FFFF that permanently disables the console feature.

3.4.2. Polling interval – handling of /SUSPEND[8]

Name	Tag	Description	Size	Min	Max
POL.CFG	$_h$70	Polling interval and /SUSPEND configuration bits. See table **a** below.	1		
POL.FST	$_h$71	Interval (in milliseconds) between polling sequences when /SUSPEND is HIGH (0 to 65.5s)	2	0	65535
POL.SLO	$_h$72	Interval (in milliseconds) between polling sequences when /SUSPEND is LOW (0 to 65.5s)	2	0	65535

Default values:

- POL.CFG = $_b$11000000
- POL.FST = 25 (25ms) if bit 7 of OPT is 0, or 250 (250ms) if bit 7 of OPT is 1 (see § 3.2.1)
- POL.OPT = 0 (polling suspended when /SUSPEND is LOW).

a. Polling interval and /SUSPEND configuration bits

Bit	Value	Meaning
7		***Handling of /SUSPEND pin***
	0	/SUSPEND pin is ignored
	1	/SUSPEND pin enabled
6	1	*RFU (set to 1)*
5 – 4		***Behaviour when /SUSPEND is asserted <u>and</u> a card is in the field :***
	00	Ignore /SUSPEND until the card leaves
	01	Enter /SUSPEND mode
	10	*RFU*
	11	*RFU*
3 – 0	0000	*RFU (set to 0000)*

[8] Only for firmware version ≥ 1.35

4. CARD ACCEPTANCE TEMPLATES

Products in the **SpringCard RFID Scanner** family are able to manage different types of cards, and different sources of data on each card.

A **Card Acceptance Template** defines how the reader will recognize the card to be read, and how it would get the actual data (serial number, block reading, file selection and reading, authentication keys to be used for Mifare or Desfire, etc).

The template also defines which formatting is to be applied to the data when sending them to the target device (translation to ASCII or to Decimal, constant prefix or suffix, etc).

This product is able to run up to 4 Card Acceptance Templates simultaneously.

This chapter is shared between the reference manual of all the products in the **SpringCard RFID Scanner** family. Therefore, some features or options may be unsupported by the device you're actually working with.

4.1. BASIS

Each Card Acceptance Template is configured through a set of configuration attributes, each attribute having its own tag.

- Template 1 uses Configuration tags $_h$10 to $_h$1F
- Template 2 uses Configuration tags $_h$20 to $_h$2F
- Template 3 uses Configuration tags $_h$30 to $_h$3F
- Template 4 uses Configuration tags $_h$40 to $_h$4F

In the following pages, we use the convention " Template t uses Configuration tags $_h$t0 to $_h$tF ". Replace t by the current template number.

4.1.1. Card lookup list

Name	Tag	Description	Size
LKL	$_h$t0	Card lookup list of the template. See table **a** below.	1

a. Available values for LKL

Value	Card(s) accepted by the template	Processing template	§
$_h$01	ISO/IEC 14443 type A (layer 3)	**ID only**	4.2
$_h$02	ISO/IEC 14443 type B (layer 3)		
$_h$03	ISO/IEC 14443 A&B (layer 3)		
$_h$04	ISO/IEC 15693		
$_h$07	ISO/IEC 14443 A&B and ISO/IEC 15693		
$_h$08	NXP ICODE1		
$_h$0C	NXP ICODE1 and ISO/IEC 15693		
$_h$0F	All of the above		
$_h$11	ISO/IEC 14443 type A (layer 4 / T=CL)	**7816-4**	4.6
$_h$12	ISO/IEC 14443 type B (layer 4 / T=CL)		
$_h$13	ISO/IEC 14443 A&B (layer 4 / T=CL)		
$_h$22	ST MicroElectronics SR family	**ID only**	4.2
$_h$23	ASK CTS256B and CTS512B		
$_h$24	Inside Contactless PicoTAG[9]		
$_h$61	NXP Mifare Classic 1k & 4k	**Mifare Classic**	4.3
$_h$62	NXP Mifare UltraLight	**Mifare UltraLight**	4.4
$_h$71	NXP Desfire 4k	**Desfire**	4.5
$_h$72	Calypso (Innovatron protocol)	**ID only** or **7816-4**	4.2 or 4.7
$_h$FF	All cards supported	**ID only**	4.2

Other values are *RFU*

The LKL tag is mandatory to enable a template group. If not found, the template group is assumed to be empty.

[9] Also HID iClass

4.1.2. Summary of other tags in templates

Depending of the card lookup list (LKL tag), a specific list of tags controls the behaviour of the Processing Template.

The table below summarize this.

Tag	ID only	Mifare UltraLight	Mifare Classic	Desfire	7816-4	Calypso
$_h$t1	Output format					
$_h$t2	Output prefix					
$_h$t3	Offset	Location of data				
$_h$t4	Options			T=CL options		C. options
$_h$t5			Auth. method & key		1st APDU	
$_h$t6			Sign. method & key		2nd APDU	
$_h$t7					3rd APDU	

Grey items are *RFU* and must be kept empty.

4.1.3. Important notice regarding template-ordering

Be careful that the 4 templates are processed one after the other. The loop is ended after the first successful match.

If a card matches two (or more) templates, it will be handled only by the first one.

Suppose you want to accept both a specific kind of 14443-B T=CL cards, with advanced file reading, and another kind of wired-logic 14443-B cards, where only the ID is significant. You must put the T=CL template *before* the ID template, otherwise the T=CL part will be skipped.

4.2. ID-ONLY ACCEPTANCE TEMPLATES

Use an ID-only Acceptance Templates when you want to read the serial number and/or the protocol-related constant bytes from a contactless card, or a group of contactless cards.

Depending on the settings you define in the Lookup List attribute (tag LKL.IDO), the reader may either

- Find any supported contactless card,
- Find only a specific family of contactless cards,
- Find ISO compliant contactless cards.

As you may have more than one ID-only Acceptance Template (up to 4 in fact), you may easily read different kinds of cards, with a format that is different for each one.

Including card's type in the returned ID is also an interesting option (see 4.2.6.b), as for instance there's no rule to prevent an ISO 14443-B card to have a different serial number than any ISO 14443-A ones.

4.2.1. Lookup list

Name	Tag	Description	Size
LKL.IDO	$_h$t0	**ID-only lookup list :** $_h$01 ≤ value ≤ $_h$0F for ISO-compliant cards, $_h$21 ≤ value ≤ $_h$2F for non-ISO cards, value = $_h$FF all the supported cards. See **4.1.1.a** for details.	1

4.2.2. Output format

Name	Tag	Description	Size
TOF.IDO	$_h$t1	ID-only output format. See table **a** below.	1

a. Output format bits

Bit	Value	Meaning
7 – 6		**Byte swapping**
	00	Do not swap ID bytes (ID is transmitted "as is")
	01	*RFU*
	10	Swap bytes for single-size (4 bytes) ISO 14443-A UIDs [10] only ; IDs of any other card is transmitted "as is"
	11	Swap ID bytes for all kind of cards
5		**Padding**
	0	Left-padding with $_h$0
	1	Right-padding with $_h$F
4		**ISO 14443-B specific**
	0	Use ISO 14443-B PUPI (4 bytes) as ID
	1	Use complete ISO 14443-B ATQ (11 bytes) as ID
3 – 0		**Output length**
	0000	Decimal, 4 bytes seen as 10 digits (i.e. 32 → 40 bits expansion)
	0001	Fixed length, 4 bytes [11]
	0010	Fixed length, 8 bytes [12]
	0011	Fixed length, 5 bytes
	0100	Fixed length, 12 bytes [13]
	0101	Fixed length, 7 bytes [14]
	0110	Fixed length, 11 bytes [15]
	0111	*RFU*
	1000	Fixed length, 16 bytes
	1001	*RFU*
	1010	*RFU*
	1011	*RFU*
	1100	Decimal, 5 bytes seen as 12 digits (i.e. 40 → 56 bits expansion)
	1101	Decimal, 5 bytes seen as 13 digits (i.e. 40 → 64 bits expansion)
	1110	Decimal, variable length (maximum 13 digits)
	1111	Variable length (depends on actual size of ID)

Default value : $_b$10000010

(8 bytes fixed length, left padding, swap bytes for short ISO 14443-A UIDs only)

[10] This is the default format in NXP's Mifare Classic related literature.

