www.securing.biz

The Tick

FIELD GUIDE FOR RED TEAM OPERATORS

document version: 1.0

author: Jakub Kramarz (SecuRing)

publication date: 2025-03-28

PUBLICATION NOTICE

TABLE OF CONTENTS

1. DOCUMENT SUMMARY

The Tick is an electronic access control system implant. When installed between access point reader and controller, it has a capability of sniffing and replying card information transmitted using Wiegand and Magstripe clock&data protocols.

This document describes the operational procedures for it:

- Hardware revision - V0.1B
- Software revision –868e477177b36d9f1d2a775cdd83b0f3abfe20f5

2. SAFETY PRECAUTIONS

Before installing The Tick for the first time, please review the guidelines below to avoid any injury and damage.

This device is not tested according to and may not conform to radiated or conducted electromagnetic compatibility standards. It is not Wi-Fi or Bluetooth Low Energy certified and may not meet standards for interoperability. It is not intended to be used by end users or for permanent installation.

2.1. Electrical isolation

The device does not feature any kind of electrical or galvanic isolation. The voltage applied to the device is present on exposed components. Operators must ensure that access control system under test nominally runs on voltage safe for human body and under device operational limits.

2.2. Ground current safety

The device does not feature a fuse in the ground return path. When simultaneously connecting to an externally powered access control system under test and a computer USB port, it is recommended to take extra caution and:

- use a laptop on battery power, with no other peripherals connected,
- use a USB 2.0 isolator.

2.3. Supported voltages

	Minimal	Nominal	Maximal
Supply (USB)	4.5V DC	5V DC	6V DC
Supply (VDC)	7V DC	12V DC	25V DC
Data	3.5V	5V	25V

2.3.1. Device hardware configuration

When using the hardware revision V0.1A, ensure that a solder bridge near the USB port is open.

The revision V0.1B may have a Schottky diode populated instead of a solder bridge – this configuration sacrifices reverse voltage protection feature for automatic power source switching.

3. DEVICE PREPARATION

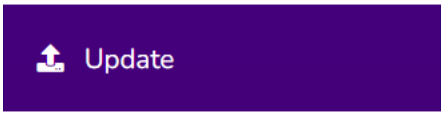
3.1. Software configuration

3.1.1. Device firmware upgrade

It is recommended to update the device firmware to the latest release version to apply bug and security fixes.

If the device firmware features OTA-upgrade

Upload provided **OTA Image** over the device HTTP interface:



The device will preserve the configuration and log files.

If the device does not feature OTA-upgrade

Connect the device using a USB-C cable and upload the provided **Full Image** using Tasmota Web Installer.

The device configuration and log files will be lost.

3.1.2. Restoring default configuration

1. Power the device using the USB connector,
2. Briefly press the button labelled RST,
3. Wait 15 seconds,
4. Repeatedly press the button labelled BOOT five (5) times,
5. Wait 5 seconds.

When the default configuration is restored, the device will create an empty configuration file and use the hard-coded defaults. Downloading a default configuration file from the source code repository should be considered, to provide configuration options reference.

3.1.3. Configuring the device

To configure the device, the operator can access the file editor in its HTTP interface. Changes to the device configuration are applied on a device restart (triggered using the device web interface, RST button press, or power cycling).

Connecting to WiFi

In the default configuration, the device creates a WiFi access point:

- ESSID: *TheTick-config*
- PSK: *accessgranted*

On subsequent runs, the device ID will replace the *config* in the ESSID.

Accessing the HTTP interface

After connecting to the hotspot, the web interface is available as:

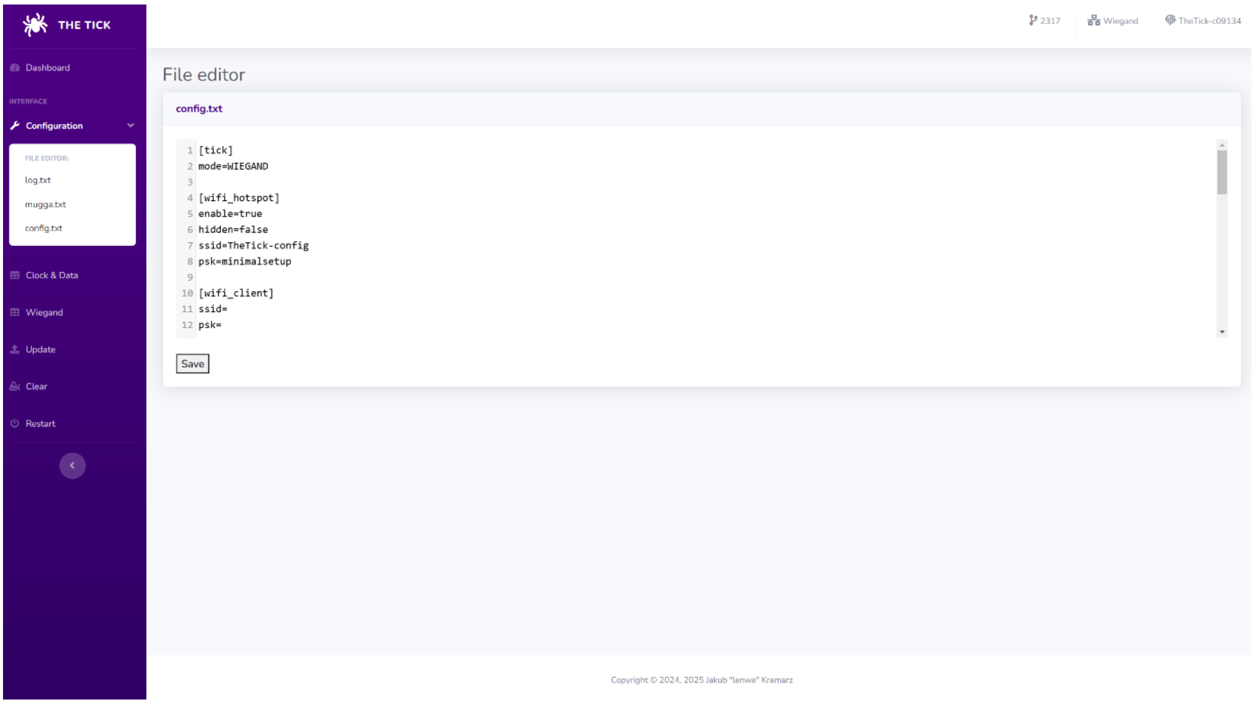
- http://TheTick.local/

or

- http://192.168.4.1/

Preforming configuration changes

Using the embedded file editor, the operator can adjust the device configuration in the following manner. Due to consideration of cache sharing policies introduced by the modern web browser, all files mandatory for interface operation are hosted by the device itself, and no Internet connection is required.



```
[tick]
mode=WIEGAND

[wifi_hotspot]
enable=true
hidden=false
ssid=TheTick-config
psk=minimalsetup

[wifi_client]
ssid=
psk=
```

