



PMA13257-CA
FINAL - PUBLIC

SPRINGCARD FUNKYGATE-IP NFC

Integration and Configuration Guide

DOCUMENT IDENTIFICATION

Category	Owner's Manual		
Family/Customer	FunkyGate NFC Series		
Reference	PMA13257	Version	CA
Status	Final	Classification	Public
Keywords			
Abstract			

File name	V:\Dossiers\SpringCard\A-Notices\RFID scanners et lecteurs\FunkyGate-IP\[PMA13257-CA] FunkyGate-IP NFC Integration and Configuration Guide.odt		
Date saved	24/02/17	Date printed	25/07/16

REVISION HISTORY

Ver.	Date	Author	Valid. by		Approv. by	Details
			Tech.	Qual.		
AA	29/09/13	JDA				Created from PMA959P
AB	24/04/14	JDA				Rewritten the authentication scheme
AC	28/05/14	JDA				Added the HTTP server and the REST API
BA	30/07/14	JDA			JDA	Network part moved to PMA14166
BB	29/07/15	JIZ				Changed reset command: §7.2.1 and §7.4.3
CA	08/07/16	JDA				Added the HTTP client

CONTENTS

1. INTRODUCTION.....	6	7.2.2. Data-field identifiers (Reader → Host).....	30
1.1. ABSTRACT.....	6	7.3. HOST → READER, BASIC OPERATIONS.....	31
1.2. AUDIENCE.....	6	7.3.1. Get Global Status.....	31
1.3. SUPPORT AND UPDATES.....	6	7.3.2. Start/Stop Reader.....	31
1.4. RELATED DOCUMENTS.....	7	7.3.3. Clear LEDs command.....	32
1.4.1. Products' specifications.....	7	7.3.4. Set LEDs command.....	32
1.4.2. Common documentations.....	7	7.3.5. Start LED sequence command.....	32
2. DEFINE THE READER'S IP ADDRESS.....	8	7.3.6. Buzzer command.....	33
2.1. ASSIGN AN IP ADDRESS USING NDDU SOFTWARE.....	8	7.4. HOST → READER, RESTRICTED OPERATIONS.....	34
2.1.1. Download and install the NDDU software.....	8	7.4.1. Write Configuration Register.....	34
2.1.2. Run the NDDU software.....	8	7.4.2. Erase Configuration Register.....	34
2.1.3. Discovered devices.....	9	7.4.3. Reset the Reader.....	34
2.1.4. Configure a Reader.....	10	7.5. READER → HOST.....	35
2.1.5. Verify the new configuration.....	12	7.5.1. Reader Identifier.....	35
2.2. ASSIGN AN IP ADDRESS USING A MASTER CARD.....	13	7.5.2. Tamper Status.....	35
3. TELNET ACCESS TO THE READER.....	14	7.5.3. Card Read.....	35
3.1. READER'S CONSOLE.....	14	7.5.4. Card Inserted.....	35
3.1.1. Open a Telnet session to the Reader.....	14	7.5.5. Card Removed.....	36
3.1.2. Sending a command to the Reader.....	15	8. EDITING READER'S CONFIGURATION.....	37
3.1.3. List of Console commands.....	16	8.1. THROUGH THE TELNET LINK.....	37
4. USING THE READER IN HTTP CLIENT MODE.....	17	8.1.1. Reading Configuration Registers.....	37
4.1. ABSTRACT.....	17	8.1.2. Writing Configuration Registers.....	38
4.2. ENABLING AND CONFIGURING THE HTTP CLIENT.....	18	8.2. USING MASTER CARDS.....	38
4.3. LIMITATIONS.....	18	8.3. THROUGH THE SPRINGCARD NETWORK DEVICE C/S PROTOCOL.....	38
4.4. HTTP CLIENT – POST REQUEST.....	19	9. GLOBAL CONFIGURATION OF THE READER.....	39
4.5. HTTP CLIENT – JSON RESPONSE.....	20	9.1. GENERAL OPTIONS.....	39
5. USING THE READER IN HTTP SERVER MODE – REST API.....	21	9.2. DELAYS AND REPEAT.....	40
5.1. ABSTRACT.....	21	9.3. LEDs AND BUZZER.....	40
5.2. ENABLING THE HTTP SERVER.....	21	9.4. SECURITY OPTIONS.....	42
5.3. LIMITATIONS.....	21	9.5. TCP CONFIGURATION.....	43
5.4. REST API – FUNCTION LIST.....	22	9.5.1. IPv4 address, mask, and gateway.....	43
5.5. REST API – POLLING LOOP.....	23	9.5.2. SpringCard Network Device C/S Protocol – Server port.....	44
5.5.1. iwmm2/read and iwmm2_cb/read.....	23	9.5.3. SpringCard Network Device C/S Protocol – Security settings and authentication keys.....	44
5.5.2. iwmm2/read/keep and iwmm2_cb/read/keep.....	24	9.5.4. SpringCard Network Device C/S Protocol – Operation Key.....	44
5.6. REST API – SENDING COMMANDS TO THE READER.....	25	9.5.5. SpringCard Network Device C/S Protocol – Administration Key.....	44
5.6.1. iwmm2/buzz and iwmm2_cb/buzz.....	25	9.5.6. HTTP client configuration.....	45
5.6.2. iwmm2/led and iwmm2_cb/led.....	25	9.5.7. HTTP client – server name.....	45
5.6.3. iwmm2/leds and iwmm2_cb/leds.....	27	9.5.8. HTTP client – query string.....	45
5.7. REST API – ERRORS.....	27	9.5.9. Ethernet configuration.....	46
6. SPRINGCARD NETWORK DEVICE C/S PROTOCOL.....	28	9.5.10. Info / Location.....	46
6.1. ABSTRACT.....	28	9.5.11. Password for Telnet access.....	47
7. SPRINGCARD NETWORK DEVICE – READER APPLICATION LAYER.....	29	10. THE TEMPLATE SYSTEM.....	48
7.1. PRINCIPLES.....	29	11. 3RD-PARTY LICENSES.....	49
7.2. LIST OF OPERATION-CODES AND DATA-FIELD IDENTIFIERS.....	30	11.1. FREERTOS.....	49
7.2.1. Operation-codes (Host → Reader).....	30	11.2. uIP.....	49

1. INTRODUCTION

1.1. ABSTRACT

SpringCard FunkyGate-IP NFC is a RFID (13.56MHz) and NFC wall-mount Reader, for access control applications. **SpringCard FunkyGate-IP NFC** features an exclusive TCP/IP over Ethernet interface.

The attractive styling and the efficiency of the Ethernet interface make it the preferred choice for corporate environments. Advanced support of the widest range of technologies and exclusive security features allow high-end access control schemes to be deployed seamlessly.

Thanks to a **versatile Template System** (shared with all other **SpringCard** Readers and RFID/NFC Scanners), **SpringCard FunkyGate-IP NFC** is able to read either a serial number or virtually any data coming from standard ISO/IEC 14443 proximity cards, ISO/IEC 15693 vicinity labels or tags. It is also able to fetch NDEF data from RFID chips formatted according to one the NFC Forum Tag specifications, and to receive NDEF data from a NFC Forum “peer-to-peer” (SNEP server on top of LLCP).