[11] ISO 14443-A single-size UID, ISO 14443-B PUPI, serial number for ASK CTS256B and CTS512B.

[12] ISO 15693 ID, serial number for NXP ICODE1, Inside Contactless PicoTag, ST MicroElectronics SR family…

[13] ISO 14443-A triple-size UID.

[14] ISO 14443-A double-size UID.

[15] ISO 14443-B complete ATQB.

4.2.3. Output prefix

Name	Tag	Description	Size
PFX.IDO	$_h$t2	ID-only output prefix.	Var.

Default value : absent *(no prefix)*

If a non-null ASCII value is specified (either a single character or a string), it will be transmitted before the data (therefore the actual length will be longer than the specified length).

4.2.4. Offset of data

Name	Tag	Description	Size
LOC.IDO	$_h$t3	Offset in the ID.	1

Default value : $_b$00000000 ($_d$0)

When TOF.IDO specifies a fixed length output, using LOC.IDO makes it possible to select some bytes in the ID, and not only the first ones. This is principally useful when working with non-ISO cards, as shown in the following paragraphs.

4.2.5. Role of LOC.IDO with non-ISO cards

A few manufacturers still offer non standard cards, most of them based on ISO 14443-B bit-level specification, but with a proprietary frame format (protocol) and a proprietary command set.

As those cards don't answer to ISO 14443 standard detection commands, a specific template must be activated to discover them.

a. ST MicroElectronics SR family

When LKL.IDO=$_h$22, the reader performs the lookup sequence for cards in the ST MicroElectronics SR family (SR176, SRX, SRIX).

An 8-byte serial number is returned by the card. Use TOF.IDO and LOC.IDO if you need to truncate it.

b. ASK CTS256B and CTS512B

When LKL.IDO=$_h$23, the reader performs the lookup sequence for cards in the ASK CTS-B family (CTS256B, CTS512B).

An 8-byte identifier is built as follow :

Byte 0	Byte 1	Byte 2	Byte 3	Bytes 4 to 7
Manufacturing code	Product code	Embedded code	Application code	4-byte serial number

- CTS256B's product code is between $_h$50 and $_h$5F,
- CTS512B's product code is between $_h$60 and $_h$6F,
- See ASK's documentation for explanations regarding other bytes.

Define LOC.IDO=$_h$04 (and TOF.IDO=$_h$01) if you need only the serial number (and don't care for card type and other data).

c. Inside Contactless PicoTAG[16]

When LKL.IDO=$_h$24, the reader performs the lookup sequence for cards in the Inside Contactless PicoTAG family (PicoTAG 16KS).

An 8-byte serial number is returned by the card. Use TOF.IDO and LOC.IDO if you need to truncate it.

[16] Also HID iClass

4.2.6. Miscellaneous options

Name	Tag	Description	Size
OPT.IDO	$_h$t4	ID-only miscellaneous options. See table **a** below.	1

a. Miscellaneous option bits

Bit	Value	Meaning
7 – 4		*RFU*
3 – 2		**Position of card's type in the output**
	00	Card type is sent before the prefix[17]
	01	Card type is sent after the prefix and before the ID[18]
	10	Card type is sent after the actual ID[19]
	11	*RFU*
1 – 0		**Send card's type in the output**
	00	Do not send card's type
	01	Send card's type on one byte (2 hex digits) *(see table **b** below)*
	10	Send card's type as a string *(see table **b** below)*
	11	*RFU*

Default value : $_b$00000000

b. Values for card's type byte or string

When OPT.IDO is configured to send card's type in the output, the possible values are :

"Physical" card's type	One byte value	String value	Remark
ISO/IEC 14443 A	$_h$01	" A "	Card must be compliant with Layer 3 or layer 4
ISO/IEC 14443 B	$_h$02	" B "	
ISO/IEC 15693	$_h$04	" V "	
NXP ICODE1	$_h$08	" I "	
Inside Contactless PicoTAG	$_h$10	" i "	Also HID iClass
ST MicroElectronics SR family	$_h$20	" s "	
ASK CTS256B and CTS512B	$_h$40	" a "	
Calypso (Innovatron protocol)	$_h$80	" C "	

[17] The actual frame is <card type><PFX.IDO><card id> (PFX.IDO may be empty)

[18] The actual frame is <PFX.IDO><card type><card id> (PFX.IDO may be empty)

[19] The actual frame is <PFX.IDO><card id><card type> (PFX.IDO may be empty)

4.3. MIFARE CLASSIC ACCEPTANCE TEMPLATE

Mifare "Classic" refers to NXP Mifare 1k (MF1ICS50) and Mifare 4k (MF1ICS70) wired-logic contactless cards.

Mifare 1k is divided into 64 16-byte blocks.

Mifare 4k is divided into 256 16-byte blocks.

Both cards have a 4-byte serial number, located at the beginning of block 0. As those cards are ISO/IEC 14443-3 compliant, you can read the serial number through the generic ID-Only template, instead of using this dedicated template.

4.3.1. Lookup list

Name	Tag	Description	Size
LKL.MIF	$_h$t0	Mifare classic lookup list, value = $_h$61. See **4.1.1.a** for details.	1

4.3.2. Output format

Name	Tag	Description	Size
TOF.MIF	$_h$t1	Mifare output format. See table **a** below.	1

a. Output format bits

Bit	Value	Meaning
7	0 1	Do not swap bytes Swap bytes
6	0 1	RAW data ASCII encoded data [20]
5		***RAW : padding mode*** *(when bit 6= 0 and read length < specified output length)* Left-padding with $_h$0 Right-padding with $_h$F ***ASCII : padding mode*** *(when bit 6= 1 and read length < specified output length)* Left-padding with <SPACE> Right-padding with <SPACE>
4	0 1 0 1	***RAW : strip leading zeros*** *(when bit 6= 0)* Do not remove leading zeros Do remove leading zeros ***ASCII : long string option*** *(when bit 6= 1)*[21] Disable long string reading option Enable long string reading option
3 – 0		**Output length** Format depends on bit 6 (RAW or ASCII). See table **b** below for RAW data (bit 6 = 0) See table **c** below for ASCII data (bit 6 = 1)

Default value : $_b$00000010

[20] If data read from the memory card is "31 32 33 43 34 35" (hexadecimal notation), output will be "123C45". Make sure that only valid digits (values from 31 to 39 and 41 to 46 or 61 to 66) are encoded in every card, otherwise actual reader output will be undefined.

[21] This option is only available on Prox'N'Roll RFID Scanner, AutomotiveReader, RDR-K632 and ProxRunner. If working with IWM-K632 or FunkyGate, please ignore this configuration tag.

b. Output length when bit 6 = 0

Bit	Value	Meaning
3 – 0	0000	Decimal, 4 bytes seen as 10 digits (i.e. 32 → 40 bits expansion)
	0001	Fixed length, 4 bytes (32 bits)
	0010	Fixed length, 8 bytes (64 bits)
	0011	Fixed length, 5 bytes (40 bits)
	0100	Fixed length, 12 bytes (96 bits)
	0101	Fixed length, 7 bytes (56 bits)
	0110	Fixed length, 11 bytes (88 bits)
	0111	*RFU*
	1000	Fixed length, 16 bytes (128 bits)
	1001	*RFU*
	1010	*RFU*
	1011	*RFU*
	1100	Decimal, 5 bytes seen as 12 digits (i.e. 40 → 56 bits expansion)
	1101	Decimal, 5 bytes seen as 13 digits (i.e. 40 → 64 bits expansion)
	1110	Decimal, variable length (maximum 13 digits)
	1111	Variable length (using $_h$0 and $_h$F as end of string markers)

c. Output length when bit 6 = 1

Bit	Value	Meaning
3 – 0	0000	Max output length = $_d$16
	0001 to 1111	Max output length from $_d$1 to $_d$15

4.3.3. Output prefix

Name	Tag	Description	Size
PFX.MIF	$_h$t2	Mifare output prefix.	Var.