Changing the device operation mode

```
[tick]
mode=WIEGAND

[wiegand]
dos_id=7fffffff:31
pin_d0=0
pin_d1=1
pulse_width=34
pulse_gap=1966
```

```
[clockanddata]
pin_clock=1
pin_data=0
pulse_width=300
```

By setting the device mode, the operator can choose the communication protocol used by the access control system under test:

Use “WIEGAND” for:

- Almost every legacy EAC system or reader running in compatibility mode (e.g. HID multiCLASS and iCLASS SE with no OSDP module).

Use “CLOCKANDDATA” for:

- Paxton readers,
- Magstripe (magnetic card) readers,
- Probably other systems mentioning the “ABA TRACK-II” format in their manual.

For these modes D0/D1 and CLOCK/DATA may be adjusted after installation if not wired properly (if the intercepted data is different than expected).

Changing the device WiFi configuration

```
[wifi_hotspot]
enable=true
hidden=false
ssid=TheTick-config
psk=accessgranted

[wifi_client]
ssid=
psk=
```

If SSID and PSK are configured in the *wifi_client* section, the device first attempts to connect to the defined access point for a period of 1 minute. If the network is not present or this operation fails, and *wifi_hotspot* is *enabled*, the device starts to broadcast its own WiFi network.

For covert deployment, it is recommended to change the SSID to an unsuspicious name (e.g. similar to common home access points in the area of operation) and/or disable beacon broadcasting by enabling hidden SSID. Implementing this change is highly recommended if the target facility wireless network controller features air marshal (e.g. Cisco Meraki) to avoid alerting network administrators.

When connecting the device to an existing WiFi network, configuring the HTTP and OTA authentication may be considered:

```
[http]
username=
password=

[ota]
password=ExtraSpecialPassKey
```

It is advised to avoid connecting the device to networks out of the control of the operator, with a high level of broadcast traffic or a public router. Due to the limited processing power of the device, such a network environment will interfere with its operations.

```
[mdns]
host=TheTick
```

Configuring the hostname changes the name used in the Multicast DNS broadcast.

```
[syslog]
server=
port=514
service=accesscontrol
priority=36
host=TheTick
```

The syslog configuration allows transmitting the sniffed credentials using UDP protocol in the UNIX format. The address may be set to the unicast address of the network server, the multicast address of a group or the network broadcast address. The communication is performed in a plaintext manner.

Changing the device BLE configuration

```
[ble]
enable=true
service=f498124f-2137-4615-9859-30eb4cecffb5
characteristic=beb5483e-36e1-4688-b7f5-ea07361baaaa
passkey=123456
```

By default, the device will provide Bluetooth Low Energy interface with a well-known passkey. To prevent unauthorized interaction the passkey must be changed or the interface must be disabled.

To avoid device BLE broadcast fingerprinting, the operator may consider changing the service and characteristic UUIDs. Additionally, mimicking the broadcast of characteristics used by common wearable devices may be considered.

Explicitly setting the passkey to 0 disables pairing and LE security features, providing a fallback to a legacy BLEKey-like operation mode.

4. DEVICE DEPLOYMENT

4.1. Connecting the device to access control system

Only if:

- the operator is competent to work on low-voltage electrical installations,
- proper tools/protective equipment required by the local code is used
- it is permitted by local work regulations,

the device may be installed between the reader and control unit without disconnecting its power source.

4.1.1. Selecting the proper device version

The Tick features insulation-displacement connectors that allow unnoticed installation of the implant without disconnecting any wires from the access control system. There are following versions of the device, featuring connectors designed to be used on different wiring gauges.

Wire gauge and type	Connector type	Recommended insertion tool
26-28 AWG solid or stranded (misused LAN cables)	Surface mount BLACK AVX 9175-000 series	Kyocera 069175701601000
22-24 AWG solid or stranded (recommended cables)	Surface mount WHITE AVX 9176-000 series	Kyocera 069176701601000
18-26 AWG solid or stranded (almost any cables)	Silicone pigtail with T-Tap type connectors	-

Devices featuring wire-to-board connectors should be used if limited space is encountered behind the reader. In the other case (e.g. if an installation box or empty wall is present behind the reader), tap connectors are easier to use.

Device pinout

Wire-to-board connectors

The device with wire-to-board connectors has 5 contacts labeled:

- V (VCC),
- G (GND),

- L (LED),
- 0 (D0/CLOCK),
- 1 (D1/DATA).

The labels are consistently present on both sides of the board.

T-tap connectors

The device with pigtailed tap connectors has 4 contacts with the following color code:

- red (VCC),
- black (GND),
- green (D0),
- yellow (D1).

4.1.2. Connecting the device

Power lines

The operator should first connect VCC and GND contacts. The device is protected against reverse polarity.

Once connected, the implant should power on and immediately start blinking. If it does not, the operator must not proceed with connecting data lines until it starts blinking. If it still does not, it is recommended to trace the wires to the reader, consult the access system installation manual or, if in a rush, reverse the wires and give it a try.

Data lines

Once the power is connected, the operator may proceed to connect data lines.