The **SpringCard FunkyGate-IP+POE NFC** adds the “powered by the network” (POE) feature.

This document provides all necessary information to configure both the **FunkyGate-IP NFC** and **FunkyGateIP-POE + NFC** Readers, and to develop a software that will handle data coming from the Reader, and to drive or re-configure the Reader when needed.

1.2. AUDIENCE

This manual is designed for use by application developers and system integrators. It assumes that the reader has a good knowledge of computer development, TCP/IP networks, and a good knowledge of the RFID/NFC technologies.

1.3. SUPPORT AND UPDATES

Useful 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 are posted on this web site as soon as they are available.

For technical support enquiries, please refer to SpringCard support page, on the web at

www.springcard.com/support

1.4. RELATED DOCUMENTS

1.4.1. Products' specifications

You'll find the feature-list and the technical characteristics of every product in the corresponding leaflet.

Document ref.	Content
PFL13276	FunkyGate NFC family leaflet

1.4.2. Common documentations

a. Network integration and configuration

SpringCard FunkyGate-IP NFC Reader shares the same network communication protocol (on top of TCP/IP) and the same way of configuring the network as **SpringCard HandyDrummer-IP I/O Module**. A document share among both products covers this part.

Document ref.	Content
PMA14166	FunkyGate-IP NFC, E663/RDR, HandyDrummer-IP, E663/MIO Network Integration and Configuration

b. Card reading & processing

All SpringCard Readers and RFID Scanners products share the same "card processing" system through 1 to 4 processing templates. How the Reader process the card is therefore detailed in a document shared among all products in the family.

Document ref.	Content
PMA13205	Readers / RFID Scanners Template System

2. DEFINE THE READER'S IP ADDRESS

The Reader comes out of factory without an IP address. This means that you must assign it an IP address before being able to access it either through Telnet link (chapter 3) or using the TCP client/server protocol depicted in chapter 6.

Using **SpringCard Network Device Discovery Utility (NDDU)** is the preferred method to assign an IP address to the Reader.

This Reader does not support the Dynamic Host Configuration Protocol (DHCP). Only fixed IPv4 addresses are supported.

2.1. ASSIGN AN IP ADDRESS USING NDDU SOFTWARE

SpringCard Network Device Discovery Utility (NDDU) is a Windows-based software that discovers and configures SpringCard Device connected on same the Local Area Network (LAN) as the computer it is running on.

Please use a wired network connection, and make sure the Reader(s) you want to configure are on the same LAN as your computer. NDDU makes use of broadcast UDP frames to discover and configure the Readers; therefore, it won't work behind a router or gateway.

2.1.1. Download and install the NDDU software

Make sure your Windows account has administrative privileges.

Download the installer from URL

www.springcard.com/download/find/file/sn13210

Install the software.

This software relies on the .NET framework version 4. Please download and install this framework from Microsoft's in case it hasn't already been deployed onto your computer.

2.1.2. Run the NDDU software

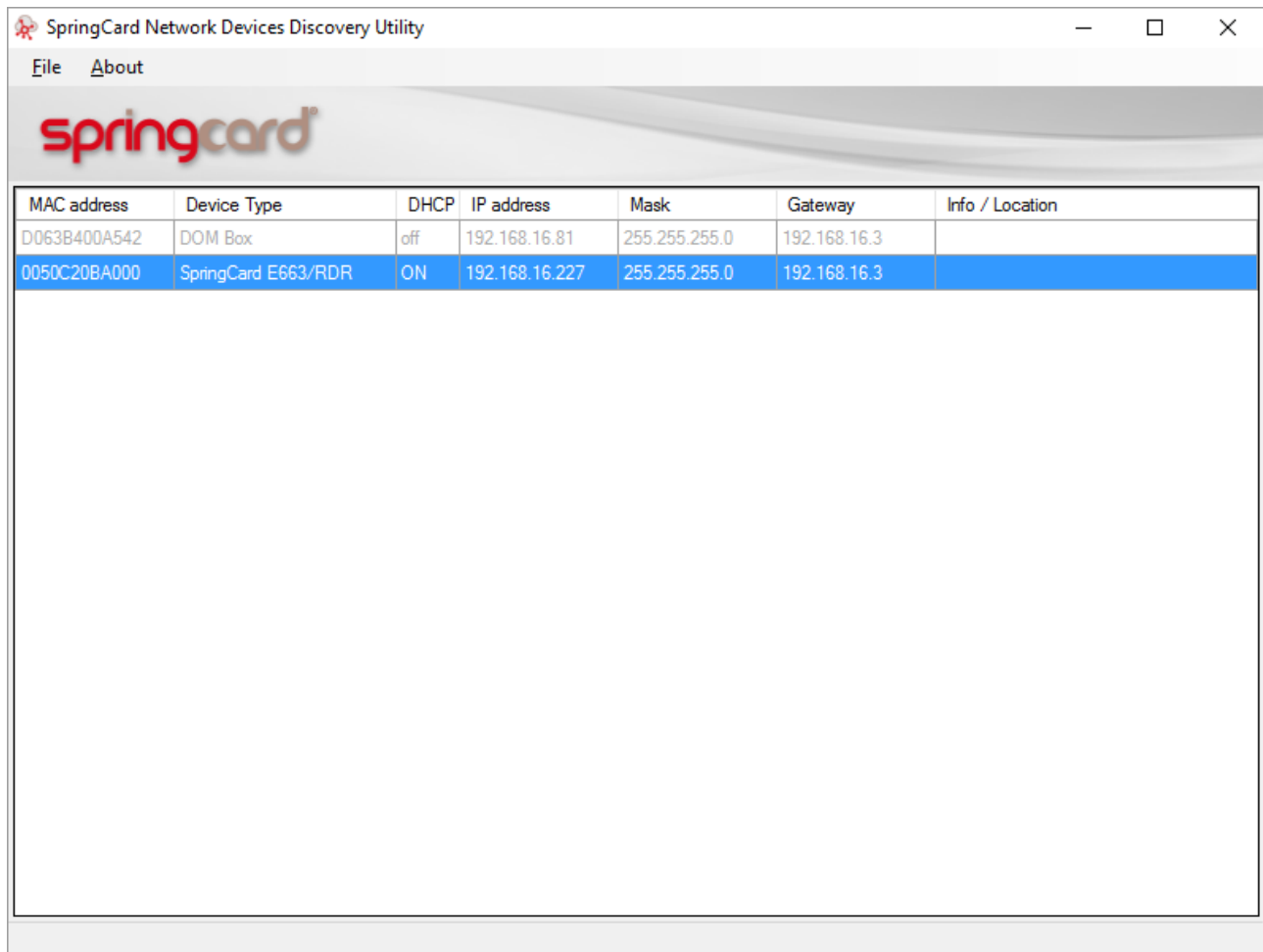
Make sure your Windows account has administrative privileges.

Launch the software: Start Menu → SpringCard → Network Discovery → Network Device Discovery Utility.

On first startup, you should be prompted by Windows Firewall whether you want to allow NDDU to access the network. Please confirm.

2.1.3. Discovered devices

After a few seconds, NDDU displays the list of devices it has found on the LAN.