Same as ID-only output prefix (see 4.2.3).

4.3.4. Location of data

Depending on the size, the LOC.MIF tag can either be

- A block number (= address of data in Mifare card) when size = 1,
- An Application Identifier (AID) when size = 2.

a. Fixed block number

Name	Tag	Description	Size
LOC.MIF	$_h$t3	Block number to be read.	1

Default value : $_b$00000100 ($_d$4)

When a Mifare card is found, the reader tries to read the block specified in LOC.MIF (16 bytes), and then truncates the data according to the length specified in TOF.MIF.

The block number shall be

- Between 0 and 63 for Mifare 1k cards,
- Between 0 and 255 for Mifare 4k cards.

Note that data must start on a block boundary.

Mifare sector trailers (security blocks) numbered 3, 7, … can be read, but their content is masked (to protect the keys). Using such a block as access control identifier is definitely not a good idea.

b. AID in MAD

Name	Tag	Description	Size
LOC.MIF	$_h$t3	AID to be selected and read.	2

When a Mifare card is found, reader reads the MAD (blocks 1 and 2 of sector 0)[22] and tries to find the specified AID. The location of the AID in the MAD is the pointer onto the actual block to be read.

Note that data must be located at the beginning of the first block marked with the specified AID.

Please refer to NXP application notes for detailed explanations of the MAD.

[22] Sector 0 must be freely readable either with base key A ("A0 A1 A2 A3 A4 A5"), with transport key ("FF FF FF FF FF FF") or with the application key specified in AUT.MIF .

4.3.5. Authentication key

Depending on the size, the AUT.MIF tag can either be

- A pointer to a key located in RC's secure EEPROM when size = 1.
- The Mifare key itself, when size = 7,
- A master key and its diversification options, when size = 9 or 17

When the AUT.MIF tag is absent, all EEPROM keys are tried out in sequence (this can take a long time…).

Name	Tag	Description	Size
AUT.MIF	$_h$t5	Mifare authentication key.	See below

Default value : absent

a. Size = 1 : pointer to a key in RC's secure EEPROM

- Values $_h$00 to $_h$0F refer to type A keys $_d$0 to $_d$15, respectively,
- Values $_h$80 to $_h$8F refer to type B keys $_d$0 to $_d$15, respectively.

b. Size = 7 : specified Mifare key

Offset	Length	Content
0	1	Key options. See table **c** below.
1	6	Mifare key value.

c. Key options bits, when size = 7

Bit	Value	Meaning
7	0 1	Key is an A key Key is a B key
6 – 0		*RFU*

d. Size = 17 : master key diversification using HMAC-MD5

Offset	Length	Content
0	1	Key options. See table **e** below.
1	16	Master key value.

e. Key options bits, when size = 17

Bit	Value	Meaning
7	0 1	Diversified key is an A key Diversified key is a B key
6	0 1	Diversification with card UID and address fixed to $_h$00 Diversification with card UID and address = sector number
5 – 4	10	Diversify the key using HMAC-MD5 algorithm
3 – 0		*RFU*

f. Size = 15 or 23 : master key diversification using RC171 algorithm

Offset	Length	Content
0	1	Key options. See table **g** below.
1	6	Mifare master key.
7	8 or 16	DES or 3-DES diversification key.

g. Key options bits, when size = 15 or 23

Bit	Value	Meaning
7	0 1	Diversified key is an A key Diversified key is a B key
6	0 1	Diversification with card UID and address fixed to $_h$00 Diversification with card UID and address = sector number
5 – 4	01	Diversify the key using RC171 algorithm
3 – 0		*RFU*

4.3.6. Reading a long string from a Mifare Classic card

Note : This option is only available on Prox'N'Roll RFID Scanner, Automotive Reader, RDR-K632 and ProxRunner.

When bits 4 and 6 in TOF.MIF are set (ASCII output, long string reading extension enabled), the reader behaves as follow :

- The output length (bits 0 to 3 of TOF.MIF) is ignored,
- The reader reads sequentially all Mifare data blocks starting at address specified in LOC.MIF (absolute address or pointer found in MAD), until one of those events occurs :
  - The end-of-string character ('\0' i.e. $_h$00) is read,
  - The end of the card is reached,
  - The authentication failed (see note below),
  - 4 blocks (64 bytes) have been read.

Doing so, the reader is able to fetch ASCII strings up to 64 characters.

Note : in this mode, the reading may cross a sector boundary (64 bytes is 4 blocks, where sectors below 32 are 3-block wide). In this case, the two sectors to be read must be formatted with the same Mifare key and the same access mode.

4.4. MIFARE ULTRALIGHT ACCEPTANCE TEMPLATE

NXP Mifare UltraLight is a low-cost wired-logic contactless card. It is divided into 16 4-byte pages. This template reads 4 pages (i.e. exactly 16 bytes) at once.

This card has a 7-byte serial number, located on blocks 0 and 1. As the card is ISO/IEC 14443-3 compliant, you can read the serial number through the generic ID-Only template, instead of using this dedicated template.

4.4.1. Lookup list

Name	Tag	Description	Size
LKL.MFU	$_h$t0	Mifare UltraLight lookup list, value = $_h$62. See **4.1.1.a** for details.	1

4.4.2. Output format

Name	Tag	Description	Size
TOF. MFU	$_h$t1	Mifare UltraLight output format.	1

Same as Mifare Classic output format (see 4.3.2).

4.4.3. Output prefix

Name	Tag	Description	Size
PFX.MFU	$_h$t2	Mifare UltraLight output prefix.	Var.

Same as ID-only output prefix (see 4.2.3).

4.4.4. Location of data

Name	Tag	Description	Size
LOC.MFU	$_h$t3	Number of the first page to be read.	1

Default value : $_b$00000000 ($_d$0)

Remember that this template always reads 4 pages (16 bytes) starting at LOC.MFU.

4.4.5. Reading a long string from a Mifare UltraLight card

Note : This option is only available on Prox'N'Roll RFID Scanner, Automotive Reader, RDR-K632 and ProxRunner.

When bits 4 and 6 in TOF.MIF are set (ASCII output, long string reading extension enabled), the reader behaves as follow :

- The output length (bits 0 to 3 of TOF.MIF) is ignored,
- The reader reads sequentially all Mifare data blocks starting at address specified in LOC.MIF (absolute address or pointer found in MAD), until one of those events occurs :
  - The end-of-string character ('\0' i.e. $_h$00) is read,
  - The end of the card is reached,
  - 16 pages (64 bytes) have been read.

Doing so, the reader is able to return ASCII strings up to 64 characters[23].

[23] Well, not really, as Mifare UltraLight currently features only 64 bytes of data, with only 48 bytes actually usable to store data.

4.5. DESFIRE ACCEPTANCE TEMPLATE

Desfire Acceptance Template has been designed for the first version of NXP Desfire 4k cards (MF3ICD40).

It should work with new Desfire versions (MF3ICD21, MF3ICD41 and MF3ICD81) as long as they are configured to remain compatible with the earlier version (DES or two-key Triple-DES authentication, same ATQ/SAK as MF3ICD40).

4.5.1. Lookup list

Name	Tag	Description	Size
LKL.DFR	$_h$t0	Desfire lookup list, value = $_h$71. See **4.1.1.a** for details.	1

4.5.2. Output format

Name	Tag	Description	Size
TOF.DFR	$_h$t1	Desfire output format.	1

Same as Mifare Classic output format (see 4.3.2).

4.5.3. Output prefix

Name	Tag	Description	Size
PFX.DFR	$_h$t2	Desfire output prefix.	Var.

Same as ID-only output prefix (see 4.2.3).

