RFID and Wiegand

Short manual

Version	0.1
Author	Sandra Gilge
Date	02.05.2018
Log	v0.1

Inhalt

1 RFID

1.1 Introduction

ADATIS RFID readers can read RFID cards operating in the high frequency range
(HF - 13.56 MHz).

Various card types are supported.

Depending on the card type, there are different card data formats that can be used for access control.

1.2 Overview

The following describes the available RFID functionality depending on the hardware version.

Hardware Option	Card type	Access control application
MIFARE	MIFARE (Classic, Plus S, DESfire EV1)	UID
Universal LEGIC	MIFARE (Classic, Plus S, DESfire EV1)	UID ADATIS format BOSCH (phg) format
	LEGIC (Advant, Prime)	UID KABA (short/long)
Universal iClass	MIFARE (Classic, Plus S, DESfire EV1)	UID ADATIS format BOSCH (phg) format
	iClass, iClass SE (HID)	UID PAC

1.3 Card types

1.3.1 MIFARE

NXP's family of Mifare cards and reader ICs is built on the ISO 14443 Type A standard. Mifare cards support multiple applications, each capable of operating independently of the others through user definable key sets and access conditions.

Readers are capable of reading any variety of Mifare cards. NXP certifies both cards and readers to ensure compatibility across generations.

According to Martin Gruber, segment director for the Transit Team at NXP, Mifare is the "overall umbrella brand" for a portfolio of products. Mifare Classic is the original NXP product that was introduced in 1995-96 when the 14443 standard was first released. Mifare Plus was launched in 2009 and features higher security than Mifare Classic. DESfire is the newest and most advanced product, providing the highest level of security and flexibility.

1.3.2 iClass

HID's iCLASS platform operates at the 13.56 MHz frequency like its fellow contactless providers, but it uses the less common ISO 15693 standard, says David Nichols, director of market strategy at HID Global. The different standard, he says, enables a longer read range and longer keys for enhanced security. "We have a 64-bit key whereas others use a 48-bit key … the longer the key the more secure it will be," he says.

The decision to go with 15693 instead of 14443 centered on usability. It provided a longer read range that was similar to HID's well-established proximity card technology. When an organization switched from prox to iCLASS, we didn't want the usability or performance to decrease, explains Nichols.

The ISO 15693 specification is divided into four parts and HID is compliant with the first two parts of the standard, Nichols says. After that iCLASS deviates with a specific access control application on the card (PAC) and other changes.

HID buys standard 15693 chips for its iCLASS cards, but then makes some changes, Nichols says. HID thoroughly tests the cards and offers a lifetime guarantee. According to Nichols, this testing and reliability separates iCLASS from standardized cards.

While the cards use the 15693 standard, iCLASS readers are also equipped to read Mifare and ISO 14443 standard cards as well.

1.3.3 LEGIC

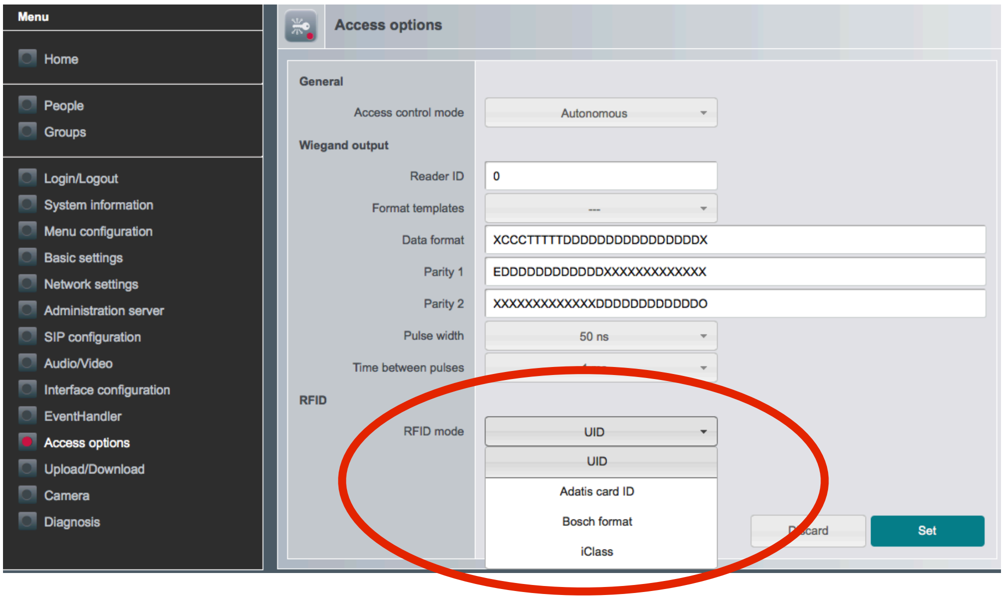
LEGIC was founded in 1990 in Zurich, Switzerland. Though the company's technology is available and in use in worldwide, it is most prevalent in Europe. LEGIC's original 13.56 MHz contactless technology, LEGIC Prime, predates the development of the ISO standards for contactless data transmission. While Prime has been widely used since its launch in 1992, a newer and more secure line called advant is now available.