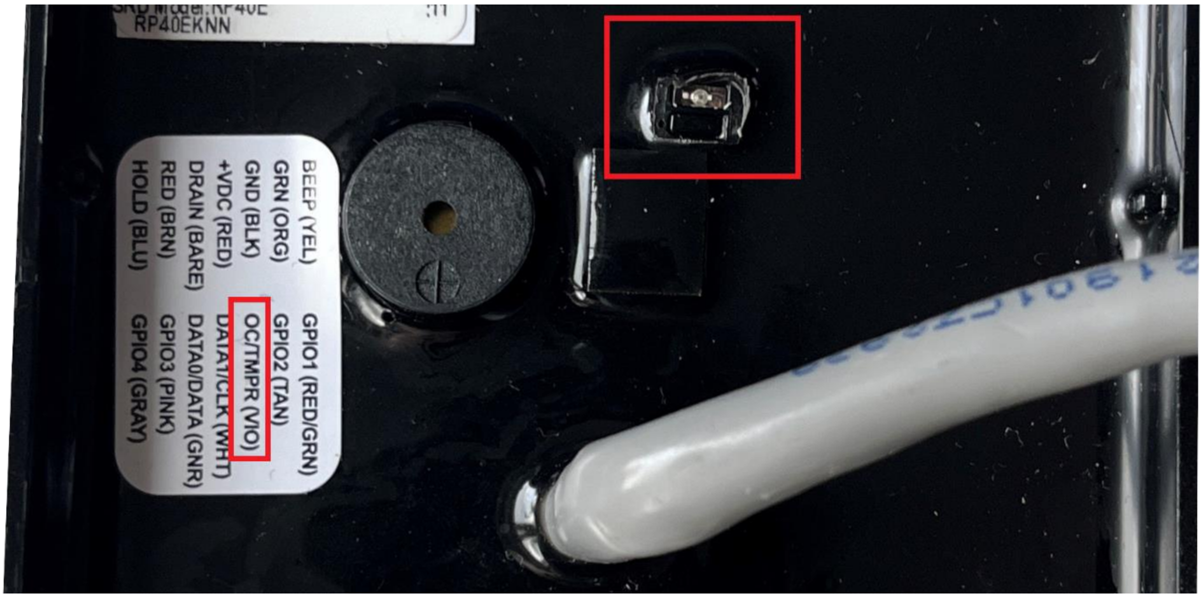
For Wiegand and Clock&Data it is recommended to follow the configured mapping when connecting D0/CLOCK and D1/DATA lines. If in a rush, it won't break the device and can be fixed later in device configuration.

Legacy protocols like Wiegand can easily spot the disappearance of the reader from the system (read: cutting the wires open), due to used signaling. At the same time, it cannot easily notice connecting the implant to the wires.

Tamper detection

Some readers feature tamper detection mechanisms. Some of them are hall-effect sensors, light sensors or mechanical switches that complete the circuit when the case is closed.

For example, in the HID RP10 reader, the information about a tamper attempt being detected is sent through violet wire:



The back of an HID reader with a tamper sensor and wiring diagram visible

In many cases in the production systems, the wires won't be connected to anything, thus allowing for the implant installation without worrying about tamper attempts being logged in the system. Even if the wires are connected, they may either trigger a sound alarm or create an event in the logs that does not immediately alert the security guards.

Still, the operator must be prepared that the alarm may be configured correctly. If after opening the reader case you see a properly wired tamper detection sensor, the good practice would be to assume that it is configured well and, if in a Red Teaming black box scenario, running away to avoid being caught.

4.1.3. Wiring reference

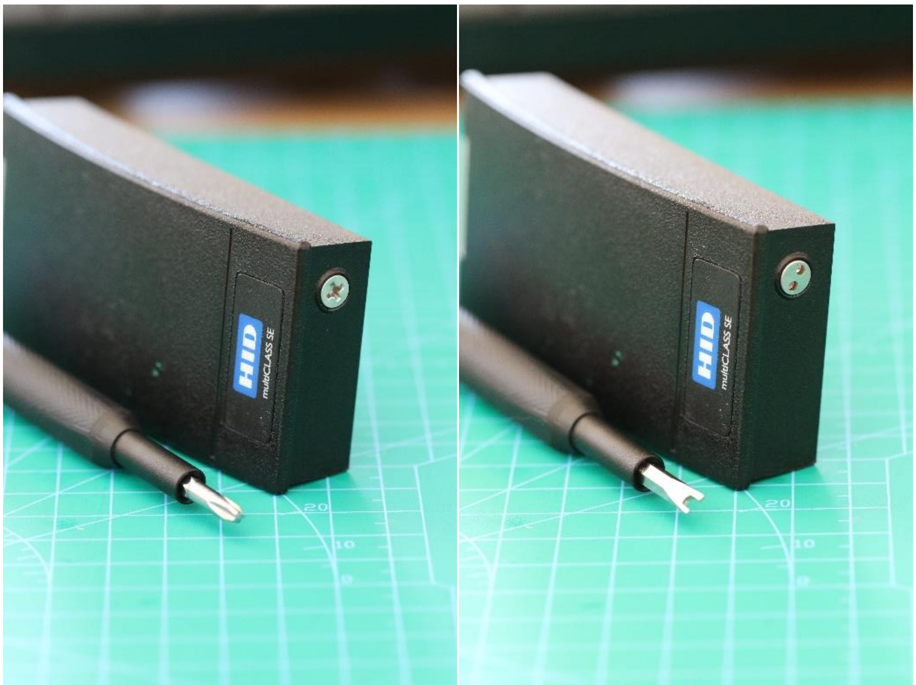
This table contains a compilation of wiring recommendations from reader installation manuals of different manufacturers. It is not guaranteed that the installer followed the recommended cable type and therefore wiring color code.

System	VCC	GND	D0 / CLOCK	D1 / DATA
Allegion MR10	red	black	green (D0) white (CLK)	white (D1) green (DATA)
Belden CR9540	red	black	yellow	blue
HID multiCLASS	red	black	green	white
Paxton Switch2	red	black	yellow	blue
Roger PRTxxLT	red	blue	green	brown
Satel ACCO	red	blue	green	black

The system names are trademarks or registered trademarks of respective companies in the US and/or other countries. Use of these names here is to clearly identify system under test does not imply any affiliation with or endorsement by the trademark holders.