4.5.4. Location of data

Name	Tag	Description	Size
LOC.DFR	$_h$t3	Location of data in Desfire card. See table **a** below.	8

a. Data location bytes

Offset	Length	Content
0	3	Application IDentifier (AID).
3	1	File IDentifier (FID). File must be a "standard data" file.
4	3	Offset of data in file.
7	1	Length of data to be read[24] (1 to 64).

Default value : unspecified.

Values are MSB first.

[24] Data will be truncated to the length specified in TOF.DFR, unless the long string reading extension is enabled.

4.5.5. T=CL options

Name	Tag	Description	Size
OPT.DFR	$_h$t4	Desfire T=CL options.	1

Same as 7816-4 T=CL options (see 4.5.5).

4.5.6. Authentication key

Name	Tag	Description	Size
AUT.DFR	$_h$t5	Desfire authentication key. See table **a** below.	9 or 17

Default value : absent

(No authentication is performed, plain read operation is used to fetch the data)

a. Authentication key bytes

Offset	Length	Content
0	1	Desfire key index and options. See table **b** below.
1	8 or 16	Key value (8 bytes for a DES key, 16 bytes for a 3-DES key).

b. Key index and options

Bit	Value	Meaning
7 – 6		**Communication mode for reading**
	00	Plain
	01	MACed with session key
	10	*RFU*
	11	Enciphered with session key
5 – 4		**Key diversification algorithm**
	00	Use the key "as is"
	01	Diversify the key using Desfire SAM algorithm
	10	Diversify the key using HMAC-MD5 algorithm
	11	*RFU*
3 – 0		**Index of key in Desfire application**
	0000 to 1110	Index of the key to be used for authentication
	1111	*RFU*

4.5.7. Reading a long string from a Desfire card

Note : This option is only available on Prox'N'Roll RFID Scanner, Automotive Reader, RDR-K632 and ProxRunner.

When bits 4 and 6 in TOF.DFR are set (ASCII output, long string reading extension enabled), the reader behaves as follow :

- The output length (bits 0 to 3 of TOF.DFR) is ignored,
- The reader reads the data up to the length specified in LOC.DFR (64 bytes max.),
- The reader returns those bytes as an ASCII string, truncated at the correct length when the end-of-string character ('\0' i.e. $_h$00) is reached.

Doing so, the reader is able to fetch ASCII strings up to 64 characters.

4.6. ISO 7816-4 Acceptance Template

4.6.1. Lookup list

Name	Tag	Description	Size
LKL.TCL	$_h$t0	7816-4 lookup list, $_h$11 ≤ value ≤ $_h$13. See **4.1.1.a** for details.	1

4.6.2. Output format

Name	Tag	Description	Size
TOF.TCL	$_h$t1	T=CL output format.	1

Same as Mifare Classic output format (see 4.3.2).

4.6.3. Output prefix

Name	Tag	Description	Size
PFX.TCL	$_h$t2	T=CL output prefix.	Var.

Same as ID-only output prefix (see 4.2.3).

4.6.4. Location of data

Name	Tag	Description	Size
LOC.TCL	$_h$t3	Offset of data in answer to APDU 3[25] (0 to 127).	1

Default value : 0.

4.6.5. T=CL options

Name	Tag	Description	Size
OPT.TCL	$_h$t4	T=CL (ISO/IEC 14443 layer 4) options. See table **a** below.	1

[25] Data will be truncated according to the length specified in TOF.TCL .

a. T=CL option bits

Bit	Value	Meaning
7 – 6		**Card to reader baudrate**
	00	No PPS, DSI = 106kbit/s
	01	Perform PPS, DSI = 212kbit/s if card allows it
	10	Perform PPS, DSI = 424kbit/s if card allows it
	11	Perform PPS, DSI = 848kbit/s if card allows it
5 – 4		**Reader to card baudrate**
	00	No PPS, DRI = 106kbit/s
	01	Perform PPS, DRI = 212kbit/s if card allows it
	10	Perform PPS, DRI = 424kbit/s if card allows it
	11	Perform PPS, DRI = 848kbit/s if card allows it
3 – 0		**Card identifier (CID)**
	0000	Empty CID = $_d$0
	0001 to 1110	CID from $_d$1 to $_d$14
	1111	CID is disabled

This tag exists only if T=CL card is selected in LST.

Default value : $_b$00001111

4.6.6. T=CL APDU 1

Typically this is a Select Application (or Select Applet) command.

May be absent if T=CL APDU 3 is sufficient to fetch the data.

Name	Tag	Description	Size
AU1.TCL	$_h$t5	TCL APDU 1.	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

4.6.7. T=CL APDU 2

Typically this is a Select File command.

May be absent if T=CL APDU 3 is sufficient to fetch the data.

Name	Tag	Description	Size
AU2.TCL	$_h$t6	TCL APDU 2.	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

4.6.8. T=CL APDU 3

APDU used to actually retrieve the data (typically this is a Read Binary command). Data have to be found in answer at offset specified in LOC.TCL.

Name	Tag	Description	Size
AU3.TCL	$_h$t7	TCL APDU 3.	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

4.6.9. Reading a long string from a T=CL card

Note : This option is only available on Prox'N'Roll RFID Scanner, Automotive Reader, RDR-K632 and ProxRunner.

When bits 4 and 6 in TOF.TCL are set (ASCII output, long string reading extension enabled), the reader behaves as follow :

- The output length (bits 0 to 3 of TOF.TCL) is ignored,
- The reader fetches the data from offset LOC.TCL up to the length of the response to APDU 3 (64 bytes max.),
- The reader returns those bytes as an ASCII string, truncated at the correct length when the end-of-string character ('\0' i.e. $_h$00) is reached.

Doing so, the reader is able to fetch ASCII strings up to 64 characters.

4.7. CALYPSO ACCEPTANCE TEMPLATE

This part deals with old Calypso cards, to be accessed only through the legacy Innovatron radio protocol.

New Calypso cards now support ISO/IEC 14443-B, and therefore can be accessed either through ID-Only or ISO/IEC 7816-4 templates.

Working with Calypso cards is subject to a specific licence fee. This function is therefore disabled in our readers, unless you order them with the Calypso option.

Depending on the specified options, this Calypso card processing template can retrieve :

- A 4-byte serial number (ID-Only template)
- Arbitrary data to be read in Calypso files (7816-4 template)

4.7.1. Lookup list

Name	Tag	Description	Size
LKL.CYO	$_h$t0	Calypso/Innovatron lookup list, value = $_h$72. See **4.1.1.a** for details.	1

4.7.2. Output format

Name	Tag	Description	Size
TOF.CYO	$_h$t1	Calypso/Innovatron output format.	1

Same as Mifare Classic output format (see 4.3.2).

4.7.3. Output prefix

Name	Tag	Description	Size
PFX.CYO	$_h$t2	Calypso/Innovatron output prefix.	Var.

Same as ID-only output prefix (see 4.2.3).

4.7.4. Location of data

Name	Tag	Description	Size
LOC.CYO	$_h$t3	Offset of data in answer to APDU 3[26] (0 to 64).	1

Default value : 0.

4.7.5. Calypso APDU 1

Typically this is a Select Application, or Select DF command.

Name	Tag	Description	Size
AU1.CYO	$_h$t5	Calypso/Innovatron APDU 1.	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

4.7.6. Calypso APDU 2

Typically this is a Select EF command.

Name	Tag	Description	Size
AU2.CYO	$_h$t6	Calypso/Innovatron APDU 2.	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

[26] Data will be truncated according to the length specified in TOF.CYO .

4.7.7. Calypso APDU 3

Typically this is a Read Binary command.

Name	Tag	Description	Size
AU3.CYO	$_h$t7	Calypso/Innovatron APDU 3	Var.

Card's Status Word is checked by the reader. A SW between $_h$9000 and $_h$9FFF is considered valid. Any other value for SW (and in particular error values as defined by ISO 7816-4 between $_h$6100 and $_h$6FFF) is considered as an error, and the reader will ignore the card.

Reader's internal buffer is limited to 128 bytes. If card's answer is longer, the answer will be discarded and the reader will ignore the card.