MAC address	Device Type	DHCP	IP address	Mask	Gateway	Info / Location
D063B400A542	DOM Box	off	192.168.16.81	255.255.255.0	192.168.16.3	
0050C20BA000	SpringCard E663/RDR	ON	192.168.16.227	255.255.255.0	192.168.16.3	

The software's main screen shows 7 columns:

- The MAC address (Ethernet address and also serial number) of every SpringCard Device found on the LAN,
- The device type. **FunkyGate-IP NFC** and **FunkyGate-IP+POE** appear under the type **SpringCard E663/RDR**,
- Whether DHCP is enabled or not (DHCP is not supported on early firmware versions),
- The device's current IP address, local network mask, and default gateway. Until the device has been properly configured, those entries show has "0.0.0.0",

- A user-defined string named “Info / location”, which will be used as an hint to identify the device in your own system.

2.1.4. Configure a Reader

Double-click one of the devices in the list. The configuration form appears:

The form shows the device's current configuration. Enter the new configuration.

a. Use DHCP?

DHCP stands for Dynamic Host Configuration Protocol. Enable DHCP on the device only if there's a DHCP server running on the network.

Note: in most situations, user software will connect as a client to a server service running in the Reader. If the Reader uses DHCP, its address is likely to change frequently, and so the client software must be reconfigured accordingly. It is recommended to reserve a permanent lease on the DHCP server for the Reader to suppress this annoyance.

b. Static configuration

IPv4 address and subnet mask are mandatory data and couldn't be left empty. The default gateway is optional; if the devices won't need to use a gateway, leave this field to “0.0.0.0”.

c. Info/Location

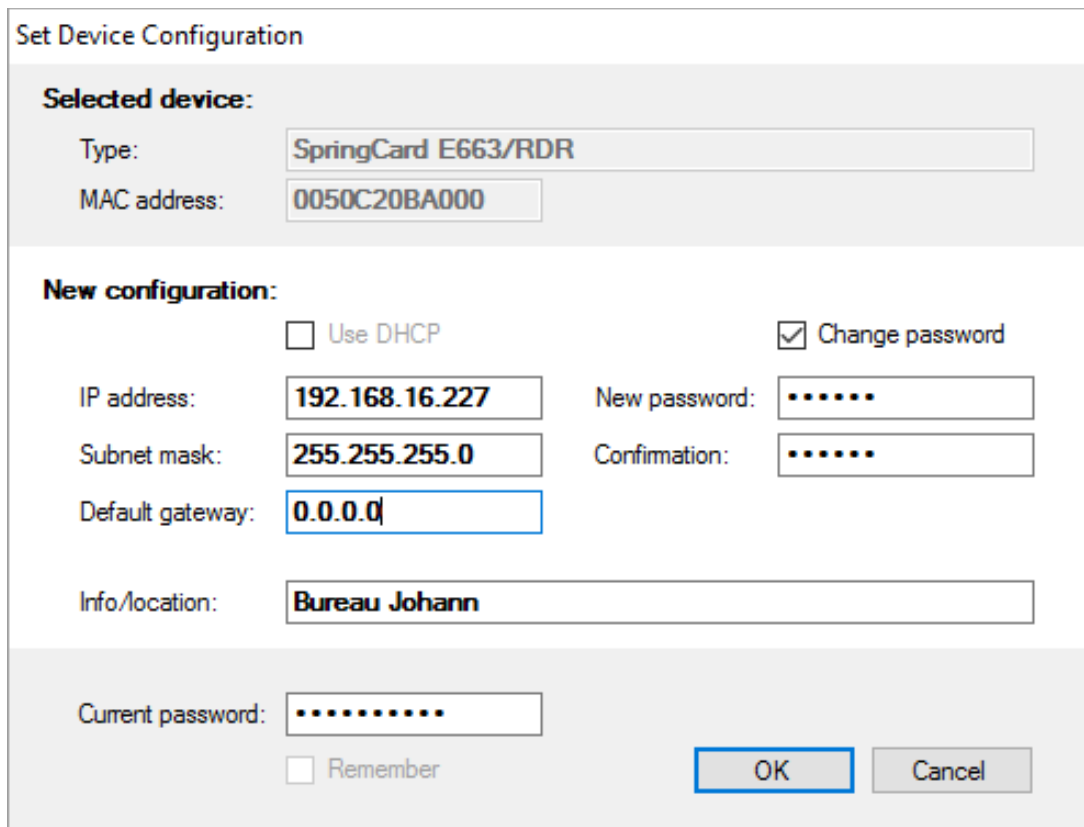
In the “info/location” field, enter a short string (less than 32 characters) as a reminder of the device's location or role.

d. Password

Check the box “change password” and enter a new password twice if you want to change the device's password.

Terminate by entering the device's current password to confirm that your allowed to change this device's configuration.

*The default password for all devices is **springcard**.*



Set Device Configuration

Selected device:

Type:

MAC address:

New configuration:

Use DHCP Change password

IP address: New password:

Subnet mask: Confirmation:

Default gateway:

Info/location:

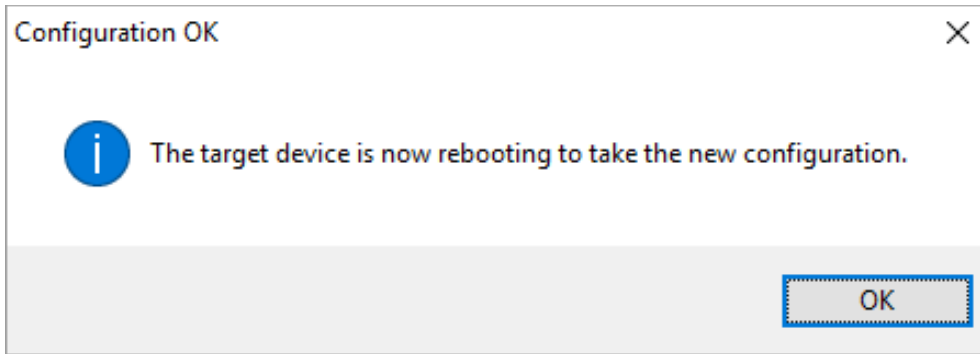
Current password:

Remember

When ready, click “OK”.

2.1.5. Verify the new configuration

If everything is OK, including the current password, the NDDU software is able to configure the Reader. The following message confirms that the new configuration has been accepted:



After a few seconds, the list of devices is refreshed and shows the new configuration:

The screenshot shows the "SpringCard Network Devices Discovery Utility" window. It has a menu bar with "File" and "About". Below the menu bar is the SpringCard logo. The main area contains a table with the following data:

MAC address	Device Type	DHCP	IP address	Mask	Gateway	Info / Location
0050C20BA000	SpringCard E663/RDR	off	192.168.16.227	255.255.255.0	0.0.0.0	Bureau Johann
D063B400A542	DOM Box	off	192.168.16.81	255.255.255.0	192.168.16.3	

2.2. ASSIGN AN IP ADDRESS USING A MASTER CARD

The Reader could be configured by the mean of a contactless Master Card.

The Master Cards are NXP Desfire cards formatted and programmed by **SpringCard Configuration Tool (ScMultiConf.exe, ref # SN14007)** for Windows.

Please refer to this software's documentation for details.