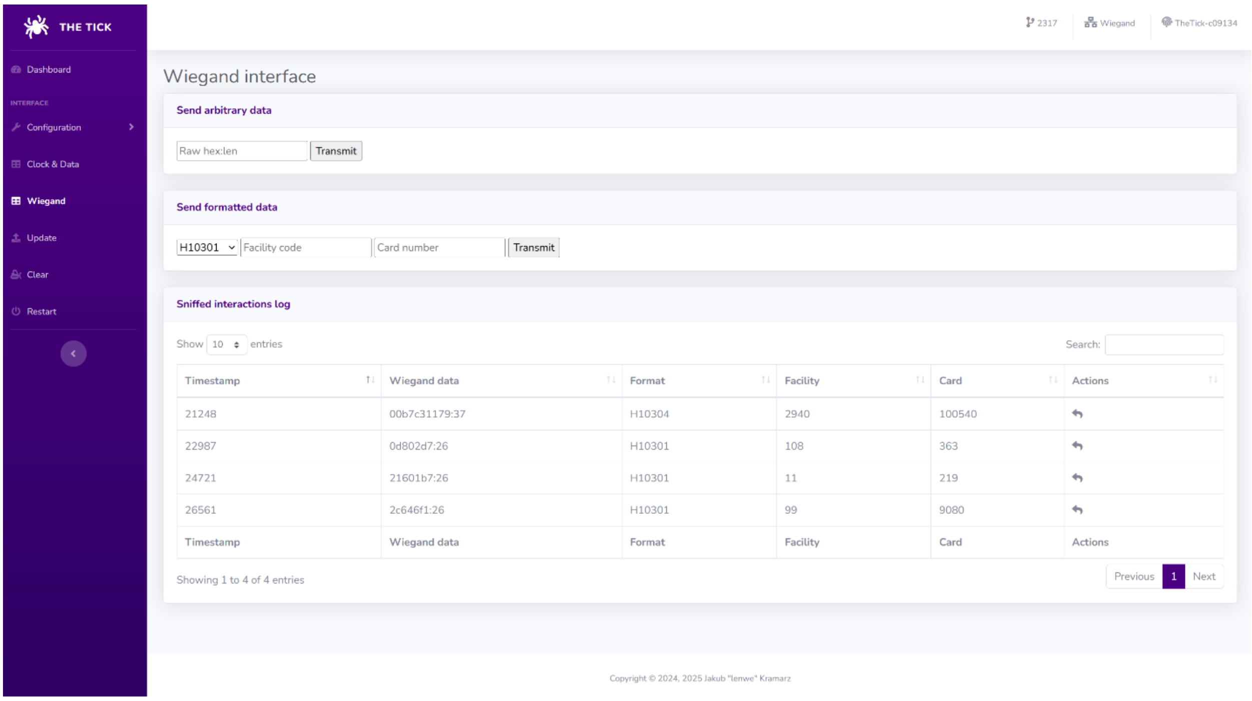
4.1.4. Dealing with security fasteners

Some readers come with two sets of bolts – "standard" and "secure" one. While dedicated tools (like HID 04-0001-03 Security Tool for Anti-Tamper Screw) are available from the vendors, all common bits are present in Mahi Precision Bit Set from iFixit.



5. DEVICE OPERATION

5.1. WiFi interface



Wiegand interface

Send arbitrary data

Raw hex:len

Send formatted data

H10301 | Facility code | Card number

Sniffed interactions log

Show 10 entries

Search:

Timestamp	Wiegand data	Format	Facility	Card	Actions
21248	00b7c31179:37	H10304	2940	100540	↶
22987	0d802d7:26	H10301	108	363	↶
24721	21601b7:26	H10301	11	219	↶
26561	2c646f1:26	H10301	99	9080	↶
Timestamp	Wiegand data	Format	Facility	Card	Actions

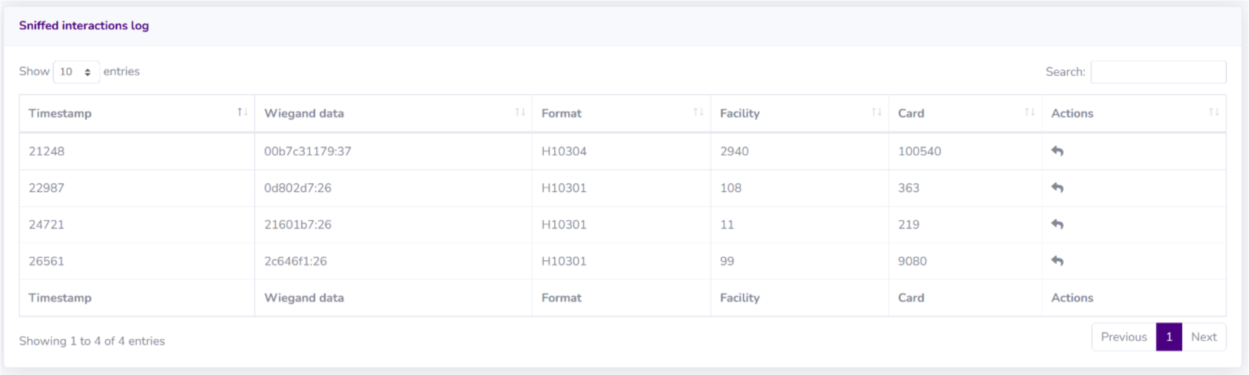
Showing 1 to 4 of 4 entries

Copyright © 2024, 2025 Jakub "lenwe" Kramarz

5.1.1. Intercepting reader communication

The device features a simple decoder for common PACS data formats in both operation modes:

Wiegand:



Sniffed interactions log

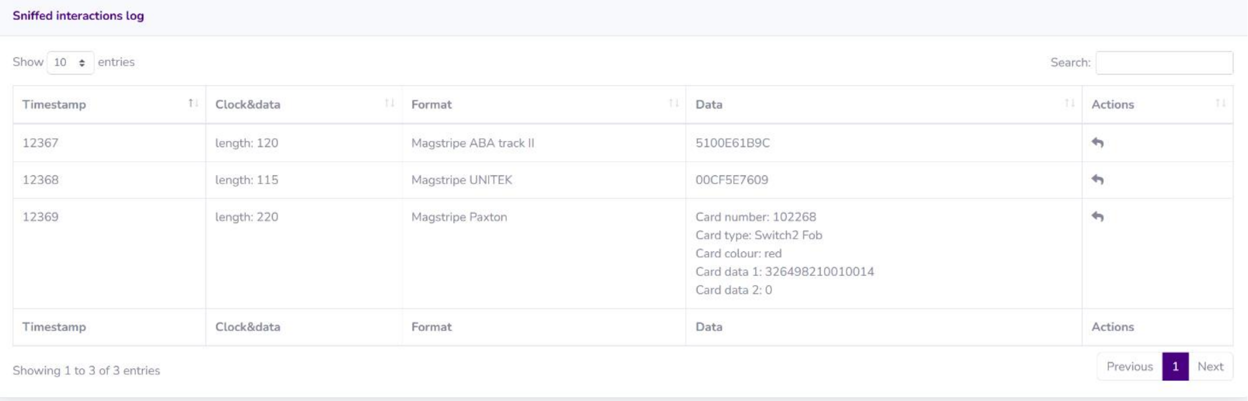
Show 10 entries

Search:

Timestamp	Wiegand data	Format	Facility	Card	Actions
21248	00b7c31179:37	H10304	2940	100540	↶
22987	0d802d7:26	H10301	108	363	↶
24721	21601b7:26	H10301	11	219	↶
26561	2c646f1:26	H10301	99	9080	↶
Timestamp	Wiegand data	Format	Facility	Card	Actions

Showing 1 to 4 of 4 entries

Magstripe Clock&Data:



Sniffed interactions log

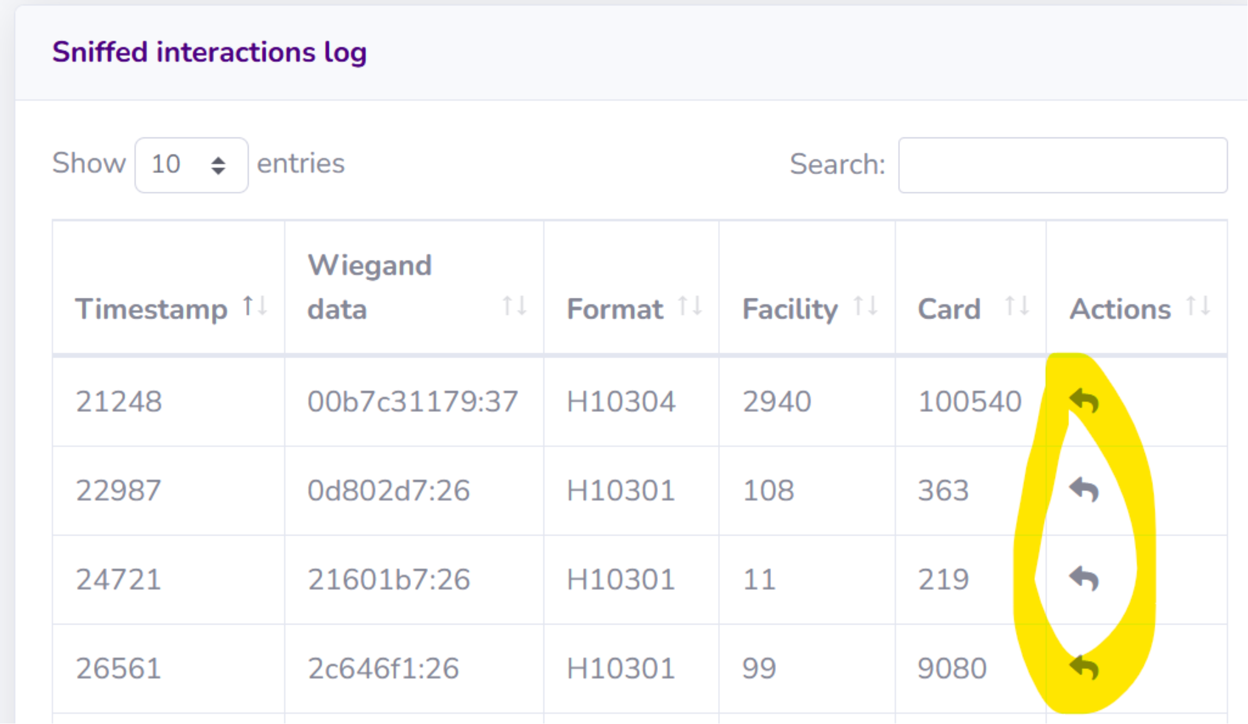
Show 10 entries Search:

Timestamp	Clock&data	Format	Data	Actions
12367	length: 120	Magstripe ABA track II	5100E61B9C	↶
12368	length: 115	Magstripe UNITEK	00CF5E7609	↶
12369	length: 220	Magstripe Paxton	Card number: 102268 Card type: Switch2 Fob Card colour: red Card data 1: 326498210010014 Card data 2: 0	↶
Timestamp	Clock&data	Format	Data	Actions

Showing 1 to 3 of 3 entries

5.1.2. Replaying sniffed cards

When accessing cards log, the operator may use an convenient option to repeat the sniffed transmission.



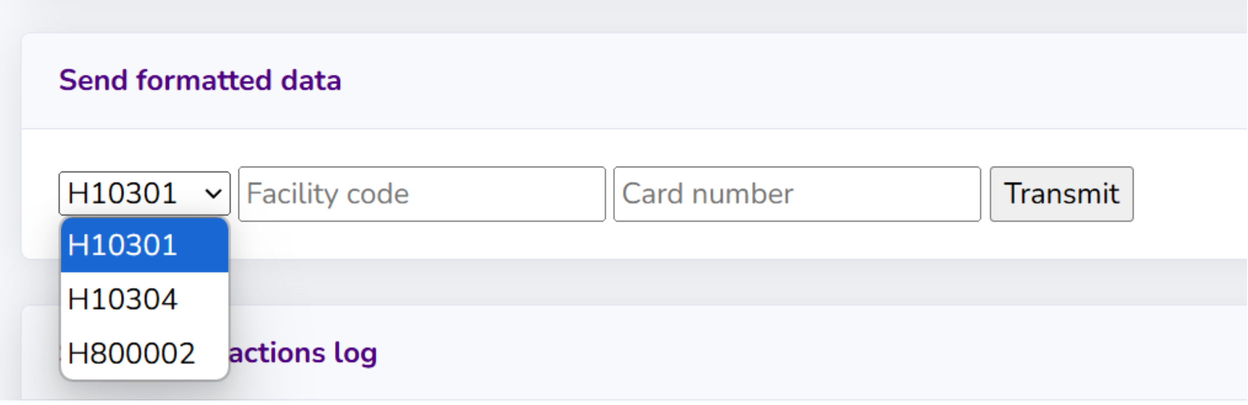
Sniffed interactions log

Show 10 entries Search:

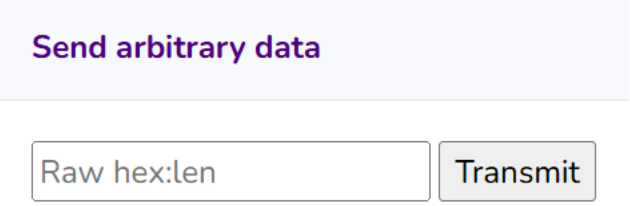
Timestamp	Wiegand data	Format	Facility	Card	Actions
21248	00b7c31179:37	H10304	2940	100540	↶
22987	0d802d7:26	H10301	108	363	↶
24721	21601b7:26	H10301	11	219	↶
26561	2c646f1:26	H10301	99	9080	↶

5.1.3. Sending arbitrary cards

The device features a simple encoder for common PACS data formats in both operation modes:

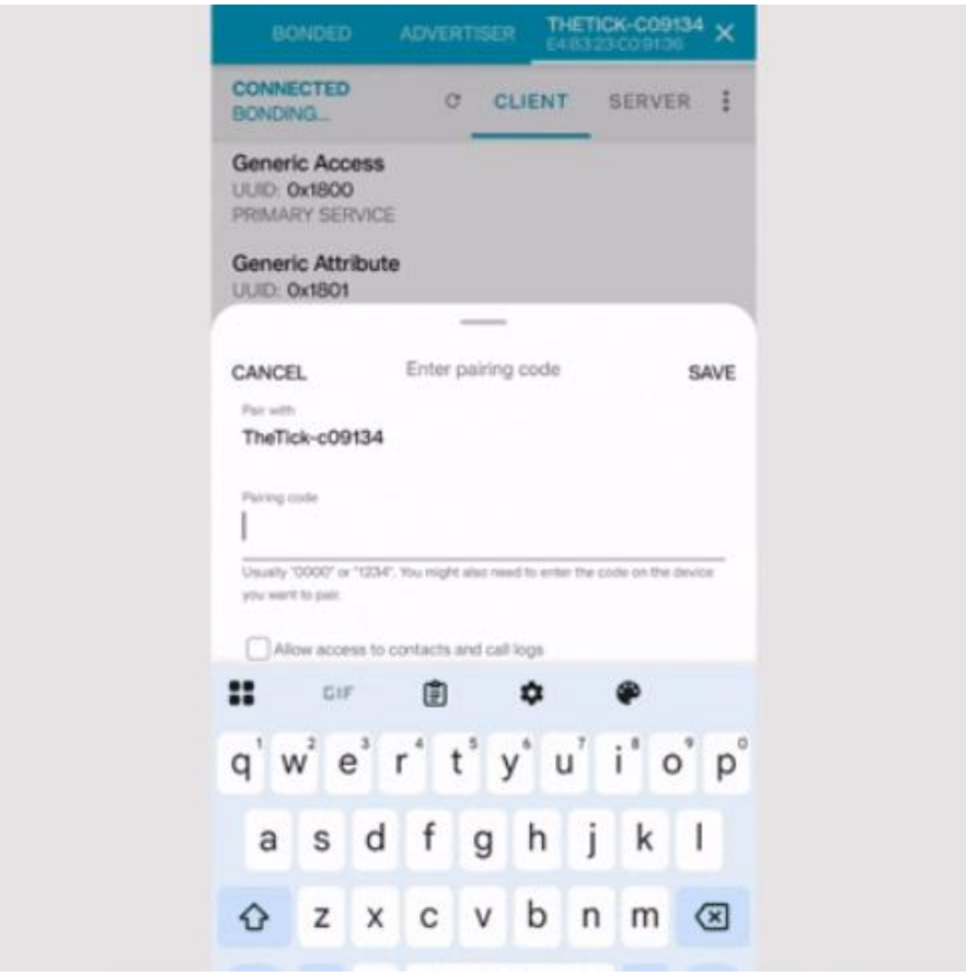


And allows transmitting arbitrary data:



5.2. BLE interface

To use BLE interface, providing the configured passkey is required:



Generic Access
UUID: 0x1800
PRIMARY SERVICE

Generic Attribute
UUID: 0x1801

Enter pairing code

Pair with
TheTick-c09134

Pairing code

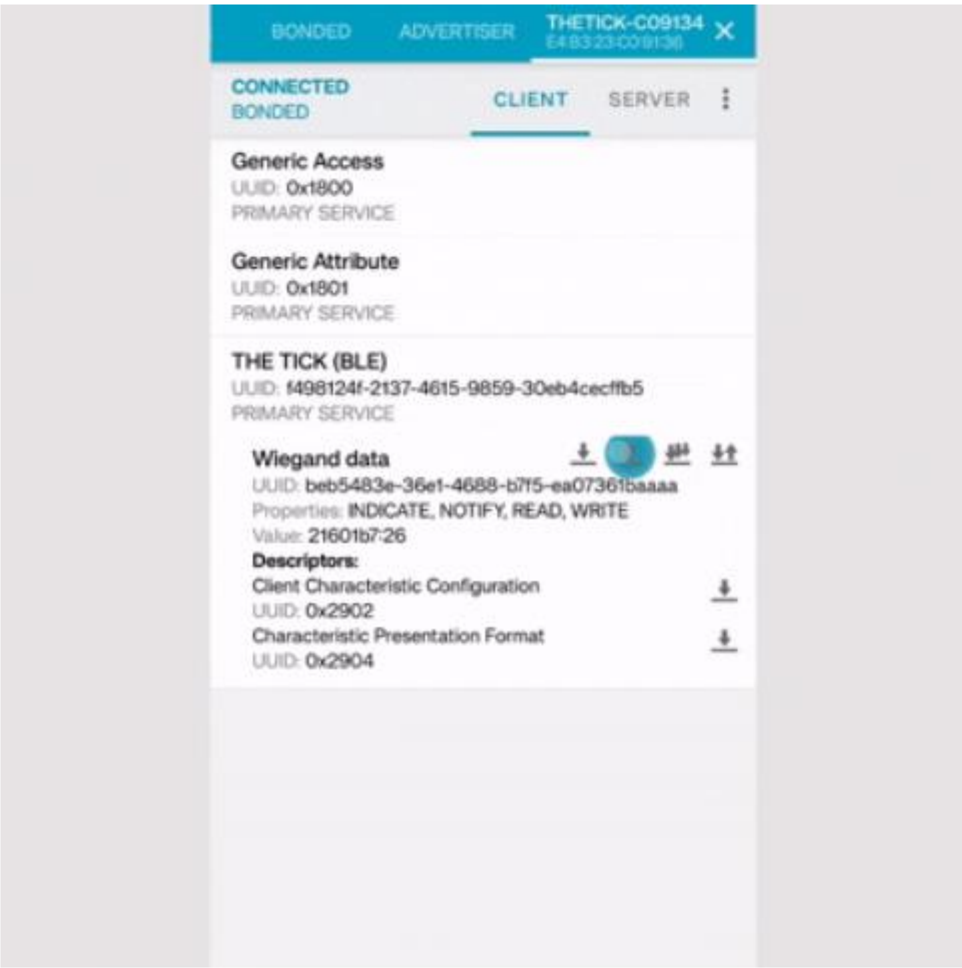
Usually "0000" or "1234". You might also need to enter the code on the device you want to pair.