5. SERIAL PROTOCOL AND COMMAND SET

5.1. SERIAL OUTPUT FORMAT

5.1.1. Frame markers

Serial frame markers are configured by bits 7-5 of SER .

a. When addressing is disabled

Consider data '01 23 45 67',

- If bits 7-5 = $_b$000, frame is "01234567".
- If bits 7-5 = $_b$001, frame is "01234567<CR><LF>" where <CR> the ASCII carriage return ($_h$0D), and <LF> the ASCII line feed ($_h$0A).
- If bits 7-5 = $_b$010, frame is "<BEL>01234567<CR><LF>" where <BEL> is the ASCII bell (or ring) character ($_h$07), <CR> the ASCII carriage return ($_h$0D), and <LF> the ASCII line feed ($_h$0A).
- If bits 7-5 = $_b$011, frame is "<TAB>01234567<CR><LF>" where <TAB> is the ASCII horizontal tab character ($_h$09), <CR> the ASCII carriage return ($_h$0D), and <LF> the ASCII line feed ($_h$0A).
- If bits 7-5 = $_b$100, frame is "<STX>01234567<ETX>" where <STX> is the ASCII "start of text" character ($_h$02), and <ETX> the ASCII "end of text" ($_h$03).
- If bits 7-5 = $_b$101, frame is "<STX>01234567<ETX><CR><LF>".
- If bits 7-5 = $_b$110, frame is "<BEL><STX>01234567<ETX><CR><LF>".
- If bits 7-5 = $_b$111, frame is "<TAB><STX>01234567<ETX><CR><LF>".

b. When addressing is enabled

Consider data '01 23 45 67' and address 'a' ($_h$1 ≤ a ≤ $_h$E),

- If bits 7-5 = $_b$000, frame is "a>01234567".
- If bits 7-5 = $_b$001, frame is "a>01234567<CR><LF>".
- If bits 7-5 = $_b$010, frame is "<BEL>a>01234567<CR><LF>".
- If bits 7-5 = $_b$011, frame is "<TAB>a>01234567<CR><LF>".
- If bits 7-5 = $_b$100, frame is "<SOH>a><STX>01234567<ETX>" where <SOH> is the ASCII "start of header" character ($_h$01).
- If bits 7-5 = $_b$101, frame is "<SOH>a><STX>01234567<ETX><CR><LF>".
- If bits 7-5 = $_b$110, frame is "<BEL><SOH>a><STX>01234567<ETX><CR><LF>".
- If bits 7-5 = $_b$111, frame is "<TAB><SOH>a><STX>01234567<ETX><CR><LF>".

5.2. SERIAL INPUT

RDR-K632 accepts short commands from the host, typically to drive its LEDs.

RDR-K632 doesn't echo back the received data.

If the received command has been understood by **RDR-K632**, it replies with an <ACK> byte before executing the requested action.

Otherwise, it replies with a <NACK> byte.

5.2.1. When addressing is disabled

Command transmission format is <command> <CR> <LF>.

5.2.2. When addressing is enabled

Command transmission format is <address> **<** <command> <CR> <LF>, where <address> must be the address of the device.

5.2.3. List of commands

Command	Action
A0	Reader goes inactive (tag polling is halted)
A1	Reader goes active
R0	Switch red LED off
R1	Switch red LED on
R2	Red LED blinks slowly
R3	Red LED blinks quickly
G0	Switch green LED off
G1	Switch green LED on
G2	Green LED blinks slowly
G3	Green LED blinks quickly
M*rg*	Same as sending R*r* + G*g*
M*arg*	Same as sending A*a* + R*r* + G*g*
RST	Reset the reader
VER	Retrieve reader's version
SHO	Retrieve reader's settings

Choose appropriate configuration in CLD to allow the device to control its LEDs.

6. CONFIGURING RDR-K632

There are two ways to configure **RDR-K632** :

- Using a Master Card, formatted with **cfgfilecreator.exe** software. See chapters 7 and 8 for details,
- Manually, by entering configuration values in reader's console (serial line access), as shown in this chapter.

Whatever the hardware, default factory settings for **RDR-K632** firmware are :
- Serial communication, 38400bps,
- Reads any kind of ID, 8 byte fixed length output.

Always configure RDR-K632 properly before installation as there are little chances that default configuration matches your requirements.

6.1. CONNECTING RDR-K632 TO A COMPUTER

Please refer to chapters 2.1 and 2.2.

Enter `info` and check that communication with **RDR-K632** has been correctly established.

6.2. ENABLING CONFIGURATION COMMANDS

RDR-K632 configuration may be protected by a pin-code (if PIN configuration tag is empty, no pin-code is needed.

If defined to $_h$FFFF, configuration commands are permanently disabled).

Enter "`pinNNNN`" to allow configuration commands, where NNNN is the actual pin-code (for instance, "`pin1234`")[27].

6.3. ACCESSING RDR-K632 CONFIGURATION

6.3.1. Reading configuration tags

Enter "`cfg`" to list all configuration tags.

Enter "`cfgXX`" to read value configuration tag XX (hexadecimal address).

Note that configuration tags $_h$55, $_h$56 and $_h$6F (keys used by Master Cards and pin-code) are masked when read back.

[27] For security reasons, configuration commands are enabled only for 3 minutes. After 3 minutes of inactivity, you'll have to enter the pin-code again.

6.3.2. Writing configuration tags

Enter "cfgXX=YYYY" to update configuration tag XX (hexadecimal address) with value YYYY (hexadecimal value).

Enter "cfgXX=!!" to delete configuration tag XX (hexadecimal address).

6.3.3. Writing keys in RC's secure EEPROM

Enter "keya0=XXXXXXXXXXXX" to update key A at index 0, "keya1=..." to update key A at index 1, and so on until "keyaf=...".

Enter "keyb0=XXXXXXXXXXXX" to update key B at index 0, "keyb1=..." to update key B at index 1, and so on until "keybf=...".

Note that keys stored in RC can't be read back.

6.3.4. Reading RC's 4-byte EEPROM

RC's chipset includes a 4-byte EEPROM to store a configuration value.

Enter "cfgRC" to read this 4-byte value.

6.3.5. Writing RC's 4-byte EEPROM

RC's chipset includes a 4-byte EEPROM to store a configuration value.

Enter "cfgRC=XXXXXXXX" to write this 4-byte value.

Content of RC's 4-byte EEPROM is currently not used by **RDR-K632** firmware.

Please keep this value to 00000000 as it may be used in future versions.

6.4. APPLYING NEW CONFIGURATION

New configuration is applied only after reset.

Cycle power or enter "rst" to reset the reader.

6.5. REVERTING TO DEFAULT

Sometimes it is necessary to put reader back in "out-of-factory" configuration (for instance when reader goes from one site to another). This is done easily by erasing all tags from reader's memory.

Enter "`cfg!!=!!`" to delete all configuration tags.

There's neither confirmation prompt nor any kind of "are you sure?" popup window. Erasing everything is immediate and unrecoverable.

Erasing all the configuration tags is not really enough to put the reader(s) back in out-of-factory configuration, since Mifare keys stored in RC's secure EEPROM are not erased.

Read paragraph 3.5.3 to see how the keys may be overwritten.

7. WORKING WITH MASTER CARDS

7.1. OVERVIEW

Master Cards for **SpringCard RFID Scanners** are NXP Desfire 4k (MF3ICD40 or MF3ICD41). You may buy them from **SpringCard** or any other NXP reseller.

SpringCard SQ844P is a software package featuring :

- A command line utility, that creates the Master Cards from a Master Configuration File, and using a SpringCard contactless reader/writer[28]
- A wizard (HTML page) that helps authoring the Master Configuration File.

SpringCard SQ844P also includes various configuration files, that show typical configuration for Prox'N'Roll RFID Scanner, IWM-K632, FunkyGate, RDR-K632, ProxRunner, Automotive Reader, etc.

SpringCard SQ844P is available only for Microsoft Windows systems.

a. Downloading and installing

Go to **www.springcard.com/download/sdks.html** and download latest version of package **sq884p**.