3. TELNET ACCESS TO THE READER

3.1. READER'S CONSOLE

The Reader features a “human” command processor (shell or console). This feature is accessible through the Telnet protocol. It is primarily made for testing and demonstration purposes. Only the few commands depicted in this chapter could safely be used for configuration and diagnostic.

Note that the SEC Configuration Register (h6E, § 9.4) may be used to disable the Console.

3.1.1. Open a Telnet session to the Reader

On most operating systems you could find a Telnet client in the default system tools. Open a console and enter

```
telnet xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the Reader's IP Address as defined in chapter 2.

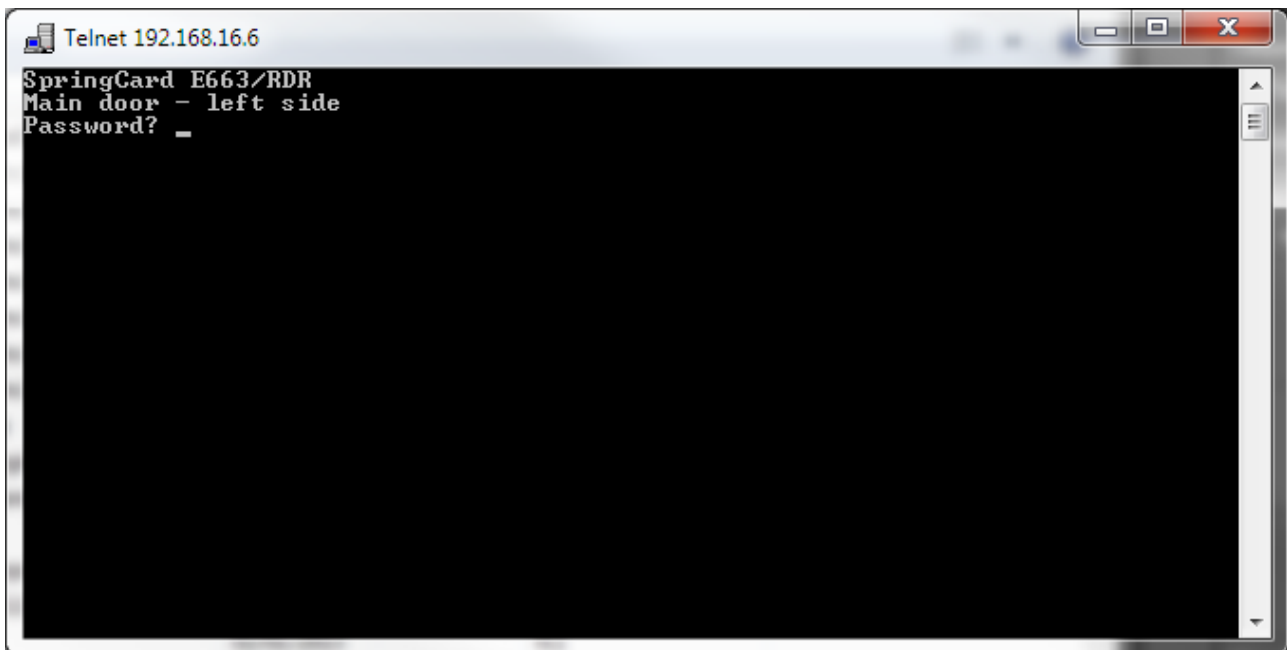
*Windows Vista / 7 / 8 / 10 : the Telnet client may be missing from your OS default install. Go to **Control Panel, Programs and Features** section, and then enable **Telnet client** in the **Turn Windows features on or off** tab.*

*Alternatively, you may download a free terminal client such as **Putty**, that is also a Telnet client.*

The Reader's Telnet shell says “SpringCard E663/RDR”, then the Info / Location string that has been entered in chapter 2, and finally prompts for a password.

Enter the Reader's password that you've defined in chapter 2.

*If you haven't changed the password, the default password is **springcard**.*



3.1.2. Sending a command to the Reader

Write the command line as documented below, and terminate by hitting the ENTER key.
Note that the Reader echoes the entered characters.

3.1.3. List of Console commands

Command	Meaning
version	Show the firmware version
info	Show the firmware information data
show	Show the current configuration
cfg	Dump all Configuration Registers written into persistent memory
cfgXX=YY...YY	Write value $_hYY...YY$ to Configuration Register $_hXX$
cfgXX=!!	Erase Configuration Register $_hXX$
cfgXX	Read Configuration Register $_hXX$
exit	Terminate the Telnet session

4. USING THE READER IN HTTP CLIENT MODE

4.1. ABSTRACT

The Reader runs a tiny embedded HTTP (web) client that is able to connect to a web server to send its data within a POST request. The content of the requests is authenticated by a one-way function (HMAC-MD5). The Reader is able to parse a JSON-formatted response to retrieve a LED or buzzer command.

To get started with HTTP and JSON, please read

- http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
- <http://en.wikipedia.org/wiki/JSON>

This feature makes it possible to use the Reader in cloud-centric architectures.

4.2. ENABLING AND CONFIGURING THE HTTP CLIENT

To select the HTTP client mode, edit the General option register (OPT, _h60, § 9.1).

The HTTP (web) client must be carefully configured before use. Here are the configuration parameters you'll need:

Parameter	Content	Constraints/Limits	Register
server	The fully-qualified DNS name of the HTTP server to send the Requests to. This could also be an IPv4 address in the form "xxx.xxx.xxx.xxx".	32 chars. Max <i>Do not add the protocol header ("http://") nor the port number to this field.</i>	_h 89
port	The port number. Default is 80.		_h 88 bytes 2-3
query	The path to the target script on the server. The Reader constructs the complete URL "http://<servername>[:<port>]/<query>"	32 chars. max Do not add the leading slash ("/") to this field.	_h 8A
hmac_key	The key used to authenticate the requests coming from the Reader.	16 byte value. If empty, authentication is disabled.	_h 8B
max_timeout	Time (in seconds) to wait for a response from the server. Default value is 30s.	The Reader stops reading until the server has answered or a timeout occurs.	_h 88 byte 0
keepalive	Interval (in seconds) after which a keepalive request is sent, to notify the server that the Reader is still there.	Minimum value is 2 * max_timeout. Set to 0 to disable this feature	_h 88 byte 1

4.3. LIMITATIONS

The Reader supports IPv4 and HTTP 1.1 only. It does not support HTTPS.

The Reader is not able to send a Request longer than 512B (including all headers).

The Reader is not able to process a Response longer than 512B (including all headers).

The Reader will not process only a Response with a HTTP code 200 ("success"). Any other response code is ignored. In particular, the code 301 ("moved permanently") does not trigger a new Request from the Reader.

Do not query the Reader's HTTP (web) server more than 4 times per second (i.e. once every 250ms) to let the Reader perform its core job of being a Reader.

4.4. HTTP CLIENT – POST REQUEST

Field name	Description
Mandatory fields (always transmitted by the Reader)	
what	Reason of the request. Possible values are: “startup”: transmitted when the Reader starts up “read”: transmitted when a card has been read and Insert/Remove mode is disabled “insert”: transmitted when a card is inserted “remove”: transmitted when a card is removed “tamper”: transmitted when the status of the tampers is changed “keepalive”: transmitted periodically if this feature is enabled
sequence	Counter incremented after every startup
counter	Counter incremented after every request
mac	Serial number / MAC address of the Reader
tampers	Current status of the tampers
Optional fields (present only when required by the context)	
id	Card Identifier transmitted together with what ="read" or what ="insert"
info	Info / Location field transmitted only if this field is non-empty
auth	Authentication string (HMAC) transmitted only if the authentication key is non-empty

4.5. HTTP CLIENT – JSON RESPONSE

Field name	Description
led-red	Action on the red LED. Possible values are: "off" "on" (default) "blink-fast" "blink-slow"
led-green	Action on the green LED. Possible values are: "off" "on" (default) "blink-fast" "blink-slow"
led-time	Duration of the sequence on the LEDs, in seconds. 0 means forever.
buzz	Duration of the buzzer's sound, in tenth of second. 0 means no sound.

5. USING THE READER IN HTTP SERVER MODE – REST API

5.1. ABSTRACT

The Reader runs a tiny embedded HTTP (web) server that listens on TCP port 80 and provides a basic REST API. The API provides its results as JSON structures, or as a script, containing a single JavaScript function call (the parameter to the function call being the same JSON structure).

To get started with REST and JSON, please read

- http://en.wikipedia.org/wiki/Representational_State_Transfer
- <http://en.wikipedia.org/wiki/JSON>

This feature makes it possible to use the Reader within an application that embeds an HTTP client component.

The HTTP server mode is intrinsically unsecure. “Serious” access control applications shall be built on top of the Authenticated Client/Server protocol depicted in chapter 6, and not on top of HTTP.

5.2. ENABLING THE HTTP SERVER

To select the HTTP server mode, edit the General option register (OPT, n60, § 9.1).

5.3. LIMITATIONS

*The Reader supports IPv4 and HTTP 1.1 only. It does not support HTTPS.
Do not query the Reader's HTTP (web) server more than 4 times per second (i.e. once every 250ms) to let the Reader perform its core job of being a Reader.*

5.4. REST API – FUNCTION LIST

Resource	Description	See §
Functions that returns a JSON response		
GET iwm2/read	Return the Card Identifier of the last Card that has been read. The Card Identifier is cleared afterwards.	5.5.1
GET iwm2/read/keep	Return the Card Identifier of the last Card that has been read. The Card Identifier is not cleared afterwards.	5.5.2
GET iwm2/buzz/{time_ms}	Drive the buzzer	5.6.1
GET iwm2/led/{color}/{mode}	Drive one LED (permanent)	5.6.2
GET iwm2/led/{color}/{mode}/{time_ms}	Drive one LED (temporary)	5.6.2
GET iwm2/leds/auto	Go back to default mode for both LEDs	5.6.3
Functions that returns a script (containing a JavaScript function call)		
GET iwm2_cb/read	Return the Card Identifier of the last Card that has been read. The Card Identifier is cleared afterwards.	5.5.1
GET iwm2_cb/read/keep	Return the Card Identifier of the last Card that has been read. The Card Identifier is not cleared afterwards.	5.5.2
GET iwm2_cb/buzz/{time_ms}	Drive the buzzer	5.6.1
GET iwm2_cb/led/{color}/{mode}	Drive one LED (permanent)	5.6.2
GET iwm2_cb/led/{color}/{mode}/{time_ms}	Drive one LED (temporary)	5.6.2
GET iwm2_cb/leds/auto	Go back to default mode for both LEDs	5.6.3

5.5. REST API – POLLING LOOP

5.5.1. `iwm2/read` and `iwm2_cb/read`

This is the Reader's main entry point. Invoke this function to get the identifier of the last card that has been read by the Reader.

The function must be invoked at least every 60 seconds, otherwise the Reader signals the “disconnected” state on its LEDs.

The last identifier is cleared when this function returns. Use `iwm2/read/keep` if the identifier must remain visible for another client request.

a. `iwm2/read`

Invoke `iwm2/read`

The Reader returns a JSON structure. 3 cases are possible:

No card has been read since last invocation – last identifier is empty

The Reader returns:

```
{ "iwm2": {  
  "success": "true",  
  "id": ""  
}}
```

A card has been read less than 1 second ago

The Reader returns:

```
{ "iwm2": {  
  "success": "true",  
  "id": "The card's identifier"  
}}
```

A card has been read more than 1 second ago (and less than 60 seconds ago)

The Reader returns:

```
{ "iwm2": {  
  "success": "true",  
  "id": "The card's identifier",  
  "seconds_ago": "Number of seconds elapsed since the card has been read"  
}}
```

b. *iwm2_cb/read*

Invoke **iwm2_cb/read**

The Reader returns a script. 3 cases are possible:

No card has been read since last invokation – last identifier is empty

The Reader returns:

```
iwm2_cb( { "iwm2": {  
    "success": "true",  
    "id": ""  
}});
```

A card has been read less than 1 second ago

The Reader returns:

```
iwm2_cb( { "iwm2": {  
    "success": "true",  
    "id": "The card's identifier"  
}});
```

A card has been read more than 1 second ago (and less than 60 seconds ago)

The Reader returns:

```
iwm2_cb( { "iwm2": {  
    "success": "true",  
    "id": "The card's identifier",  
    "seconds_ago": "Number of seconds elapsed since the card has been read"  
}});
```

5.5.2. *iwm2/read/keep* and *iwm2_cb/read/keep*

Same as **iwm2/read** and **iwm2_cb/read/keep** but the last identifier remains alive.

5.6. REST API – SENDING COMMANDS TO THE READER

5.6.1. `iwm2/buzz` and `iwm2_cb/buzz`

Turns the buzzer ON/OFF.

- To turn the buzzer ON, invoke `iwm2/buzz/{time_ms}` where `{time_ms}` is the decimal value of the sound's duration, expressed in milliseconds (1 to 65534).
- To turn the buzzer OFF, invoke `iwm2/buzz/0`.

a. `iwm2/buzz`

Invoke `iwm2/buzz/{time_ms}`

The Reader returns:

```
{ "iwm2": {  
  "success": "true"  
}}
```

b. `iwm2_cb/buzz`

Invoke `iwm2_cb/buzz/{time_ms}`

The Reader returns:

```
iwm2_cb( { "iwm2": {  
  "success": "true"  
}});
```

5.6.2. `iwm2/led` and `iwm2_cb/led`

This command makes it possible to drive the Reader's LEDs.

Complete syntax is `iwm2/led/{color}/{mode}/{time_ms}`

Allowed values for the `{color}` parameter are

- **red**
- **green**

The Blue LED can't be driven explicitly.

Allowed values for the **{mode}** parameter are

- **on**
- **fast**
- **slow**
- **heart**

The **{time_ms}** parameter is the decimal value of the command's duration, expressed in milliseconds (1 to 65534). Suppress the **{time_ms}** parameter (or set it to 0) to make it permanent.

a. *iwm2/led*

Invoke **iwm2/led/{color}/{mode}/{time_ms}**

The Reader returns:

```
{ "iwm2": {  
  "success": "true"  
}}
```

b. *iwm2_cb/led*

Invoke **iwm2_cb/led/{color}/{mode}/{time_ms}**

The Reader returns:

```
iwm2_cb( { "iwm2": {  
  "success": "true"  
}});
```

5.6.3. *iwm2/leds* and *iwm2_cb/leds*

Invoke command ***iwm2/leds/auto*** to cancel a pending LED command (§ 5.6.3).

a. iwm2/leds

Invoke ***iwm2/leds/auto***

The Reader returns:

```
{ "iwm2": {  
  "success": "true"  
}}
```

b. iwm2_cb/leds

Invoke ***iwm2_cb/leds/auto***

The Reader returns:

```
iwm2_cb( { "iwm2": {  
  "success": "true"  
}});
```

5.7. REST API – ERRORS

a. iwm2 namespace

Upon any error, the Reader returns:

```
{ "iwm2": {  
  "success": "false"  
}}
```

b. iwm2_cb namespace

Upon any error, the Reader returns:

```
iwm2_cb( { "iwm2": {  
  "success": "false"  
}});
```

6. SPRINGCARD NETWORK DEVICE C/S PROTOCOL

6.1. ABSTRACT

SpringCard Network Device C/S Protocol is a light-weight, bandwidth-efficient network protocol. The Reader is a TCP Server, and the Host (access control unit or computer in charge) is the Client.

Note that the Reader is not able to accept more than one Client at the time. Trying to connect to the same Reader from two different Host is not supported, and shall not be tried. An undefined behaviour may occur.

There are two communication modes:

- **Plain mode**, with no security involved
- **Secure mode**, based on AES cryptography.

In Secure mode, there are two authentication keys, leading to two authentication levels:

- The **Operation key** gives access to the basic operations of the Reader (§ 7.3). This is the key an access control unit would use to operate the Reader.
- The **Administration Key** makes it possible to change the Readerss configuration (§ 7.4). This key would typically used by a configuration software, when installing the Reader.

The Protocol is fully documented in [PMA14166], chapters 5 and 6.

7. SPRINGCARD NETWORK DEVICE – READER APPLICATION LAYER

7.1. PRINCIPLES

This chapter describes the **Reader Application Layer**, whose Application-Level Datagrams are transmitted on top of the Protocol described in [PMA14166], chapters 5 and 6.

The Application Layer is fully documented in [PMA14166], chapter 7. This chapter is only an extract that summarizes only the Reader's features.

*The **SpringCard Network Device C/S Protocol** is not a Request/Response Protocol; since a TCP channel is truly full-duplex, both the Host and the Reader may talk at any time. Therefore, the Host must be ready to process (or at least to queue) an Application-Level Datagram coming from the Reader at any time.*

7.2. LIST OF OPERATION-CODES AND DATA-FIELD IDENTIFIERS

7.2.1. Operation-codes (Host → Reader)

T (Tag)	Operation	See §
h00	Get Global Status	7.3.1
h0A	Start / Stop Reader	7.3.2
hD000	Clear LEDs	7.3.3
	Set LEDs	7.3.4
	Start LEDs	7.3.5
hD100	Buzzer	7.3.6
Restricted operations (available only after authentication using Administration Key)		
h0C	Write Configuration	7.4.1
	Erase Configuration	7.4.2
h0B	Reset the Reader (to apply the Configuration)	7.4.3

7.2.2. Data-field identifiers (Reader → Host)

T (Tag)	Operation	See §
h8100	Reader Identifier	7.5.1
h2F	Tamper Status	7.5.2
hB000	Card Read	7.5.3
hB100	Card Inserted	7.5.4
	Card Removed	7.5.5

7.3. HOST → READER, BASIC OPERATIONS

The operations listed in this chapter are available **whatever the mode**:

- Plain (no authentication),
- Secure, after authentication using the Operation Key,
- Secure, after authentication using the Administration Key.

7.3.1. Get Global Status

T	L
h00	h00

The Reader answers by 2 frames:

1. Reader Identifier
2. Tamper Status

7.3.2. Start/Stop Reader

T	L	V
h0A	h01	mode

- **mode**: start/stop command
 - h00 Reader goes OFF (RF field OFF, no activity on RF)
 - h01 Reader goes ON

7.3.3. Clear LEDs command

Both LEDs go OFF.

T	L
hD000	h00

7.3.4. Set LEDs command

Both LEDs are driven – until a Clear LEDs command is received.

T	L	V	
hD000	h02	red	green

- **red:** command for red LED
 - h00 OFF
 - h01 ON
 - h02 blinks slowly
 - h03 blinks quickly
- **green:** command for green LED
 - h00 OFF
 - h01 ON
 - h02 blinks slowly
 - h03 blinks quickly

7.3.5. Start LED sequence command

Both LEDs are driven – until a Clear LEDs command is received or a timeout occurs.

T	L	V		
hD000	h04	red	green	time (sec)

- **red:** same as above,
- **green:** same as above,
- **time:** time (in seconds, MSB-first) before returning to all-LED-OFF state.

7.3.6. Buzzer command

T	L	V
hD100	h01	seq.

- **seq:**
 - h00 buzzer OFF,
 - h01 buzzer ON,
 - h02 buzzer short sequence,
 - h03 buzzer long sequence.

7.4. HOST → READER, RESTRICTED OPERATIONS

The operations listed in this chapter are available only in **Secure mode, after authentication using the Administration Key.**

7.4.1. Write Configuration Register

The Reader's behaviour is defined by Configuration Registers documented in chapters 9 and 10. The Write Configuration Register command allows to write into any Configuration Register given its address.

<addr> is the Register number on one byte (valid values are $_{h}00$ to $_{h}FE$).

T	L	V	
$_{h}0C$	<var.>	<addr>	<value>

7.4.2. Erase Configuration Register

The Reader's behaviour is defined by Configuration Registers documented in chapters 9 and 10. The Erase Configuration Register command allows to delete any Configuration Register given its address. Once a Register is deleted, the default value for this Register is used.

<addr> is the Register number on one byte (valid values are $_{h}00$ to $_{h}FE$).

T	L	V
$_{h}0C$	$_{h}01$	<addr>

7.4.3. Reset the Reader

The Reader must be re-setted in order for the new configuration to take effect. When receiving this command, the Reader drops the connection and resets.

T	L	V	
$_{h}0B$	$_{h}02$	$_{h}DE$	$_{h}AD$

7.5. READER → HOST

7.5.1. Reader Identifier

This T,L,V is transmitted in response to the **Get Global Status** command.

T	L	V
h8100	h1C	SpringCard E663/RDR x.xx

7.5.2. Tamper Status

This T,L,V is transmitted in response to the **Get Global Status** command or when one of the tampers is broken/restored.

T	L	V
h2F	h01	Bit field, the broken tampers are denoted by the corresponding bit set to 1. V = h00 when all tampers are OK.

7.5.3. Card Read

This T,L,V is transmitted when the Reader has read a card, if the Insert/Remove mode is disabled.

T	L	V
hB000	<var.>	Card Identifier

7.5.4. Card Inserted

This T,L,V is transmitted when the Reader has read a card, if the Insert/Remove mode is enabled.

T	L	V
hB100	<var.>	Card Identifier

7.5.5. Card Removed

This T,L,V is transmitted when the card is removed, if the Insert/Remove mode is enabled.

T	L
_h B100	_h 00

8. EDITING READER'S CONFIGURATION

The Reader's configuration is stored in a set of non-volatile Configuration Registers. There are two groups of Registers:

- The Registers that control the behaviour of the Reader are fully documented in chapter 9. Some of them are common to various SpringCard Readers, but some of them are very specific to the **SpringCard FunkyGate-IP NFC**.
- The Registers that control the Template System are shared among all SpringCard Readers. Chapter 10 is therefore a place-holder that redirects to the document describing this Template System precisely.

But this subtle distinction between these two groups is only there to keep the documents short, and to ease switching from one Reader to the other. Technically speaking, all Registers are defined (and accessed) the same way.

There are four ways to edit the Reader's Configuration Registers:

1. Through the Telnet link
2. Using Master Cards
3. Using the SpringCard Network Device C/S Protocol, after authentication with Administration Key.

Note that the SEC Configuration Register ($_{h}6E$, § 9.4) may be used to disable either way to access the Configuration Registers.

Administration Key is defined in the IPS Configuration Register ($_{h}83$, § 9.5.3)

8.1. THROUGH THE TELNET LINK

Open a Telnet session to the Reader as instructed in § 3.1.

8.1.1. Reading Configuration Registers

Enter "cfg" to list all Configuration registers currently defined (registers that are not explicitly defined keep their default value).

Enter "cfgXX" to read the value of the Configuration register $_{h}XX$.

Note that Configuration registers $_{h55}$, $_{h56}$, $_{h6E}$ and $_{h6F}$ that hold sensitive data (the keys used by Master Cards and the Reader's secret keys and password) are masked.

8.1.2. Writing Configuration Registers

Enter "cfgXX=YYYY" to update Configuration Register $_{hXX}$ with value $_{hYYYY}$. YYYY can be any length between 1 and 32 bytes.

Enter "cfgXX=!!" to erase Configuration Register $_{hXX}$.

8.2. USING MASTER CARDS

The Master Cards are NXP Desfire cards formatted and programmed by **SpringCard Configuration Tool (ScMultiConf.exe, ref # SN14007)** for Windows.

Please refer to this software's documentation for details.

8.3. THROUGH THE SPRINGCARD NETWORK DEVICE C/S PROTOCOL

Please refer to [PMA14166].

9. GLOBAL CONFIGURATION OF THE READER

9.1. GENERAL OPTIONS

Name	Tag	Description	Size
OPT	_h 60	General option, see table below	1 or 2

General options bits

Bits	Value	Meaning	
Byte 0			
7	0	Normal mode	
	1	Power saving mode (the Reader is slower)	
6	0	Track the cards by their ID only	
	1	Keep the RF field active to track the cards (works with Random IDs)	
5 - 4	Anti-collision mode		
	00	Read every card one after the other	
	01	RFU	
	10	Read only one card at a time (ignore the other ones)	
3 - 2	Master Card and NFC configuration		
	00	Disable configuration by Master Card or NFC	
	01	Allow configuration by Master Card or NFC at power up only	
	10	RFU	
1 - 0	Communication mode		
	00	The Reader uses the SpringCard Network Device C/S Protocol (§ 6)	
	01	The Reader runs in HTTP server mode (§ 5)	
	10	The Reader runs in HTTP client mode (§ 4)	
7	Byte 1 (optional)		
	0	Insert/Remove mode is disabled (§ 7.5.3)	
	1	Insert/Remove mode is enabled (§ 7.5.4 and § 7.5.5)	
	6	0	RFU (set to 0)
	5	0	RFU (set to 0)
	4	0	RFU (set to 0)
	3	0	RFU (set to 0)
	2	0	RFU (set to 0)
1	0	RFU (set to 0)	

0	0	Reader is active on startup
	1	Reader is not active on startup (Host must send an activation command)

Default value: $_b00001100\ 00000000$

9.2. DELAYS AND REPEAT

Name	Tag	Description	Min	Max
ODL	$_h61$	Min. delay between 2 consecutive outputs (0.1s)	0	100
RDL	$_h62$	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)

9.3. LEDs AND BUZZER

Name	Tag	Description	Size
CLD	$_h63$	LEDs control, see table below	1
CBZ	$_h64$	Buzzer control, see table below	1

LEDs control bits

Bits	Value	Meaning
7	0	Short LED sequences (3 seconds)
	1	Long LED sequences (10 seconds)
6 - 5	00	When idle, blue LED blinks slowly (“heart beat” sequence)
	01	When idle, blue LED is always on
	10	When idle, blue LED is always off
	11	RFU
4	0	Green LED stays OFF
	1	Green LED blinks when a valid card has been processed
3	0	Red LED stays OFF
	1	Red LED blinks when an unsupported card has been processed
2	0	Green LED stays OFF
	1	Green LED blinks as soon as a card is seen in the field
1 - 0	00	RFU, do not use
	01	LED driven by Host commands only
	10	RFU, do not use
	11	LED driven by internal state machine and Host commands

Default value: $_b00001111$

Buzzer control bits

Bits	Value	Meaning
7	0	Buzzer short pulse = 0,2 sec
	1	Buzzer short pulse = 0,5 sec
6	0	Buzzer long pulse = 0,7 sec
	1	Buzzer long pulse = 1,5 sec
5		<i>RFU</i>
4	0	No action on buzzer before specified by host controller
	1	Short pulse when a valid card has been processed
3	0	No action on buzzer for unsupported cards
	1	Long pulse when an unsupported card has been processed
2	0	No action on buzzer before processing is achieved
	1	Short pulse as soon as a card is seen in the field
1 - 0	00	Buzzer is disabled, other settings are ignored
	01	Buzzer controlled by serial commands, other settings are ignored
	10	Buzzer controlled by internal software, serial commands are ignored
	11	Buzzer controlled by both internal software and serial commands

Default value : $\text{,}00010010$

9.4. SECURITY OPTIONS

Name	Tag	Description	Size
SEC	_h 6E	Security option bits. See table below	1

Security option bits

Bits	Value	Meaning
Standard network servers		
7	0	Telnet server is disabled
	1	Telnet server is enabled
6	0	<i>RFU (set to 0)</i>
5	0	<i>RFU (set to 0)</i>
4	0	SpringField Colorado notifier is disabled
	1	SpringField Colorado notifier is enabled ¹
3	0	<i>RFU (set to 0)</i>
Tampers		
2	0	Do not signal tamper alarms on buzzer
	1	Signal tamper alarms on buzzer
1	0	Reader keeps on reading even if a tamper is broken
	1	Reader stops reading when a tamper is broken
0	0	Do not raise alarm if a tamper is broken at power up
	1	Raise alarm on tamper broken even at power up

Default value: _b10010100

¹ SpringField Colorado is a NFC-enabled application running on Android, or embedded in a specific NFC Tag, that retrieves and shows the Reader's data: firmware name and version, serial number, IP address etc.

9.5. TCP CONFIGURATION

9.5.1. IPv4 address, mask, and gateway

Name	Tag	Description	Size
IPA	$_{h}80$	IPv4 configuration bytes, see table below	4 to 20

IPv4 configuration bytes

Bytes	Contains	Remark
0	Address, 1 st byte	Device's IPv4 Address. If these bytes are missing, the default IP Address $_{h}C0 A8 00 FA$ (192.168.0.250) is taken.
1	Address, 2 nd byte	
2	Address, 3 rd byte	
3	Address, 4 th byte	
4	Mask, 1 st byte	Network Mask. If these bytes are missing, the default Mask $_{h}FF FF FF FF$ (255.255.255.0) is taken.
5	Mask, 2 nd byte	
6	Mask, 3 rd byte	
7	Mask, 4 th byte	