□ Allow access to contacts and call logs

No special client application is currently available, so generic BLE inspection tools is required. The device uses UTF-8 values encoding.

5.2.1. Intercepting reader communication

The last card sniffed by the reader is available on BLE characteristic. It is possible to subscribe to notifications of new data:



Generic Access
UUID: 0x1800
PRIMARY SERVICE

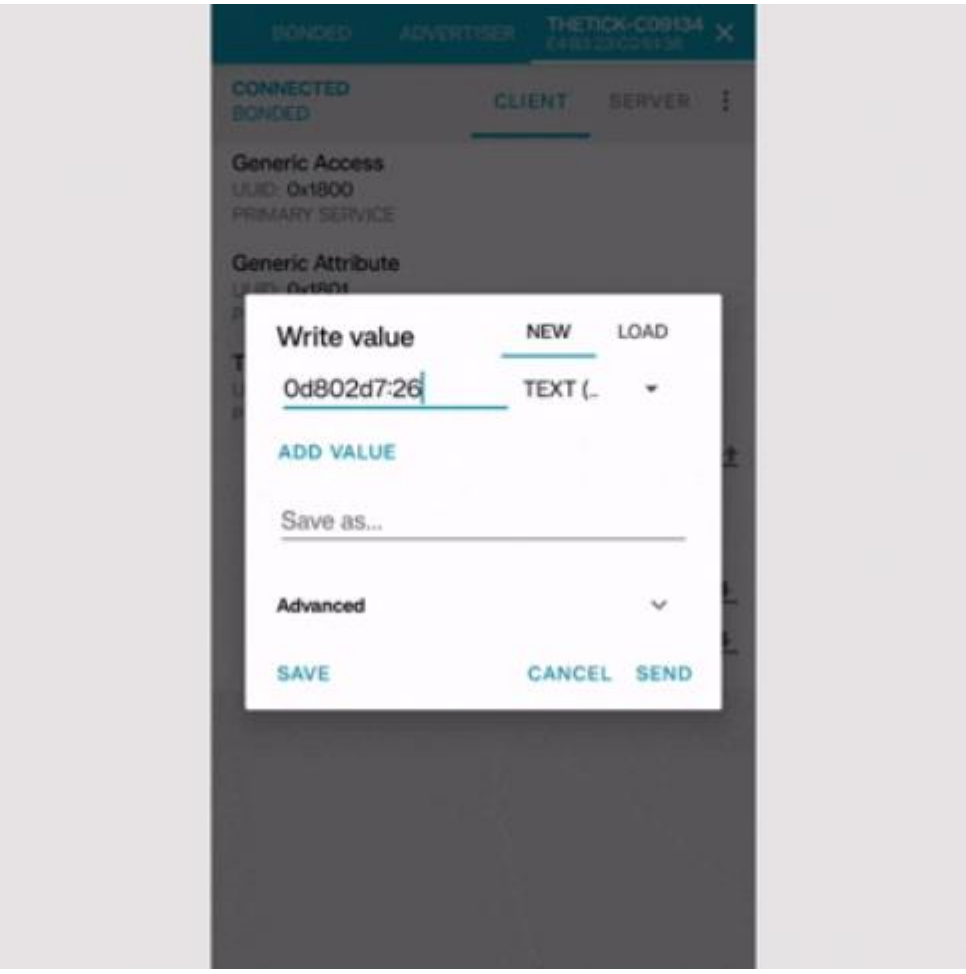
Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

THE TICK (BLE)
UUID: f498124f-2137-4615-9859-30eb4cecffb5
PRIMARY SERVICE

Wiegand data
UUID: beb5483e-36e1-4688-b7f5-ea07361baaaa
Properties: INDICATE, NOTIFY, READ, WRITE
Value: 21601b7:26
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Characteristic Presentation Format
UUID: 0x2904

5.2.2. Sending arbitrary cards

Following the same format as read from the characteristic, by writing it is possible to send arbitrary communication. By sending the same value, it is possible to replay the last card:



0d802d7:26

TEXT (..

6. CLEANING UP

6.1. Removing the device from the facility

T-taps can be opened by releasing the latch using a flat-head screwdriver.

Gently pry the cables from the connector.

6.1.1. Repairing wire insulation

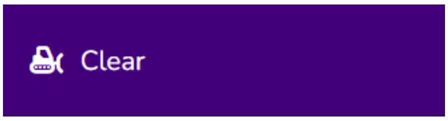
- Once the connectors are removed and wires slightly stretched, the insulation damage should not be noticeable and should not create any risk of shortening.
- As a precaution or if needed, apply a bit of insulating tape or liquid tape.

6.1.2. Verifying reader operation

- Check if it reads or the cables went bad.
- If they did, repair.