Double-click the downloaded file to launch the installer, and follow the wizard.

b. The cfgfilecreator.exe command line utility

cfgfilecreator.exe is a Windows command line software.

Enter **cfgfilecreator.exe -h** to read the complete list of command line switches and options, and the complete list of sections and variables for configuration files.

cfgfilecreator.exe software comes with various sample configuration files that show typical configurations of IWM-K632, FunkyGate, Prox'N'Roll RFID Scanner, etc.

[28] **SpringCard Prox'N'Roll PC/SC** (or Legacy) typically. CSB4 or any product in the CSB6 family may be used to create Master Cards too.

c. The cfgfilecreator.exe web page

cfgfilecreator.html is a standalone web page that helps creating configuration files for **cfgfilecreator.exe** .

7.2. CONFIGURATION FILES

cfgfilecreator.exe uses a configuration file to retrieve configuration data to be written into the Master Card.

Configuration files are written like standard Windows "INI" files. They can be created using Notepad or any other text editor, or using **cfgfilecreator.html** .

Each line of each section uses the format "name=value" where "name" is either the name or the tag of the configuration variable (e.g. either "opt" or "60"), and "value" its value in hexadecimal.

7.2.1. The "general" section

This section maps to tags $_h$60 to $_h$6F. Default content is :

```
[general]
opt=0C      ; value for OPT
odl=02      ; value for ODL
rdl=0A      ; value for RDF
cld=0F      ; value for CLD
cbz=13      ; value for CBZ
wgd=0A      ; value for WGD
dtc=0A      ; value for DTC
```

```
ser=C5      ; value for SER
shd=00      ; value for SHD
pin=0000    ; value for PIN
```

7.2.2. The "rckeys" section

This section holds the Mifare access keys to be written in RC's secure EEPROM.

Type A keys are named "a0" to "a15", and type B keys "b0" to "b15".

Here's an example of content :

```
[rckeys]
a0=A0A1A2A3A4A5 ; Mifare type A base key (for MAD)
a1=FFFFFFFFFFFF ; NXP transport key
a2=000000000000 ; other transport key
a3=CCCCCCCCCCCC ; unused
(...)
a15=CCCCCCCCCCCC ; unused
b0=B0B1B2B3B4B5 ; Mifare type B base key (for MAD)
b1=FFFFFFFFFFFF ; NXP transport key
b2=000000000000 ; other transport key
b3=CCCCCCCCCCCC ; unused
(...)
b15=CCCCCCCCCCCC ; unused
```

This section (and each line in it) is optional. Only keys listed in this section will be written, other keys will be left unchanged.

7.2.3. Sections for Card Processing Templates

SpringCard RFID Scanners run 1 to 4 card accepting templates.

Each template is configured by sections "tpl1", "tpl2", "tpl3" and "tpl4" respectively.

Mandatory and optional content for each section depends on the card lookup list (LKL field) of the section itself.

a. ID-Only example

This sample section configures template 4 to read any kind of ID. Output format is : 8-byte fixed length, prefixed by the string "ID=" :

```
[tpl4]
lkl=0F                  ; wants any kind of ID
tof=82                  ; 8-byte output, swap 14443 A short IDs
pfx=49443D              ; prefix = "ID="
```

b. Desfire example

This sample section configures template 1 to read 8 bytes of data from a Desfire card. Output format is : 8-byte fixed length, no prefix :

```
[tpl1]
lkl=71                  ; wants Desfire cards
tof=02                  ; 8-byte output
pfx=                    ; no prefix
loc=123456 01 000100 08 ; 8 bytes of data to be read in application
                        ; 0x123456, field 0x01, at offset 0x000100
```

```
aut=00 A0A1A2A3A4A5A7    ; authentication with key 0, plain comm.
                         ; mode, no diversification. Key is a single
                         ; DES key (8 bytes)
```

7.2.4. Master Cards related sections

a. Specifying a new configuration for future Master Cards

The "tpl5" section allows to update the card processing template reserved to Master Cards. See paragraph 7.4.1 for details.

```
[tpl5]
aut=E0 xx...xx        ; 16-byte authentication key
```

This 16-byte authentication key in the "tpl5" section is the one that will be written in the reader(s) by the Master Card.

It is not the key that will be used to create the Master Card itself.

b. Specifying configuration to be used by current Master Card

The "master" section defines how the Master Card shall be created. See paragraph 7.4.2 for details.

```
[master]
aut=E0 xx...xx        ; 16-byte authentication key
```

This 16-byte authentication key in the "master" section is the one that will be used to create the Master Card.

It has no impact on the key written in the reader(s).

7.3. OPERATION INSTRUCTIONS

- Open **Configuration files creator** (**cfgfilecreator.html**) (on Windows : Start Menu → All Programs → SpringCard → Configuration Tools),
- Create your configuration file and save it in the directory where **cfgfilecreator.exe** is installed, for instance with the name *siteconf.ini* (on Windows : C:\Program Files\SpringCard\SQ844P),
- Open **Configuration tools directory** (on Windows : Start Menu → All Programs → SpringCard → Configuration Tools),
- Plug and power-on your Prox'N'Roll PC/SC (or legacy),
- Put a virgin Desfire card on the Prox'N'Roll PC/SC (or legacy),
- Enter **cfgfilecreator.exe –c *siteconf.ini***,
- Wait until Master Card is written.

If the Desfire card is not virgin, the **software will try to format it** (i.e. erase the whole file structure with all the data) **without prior notification**.

Be sure to put on the reader only a virgin card, or an old Master Card to be overwritten.

You've been warned…

7.4. CHANGING AUTHENTICATION KEY FOR MASTER CARDS

All **SpringCard** products ship with the same out-of-factory authentication key. To secure their site, customers should replace the default key by their own key before installing the readers.

SpringCard recommends making (and keeping) at least two distinct Master Cards for each customer or site :

- ***1st level Master Card*** alters only the authentication key (replace default key by site specific key).
  - All readers bought for this site shall be configured using this *1st level Master Card* as soon as they are received.
- ***2nd level Master Card*** actually configures the reader (card processing templates, output mode and format, and so on).
  - It uses the site specific key for authentication, but doesn't update the key that is already inside the reader.
  - The *2nd level Master Card* shall be used during installation and whenever you wish to change reader configuration.

Note that more than one *2nd level Master Cards* can be created (one for each kind of output settings, one for each people in charge of installation…) whereas only one *1st level Master Card* should be created and be kept in a secure place[29].

Be sure to remember the new authentication key you put in a reader. If you forget the authentication key, and forget the pin-code (or define pin-code to hFFFF), it will be impossible to change reader configuration again !

You've been warned…

7.4.1. Creating a first level Master Card

- Create a configuration file (say, "*master.ini*") with only those 4 lines :

```
[master]
; Master section is empty, we use SpringCard's default keys

[tpl5]
aut=E0 xx...xx
```

where *xx…xx* is the site specific 16-byte authentication key[30],

- Put a virgin card on the Prox'N'Roll, label it "1st level Master Card",
- Enter **cfgfilecreator.exe –c *master.ini*** ,
- Use this Master Card to write the new authentication key in the reader(s).

7.4.2. Creating a second level Master Card

- Create a complete configuration file as seen earlier .
- Terminate the file with those 4 lines :

```
[master]
aut=E0 xx...xx

[tpl5]
; Template 5 section is empty, we keep current keys in the reader
```

where *xx…xx* is the site specific 16-byte authentication key,

- Put a virgin card on the Prox'N'Roll, label it "2nd level Master Card",
- Enter **cfgfilecreator.exe –c *siteconf.ini*** ,
- Use this Master Card to write complete configuration in the reader(s).

[29] That's because *1st level Master Card* has got the authentication key written in it, and anybody may retrieve it using **cfgfilecreator** software, as the authentication key is only used to secure *2nd level Master Cards* and is not written in them.

[30] This is key 0 inside Master Card application; the key will be diversified using HMAC-MD5 algorithm, so the "E0" header is mandatory.