8	Gateway, 1 st byte	Default Gateway. If these bytes are missing, the value $_{h}00 00 00 00$ (0.0.0.0) is taken, meaning that there's no Gateway.
9	Gateway, 2 nd byte	
10	Gateway, 3 rd byte	
11	Gateway, 4 th byte	
12	DNS server 1, 1 st byte	Address of 1 st DNS server. If these bytes are missing, the value $_{h}00 00 00 00$ (0.0.0.0) is taken, meaning that there's no DNS server.
13	DNS server 1, 2 nd byte	
14	DNS server 1, 3 rd byte	
15	DNS server 1, 4 th byte	
16	DNS server 2, 1 st byte	Address of 2 nd DNS server. If these bytes are missing, the value $_{h}00 00 00 00$ (0.0.0.0) is taken, meaning that there's no DNS server.
17	DNS server 2, 2 nd byte	
18	DNS server 2, 3 rd byte	
19	DNS server 2, 4 th byte	

Default value: $_{h}C0 A8 00 FA FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00$

(address = 192.168.0.250, mask = 255.255.255.0, no gateway, no DNS servers)

9.5.2. SpringCard Network Device C/S Protocol – Server port

Name	Tag	Description	Size
IPP	_h 81	Listen TCP port for the server (2 bytes, MSB-first)	2

Default value: _h0F 9F (server TCP port = 3999)

9.5.3. SpringCard Network Device C/S Protocol – Security settings and authentication keys

Name	Tag	Description	Size
IPS	_h 84	Server security settings bits, see table below	1

Security settings bits

Bits	Value	Meaning
7	0	RFU (set to 0)
6	0	RFU (set to 0)
5	0	RFU (set to 0)
4	0	RFU (set to 0)
3	0	RFU (set to 0)
2	0	The Administration Key is enabled
	1	The Administration Key is disabled
1	0	The Operation Key is enabled
	1	The Operation Key is disabled
0	0	Plain communication is allowed
	1	Secure communication is mandatory

Default value: _b00000100

(only Operation Key is enabled, plain communication is allowed)

9.5.4. SpringCard Network Device C/S Protocol – Operation Key

Name	Tag	Description	Size
IPK.OPE	_h 85	C/S Protocol Operation Key	16

Default value: _h00 ... _h00

9.5.5. SpringCard Network Device C/S Protocol – Administration Key

Name	Tag	Description	Size
IPK.ADM	_h 86	C/S Protocol Administration Key	16

Default value: _h00 ... _h00

9.5.6. HTTP client configuration

Name	Tag	Description	Size
HTC	<code>h88</code>	HTTP client configuration bytes. See table below	1

HTTP client configuration bytes

Bytes	Contains	Remark
0	Network timeout, in seconds	The same timeout applies to DNS queries, TCP channel openings, and HTTP exchanges. Default is 30s
1	Keep-alive interval, in seconds	Default is 0 (keep-alive is disabled)
2	TCP port of the HTTP server, MSB	Default port is 80 (<code>h0050</code>)
4	TCP port of the HTTP server, LSB	

Default value: `h1E 00 00 50`

9.5.7. HTTP client – server name

Name	Tag	Description	Size
HTS	<code>h89</code>	HTTP client – name of the remote HTTP server	0 to 32

9.5.8. HTTP client – query string

Name	Tag	Description	Size
HTQ	<code>h8A</code>	HTTP client – query string on the remote HTTP server	0 to 32

9.5.9. Ethernet configuration

Name	Tag	Description	Size
ETC	_h 8D	Ethernet configuration bits. See table below	1

Ethernet configuration bits

Bits	Value	Meaning
7	0	RFU (set to 0)
6	0	RFU (set to 0)
5	0	RFU (set to 0)
4	0	RFU (set to 0)
3	0	RFU (set to 0)
2	0	RFU (set to 0)
1	0	RFU (set to 0)
0	0	Use auto-configuration (10/100Mbps, half or full-duplex)
	1	Force bitrate = 10Mbps, half-duplex

Default value: `b_00000000`

9.5.10. Info / Location

Name	Tag	Description	Size
ILI	_h 8E	Info / Location string	Var. 0-30

Default value: empty

The **Info / Location** string is a text value (ASCII) that appears

- When someone tries to connect on Telnet,
- In the NDDU software (§ 2.1.3).

Use this string as a reminder of where your Reader is installed, or what is its role in your access-control system.

9.5.11. Password for Telnet access

Name	Tag	Description	Size
ITP	_h 8F	Password for Telnet access string	Var. 0-16

Default value: "springcard"

The **Password for Telnet access** string is a text value (ASCII) that protects the access to the Reader using Telnet protocol.

The password is mandatory. If this registry is not set, default value "springcard" is used.

10. THE TEMPLATE SYSTEM

SpringCard FunkyGate-IP NFC provides 4 “Card Processing Templates” that defines how the Reader which fetch data from various cards/tags, and how the Card Identifier will be constructed from these data before being sent to the Host.

The template system is fully described in document **[PMA13205] “RFID/NFC Scanners Template System”**.

Please use this document as reference to configure the “Reader part” of your **SpringCard FunkyGate-IP NFC**.

11. 3RD-PARTY LICENSES

SpringCard FunkyGate-IP NFC has been developed using open-source software components.

11.1. FREERTOS



FreeRTOS is a market leading real time operating system (or RTOS) from Real Time Engineers Ltd. SpringCard FunkyGate-IP NFC runs on FreeRTOS v7.5.2.

FreeRTOS is distributed under a modified GNU General Public License (GPL) that allows to use it in commercial, closed-source products.

For more information, or to download the source code of FreeRTOS, please visit

www.freertos.org

11.2. μ IP

μ IP is an open-source TCP/IP stack initially developed by Adam Dunkels and licensed under a BSD style license.

SpringCard FunkyGate-IP NFC uses FreeTCPIP, a modified version of μ IP that comes with FreeRTOS. To comply with the original license of μ IP, we have to copy the full text here:

Copyright (c) 2001-2003, Adam Dunkels.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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 SPRINGCARD and you. No information provided in this document shall be considered a substitute for your independent investigation.

The information provided in 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 SPRINGCARD 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. SPRINGCARD reserves the right to change the information at any time without notice.

SPRINGCARD doesn't warrant any results derived from the use of the products described in this document. SPRINGCARD 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 product may result in personal injury. SPRINGCARD customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify SPRINGCARD 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 SPRINGCARD 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 documents, and you are not allowed to publish or reproduce this document, either on the web or by any mean, without written permission of SPRINGCARD.

Copyright © SPRINGCARD SAS 2017, all rights reserved.

EDITOR'S INFORMATION

SPRINGCARD SAS company with a capital of 227 000 €

RCS EVRY B 429 665 482

Parc Gutenberg, 2 voie La Cardon

91120 Palaiseau – FRANCE

CONTACT INFORMATION

For more information and to locate our sales office or distributor in your country or area, please visit

www.springcard.com