6.2. Clearing device configuration and logs

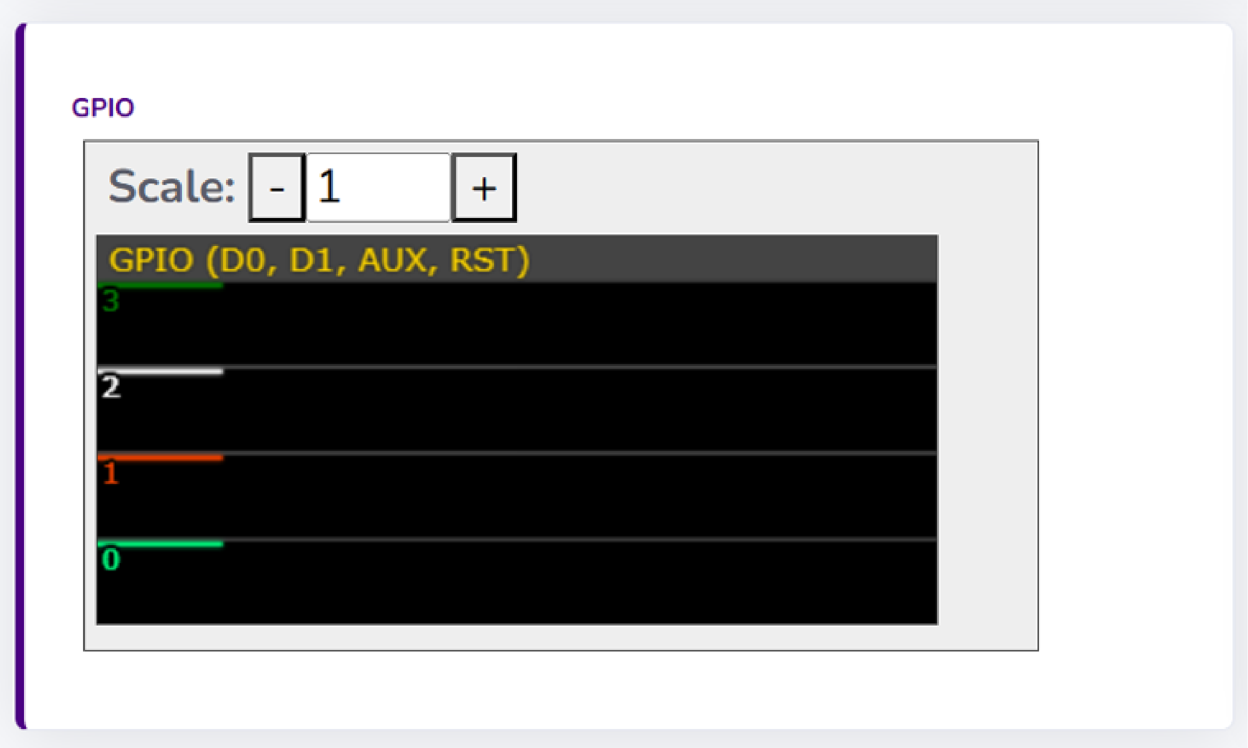
- Download device interactions log if required.
- Reset to defaults or clear the device to remove stored data:



7. DEVICE OPERATIONS BACKGROUND

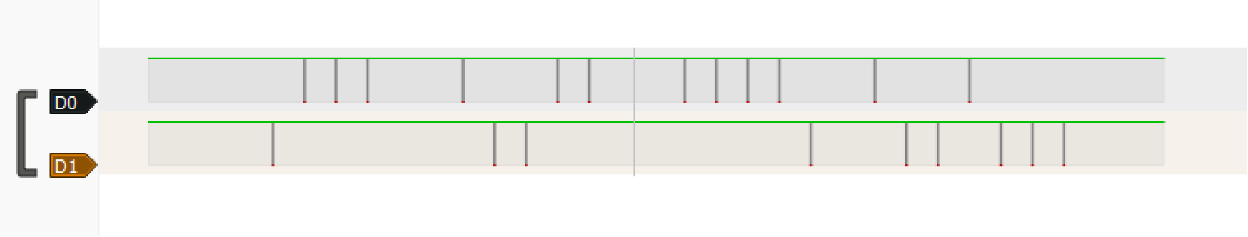
The device is capable of sampling transmission wires in accordance with various protocols. It can respond to falling or raising of the signals, differentiating between LOW (close to ground level) and HIGH (over 3.3V higher than ground level) states.

Communication wires should default to the high state. This can be inspected in the device dashboard. For transmitting capability, it can pull the lines to ground respectively.



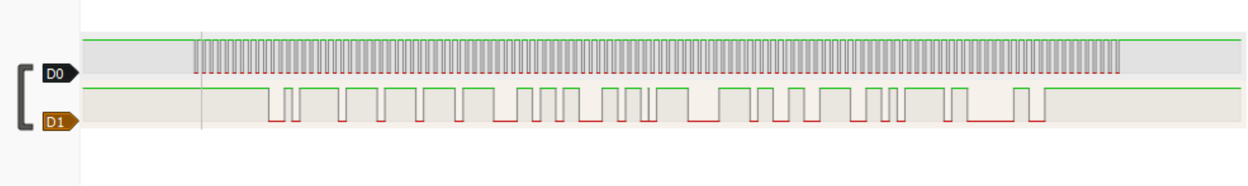
7.1. Wiegand protocol

In the Wiegand protocol both data wires are by default kept in high state. Transmission is performed by pulling the D0 and D1 lines down respectively for 0 or 1 in card number:



7.2. Magstripe Clock&Data

In the Magstripe protocol both data wires are by default kept in high state. Transmission is synchronized by CLOCK signal. On its falling edge, DATA line is sampled to read 0 (high) or 1 (low) in card number:



If transmission happens in accordance with ABA TRACK-II format, it is led and trailed by 10 zeroes.

8. DEVICE REVISIONS AND DOCUMENT CHANGE LOG

8.1. Hardware revisions

V0.1A

- Initial release.

V0.1B

- Additional USB back power protection.

8.2. Software revisions

63730c4a1eb2c74d2116fb57024f4e3ab42d946b

- Initial release.

868e477177b36d9f1d2a775cdd83b0f3abfe20f5

- Clock&Data support,
- BLE security introduced.

8.3. Document revisions

1.0

- Initial public release.

9. CONTACT

Jakub Kramarz
e-mail: Jakub.Kramarz@securing.pl
https://linkedin.com/in/jkramarz/

securing
http://www.securing.pl
e-mail: info@securing.pl
Kalwaryjska 65/6
30-504 Kraków
tel./fax.: +48 (12) 425 25