7.5. REVERTING TO DEFAULT

Sometimes it is necessary to put reader back in "out-of-factory" configuration (for instance when reader goes from one site to another). This is done easily by erasing all tags from reader's memory.

- Create a configuration file (say, "*factory.ini*") with only those 3 lines :

```
[master]
aut=E0 xx...xx
clear=1
```

where *xx…xx* is the site specific 16-byte authentication key

- Put a virgin card on the Prox'N'Roll, label it "Erase all Master Card",
- Enter **cfgfilecreator.exe –c *factory.ini***
- Use this Master Card to put the reader(s) back in out-of-factory configuration.

Erasing all the configuration tags is not really sufficient to put the reader(s) back in out-of-factory configuration, since Mifare keys stored in RC's secure EEPROM are not erased.

Just add an "rckeys" section, with dummy keys, to overwrite those keys.

8. SPECIFICATION OF MASTER CARDS

This chapter is provided as a mean for security experts to evaluate the Master Card architecture of **SpringCard RFID Scanners**.

Customers do not need to implement this part themselves, since **cfgfilecreator.exe** software is a convenient tool to create Master Cards. See chapter 7 for details.

8.1. BUILDING A MASTER CARD

- The Master Card must be a Desfire 4k,
- The reader tries to fetch configuration data from Desfire cards according to the Master Card template specified in next paragraph. Data are protected by an authentication key that may be changed on a per-customer or per-site basis (i.e. Master Cards belonging to customer X will not work on customer Y's readers),
- Before storing new settings in its non-volatile memory, the reader checks that data comes with a valid digital signature. The signing key can't be changed, and is only known by **SpringCard**'s software. This ensures that only data that has been pre-validated by genuine software can be loaded in reader's non-volatile memory.

8.2. TEMPLATE FOR MASTER CARDS

8.2.1. Location of data

Name	Tag	Description	Size
LOC.MAS	$_h$53	Location of data in master cards. See table **a** below.	5

a. Data location bytes

Offset	Length	Content	Specified value
0	3	Application IDentifier (AID).	$_h$504143
3	1	File IDentifier (FID) for configuration data.	$_h$01
4	1	File IDentifier (FID) for digital signature.	$_h$02

8.2.2. Authentication key

Out-of-factory key used for authentication of Master Cards is confidential.

Only **SpringCard** genuine software –such as **cfgfilecreator.exe**– is able to create Master Cards with the default authentication key.

To secure their installation, customers should replace this key as soon as they receive the readers, as explained in 7.4 .

This is the same structure as AUT.DFR .

Name	Tag	Description	Size
AUT.MAS	$_h$55	Authentication key. See table **a** below.	17

a. Authentication key bytes

Offset	Length	Content
0	1	Authentication key index and options. See table **b** below.
1	16	***Authentication key for Master Cards*** (this is 3-DES key).

b. Authentication key index and options

Bit	Value	Meaning
7 – 6		**Communication mode in read operation**
	00	Plain
	01	MACed with session key
	10	*RFU*
	11	Enciphered with session key
5 – 4		**Key diversification algorithm**
	00	Use the key "as is"
	01	Diversify the key using Desfire SAM algorithm
	10	Diversify the key using HMAC-MD5 algorithm
	11	*RFU*
3 – 0		**Index of key in Desfire application**
	0000 to 1110	Index of the key to be used for authentication
	1111	*RFU*

Specified value : $_h$E0 *(key 0, HMAC-MD5 diversification, ciphered reading)*

8.2.3. Signing key

Name	Tag	Description	Size
SGN.MAS	$_h$56	Signing key. See table **a** below.	17

Key used for digital signature of master cards is confidential.

Only **SpringCard** genuine software –such as **cfgfilecreator.exe**– is able to sign the Master Cards[31].

Customers shall not try to change this parameter, unless advised to by **SpringCard**.

a. Signing key bytes

Offset	Length	Content
0	1	Index and options. See table **b** below.
1	16	***Key data*** (this is 128-bits key).

b. Signing key index and options

Bit	Value	Meaning
7 – 6	00	*Those bits are RFU and must be 00*
5 – 4		**Key diversification algorithm**
	00	Use the key "as is"
	01	Diversify the key using Desfire SAM algorithm
	10	Diversify the key using HMAC-MD5 algorithm
	11	*RFU*
3 – 0	0000	*Those bits are RFU and must be 00*

Specified value : $_h$20 *(HMAC-MD5 diversification)*

8.3. DATA STRUCTURE

8.3.1. Size of file

File holding configuration data and Mifare keys (offset 3 in LOC.MAS) must be exactly 512-byte long. In case used size is shorter than 512 bytes, file must be padded with $_h$00.

8.3.2. Configuration data

The configuration data block uses the T,L,V (tag, length, value) encoding scheme.

- Tag is 1 byte-wide,
- Len is 1 byte-wide,
- Value is 0 to 24 byte-wide.

[31] This choice has been done to ensure that data inside the Master Card have been pre-validated according to reader specifications, and have not been corrupted afterwards.

Items found in T,L,V blocks will overwrite data with the same tag already present in reader's non-volatile memory.

Set Len = 0 to delete an existing tag from the non-volatile memory, without replacing it.

Last T,L,V of the configuration data block must be the (valid) signature of the whole block, according to the HMAC-MD5 digital signature algorithm specified in next chapter.

8.3.3. Mifare keys to be loaded into RC's secure EEPROM

Keys to be loaded into RC's secure EEPROM use the T,L,V scheme, as follow :

- Tag (1 byte) = $_h$80 + key index (see chapter "Mifare Classic Card Acceptance Template"),
- Len (1 byte) = $_h$06,
- Value is the Mifare key (6 bytes exactly).

8.4. DIGITAL SIGNATURE

8.4.1. Size of file

File holding the signature (offset 4 in LOC.MAS) must be exactly 16-byte long.

8.4.2. Algorithm

This is the signature algorithm when default parameters in SGN.KEY are used :

- Let *Content* be the 512-byte configuration block as written in the card[32],
- Let *SignKey* be the 16-byte key,
- Diversify *SignKey* from card's UID, using HMAC-MD5 diversification algorithm[33] to get *DivKey*,
- Compute *Sign* = HMAC-MD5 (*Block*) using *DivKey* [34].

The value of *SignKey* is confidential. Customers shall not try to change the key, nor the signature algorithm.

[32] This is the configuration data plus the Mifare keys to be loaded into RC's secure EEPROM. Total size is up to 512 bytes. Note that signature is computed over the whole file, including its padding, whatever the used length is.

[33] See next chapter "Security algorithms"

[34] See next chapter "Security algorithms"

9. SECURITY ALGORITHMS

9.1. HMAC SIGNATURE AND KEY DIVERSIFICATION

9.1.1. Abstracts

A message authentication code, or MAC, is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and a message, and outputs a MAC that protects both message's integrity and authenticity.

An HMAC (or keyed-hash message authentication code) is a type of MAC function were a cryptographic hash function is used to compute the output.

a. HMAC algorithm

$$\mathrm{HMAC}_K(m) = h\left((K \oplus \mathrm{opad}) \| h\left((K \oplus \mathrm{ipad}) \| m\right)\right),$$

Where *h* is the hash function, *K* is the secret key padded with extra zeros up to 64 bytes, *m* is the message to be authenticated. *opad* is the value $_h$5C repeated 64 times, and ipad the value $_h$36 repeated 64 times.

b. HMAC-MD5

HMAC-MD5 is a particular HMAC function where *h* is the MD5 standard function, as defined by RSA laboratories. Size of HMAC is 16 bytes exactly.

In the **SpringCard RFID Scanners** family, we use HMAC-MD5 for both signature and key diversification.

9.1.2. HMAC-MD5 for digital signature

HMAC protects both message's integrity and authenticity, so it can be considered as a digital signature[35].

IWM implementation allows only 16-byte keys. The key can be used "as is" or be the result of a diversification from a master key.

9.1.3. HMAC-MD5 for key diversification

In this particular mode, we name *K* the "master key" and we compute the HMAC over card's identifier to establish a "diversified key" *Ku*.

[35] Literature often reserve the name "digital signature" to public key schemes, where verifier doesn't need to know signer's private key to verify the signature. HMAC is a scheme where signer and verifier must share the same secret key.

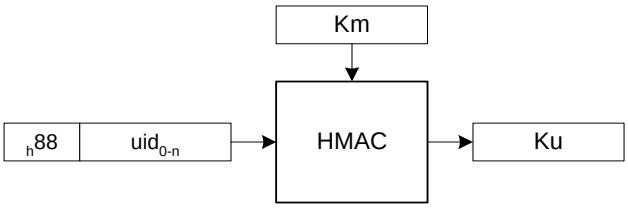
a. DES or Triple-DES key diversification

The algorithm takes as inputs :

- A 16-byte master key (Km)
- The card serial number (uid)[36]

It provides as output :

- The 16-byte diversified key specific to this card (Ku).



The diversified key can now be used either for Desfire authentication, or for HMAC-MD5 signature.

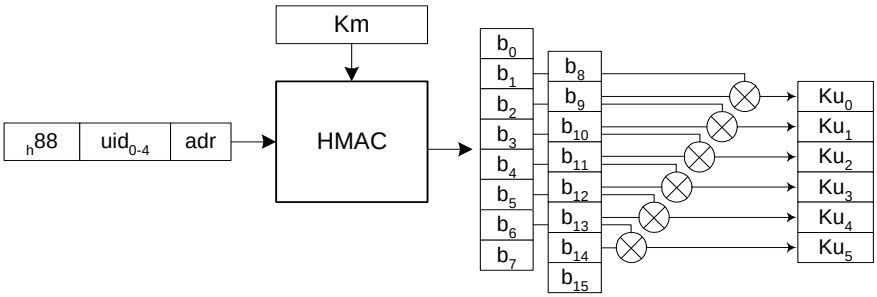
b. Mifare key diversification

The algorithm takes as inputs :

- A 16-byte master key (Km)
- The 4-byte card serial number (uid)
- The 1-byte block address (adr)

It provides as output :

- The 6-byte Mifare key specific to the couple card + address (Ku).



Note : the *adr* parameter is the either the sector number (not the block) number) or fixed to h00, depending on the configuration in the Mifare Classic Card Acceptance Template.

[36] The UID is 7-byte long for a Desfire card, 4-byte long for a Mifare card. The same diversification algorithm is usable whatever the length is.

9.2. DESFIRE SAM / RC171 KEY DIVERSIFICATION

9.2.1. DES or Triple DES key diversification

The key diversification algorithm described here is the one provided by Desfire SAM. Please refer to the corresponding datasheet for details.

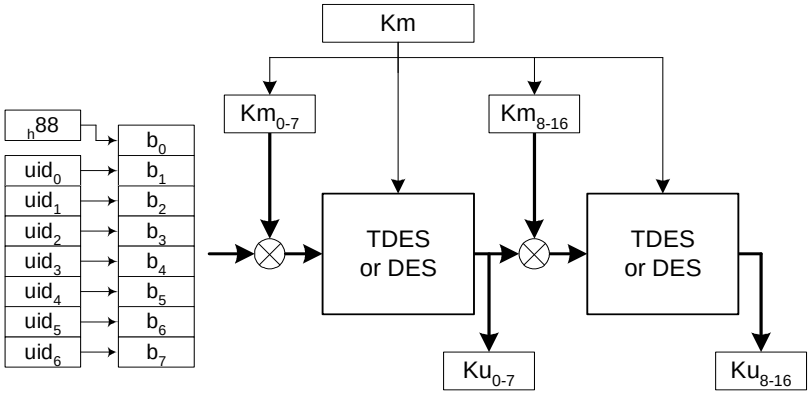
The algorithm takes as inputs :

- A 16-byte Triple-DES master key (Km)[37]
- The 7-byte card serial number (uid)

It provides as output :

- The 16-byte diversified key specific to this card (Ku).

Here's the flowchart :



The diversified key now is used for Desfire authentication.

9.2.2. Mifare key diversification

The Mifare diversification algorithm described here is provided both by Desfire SAM and by NXP RC171 coprocessor. Please refer to the corresponding datasheets for details.

a. Basis

The algorithm takes as inputs :

- A 6-byte master key (Km)
- A 16-byte Triple-DES diversification key (Kd)[38]

[37] If both halves are equals, the key maps to a single DES key

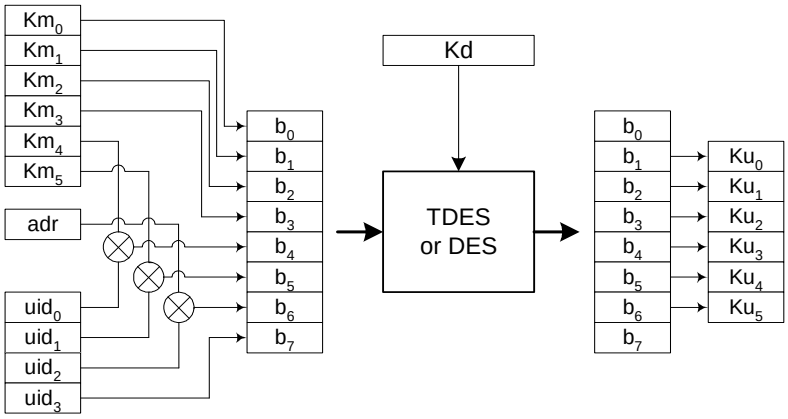
[38] If both halves are equals, the key maps to a single DES key

- The 1-byte block address (adr)
- The 4-byte card serial number (uid)

It provides as output :

- The 6-byte Mifare key specific to the couple card + address (Ku).

Here's the flowchart :



b. Diversification based on UID only

If this option is selected, the *adr* input parameter is fixed to $_h$00 whatever the block to be read is.

c. Diversification based on UID and address

If this option is selected, the *adr* input parameter is the Mifare sector number (not the block).

Here's an example with a Mifare 1k card :

- Data is located on block 29,
- Block 29 belongs to sector 7 (29 / 4),
- The diversification algorithm will be fed with adr = 7.

Here's an example with a Mifare 4k card :

- Data is located on block 231,
- Block 231 belongs to sector 38 (32 + (231-128) / 16),
- The diversification algorithm will be fed with adr = 38.

DISCLAIMER

This document is provided for informational purposes only and shall not be construed as a commercial offer, a license, an advisory, fiduciary or professional relationship between PRO ACTIVE and you. No information provided in this document shall be considered a substitute for your independent investigation.

The information provided in this document may be related to products or services that are not available in your country.

This document is provided "as is" and without warranty of any kind to the extent allowed by the applicable law. While PRO ACTIVE will use reasonable efforts to provide reliable information, we don't warrant that this document is free of inaccuracies, errors and/or omissions, or that its content is appropriate for your particular use or up to date. PRO ACTIVE reserves the right to change the information at any time without notice.

PRO ACTIVE does not warrant any results derived from the use of the products described in this document. PRO ACTIVE will not be liable for any indirect, consequential or incidental damages, including but not limited to lost profits or revenues, business interruption, loss of data arising out of or in connection with the use, inability to use or reliance on any product (either hardware or software) described in this document.

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products may result in personal injury. PRO ACTIVE customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify PRO ACTIVE for any damages resulting from such improper use or sale.

COPYRIGHT NOTICE

All information in this document is either public information or is the intellectual property of PRO ACTIVE and/or its suppliers or partners.

You are free to view and print this document for your own use only. Those rights granted to you constitute a license and not a transfer of title: you may not remove this copyright notice nor the proprietary notices contained in this document, and you are not allowed to publish or reproduce this document, either on the web or by any mean, without written permission of PRO ACTIVE.

EDITOR'S INFORMATION

PRO ACTIVE SAS company with a capital of 227 000 €
RCS EVRY B 429 665 482
Parc Gutenberg, 13 voie La Cardon
91120 Palaiseau – France