The LEGIC advant system is a set of products that includes cards, readers and applications, according to Marcel Brand, manager of marketing communications at the company. LEGIC ensures its card readers are compliant with both the ISO 14443 and ISO 15693 standards as well as its own proprietary technology.

LEGIC has designed its system to be flexible so that adding applications and upgrading readers can be done simply.

1.4 Access Controll Application

The different access functions can be configured on the web pages of the terminal, whereby only those modes are available that the built-in hardware variant can also process.



1.4.1 UID (CSN)

The UID is used to identify the card itself. The UID is read when RFID cards are detected.

The simplest variant of access control is to use the UID as an identification feature. It has the advantage that different card types can be used depending on the hardware variant.

Via Wiegand only a part of the number can be output. This does not prevent different cards from generating the same Wiegand output.

The UID is read unencrypted.

1.4.2 ADATIS Format

The ADATIS format can be used in conjunction with MIFARE cards.

If the ADATIS format is used, a card number is written to the data area of the card during enrollment. The card format can only be used in combination with ADATIS readers.

The written card number is unique and it is excluded that different ADATIS customers are assigned the same card number.

Reading the data is encrypted. A unique number is guaranteed for each customer. Cards from other customers are not accepted.

1.4.3 LEGIC/KABA

If a KABA access system already exists, ADATIS readers of the hardware variant Universal LEGIC can be conveniently integrated there.

With the KABA short format only the chip ID (five digits) is read out. With the KABA long, the customer header is also read out.

1.4.4 BOSCH (phg)

If a Bosch or phg access system already exists, ADATIS readers of the hardware variant Universal LEGIC or Universal iClass can be conveniently integrated there.

1.4.5 iCLASS/PAC

HID has defined its own access format. (PAC = Personal Access Control)
ADATIS readers of the hardware version Universal iClass, can be integrated into HID access systems with this version.

1.5 Installation environment

If you want to install the reader in a metal housing, it may be necessary to tune the reader to the installation situation.

This can be done by us within the scope of a project order.

Background:

The resonant frequency of the antenna changes, especially metallic environment. Ferrite (film) also influences the resonance frequency. Therefore it is advisable or necessary to optimize the tuning of the antenna to the installation situation and to adapt the tuning network accordingly.

In addition, eddy currents can occur in the metal, which is too close to the antenna, which have a negative effect on the reading range. From this aspect it is advisable to keep metal as far away from the antenna as possible.

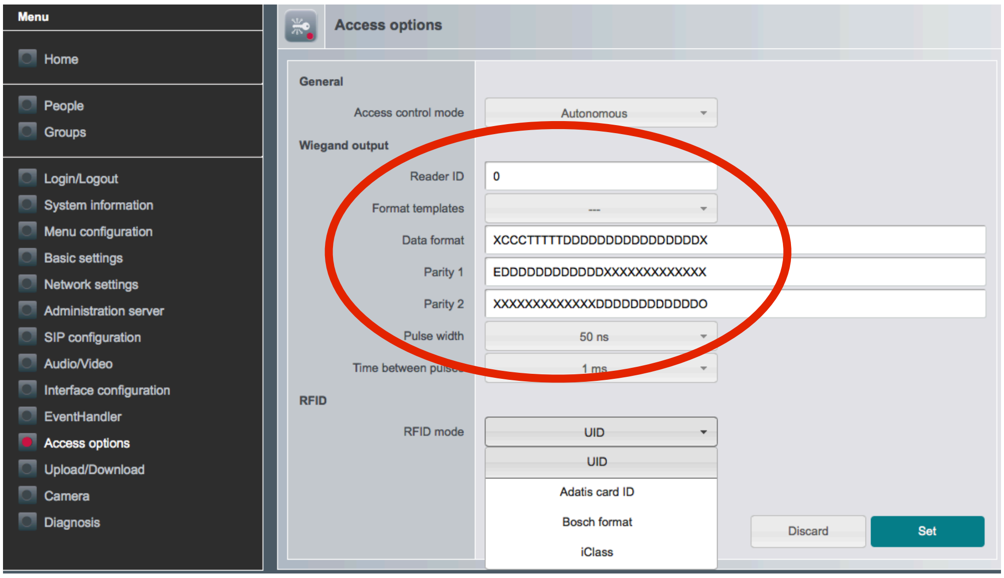
2 Wiegand

2.1 General

The Wiegand protocol is still widely used to send card data from readers to access controllers. There is only one standard data format: 26bit Wiegand with leading even parity bit and final odd parity bit, 8bit facility code and 16bit card number. The disadvantage of this format is that longer card numbers cannot be transmitted unambiguously. Meanwhile there are various proprietary non-standard Wiegand data formats of different lengths.

2.2 Configuration

In order to offer the variety of proprietary data formats, the Wiegand interface of the ADATIS reader was implemented in a configurable way. The Wiegand interface of the ADATIS reader can output a maximum of 128 bits. The content of the Wiegand output can be configured according to customer requirements on the webpages of the terminal.



The configuration is done in the WEB-GUI with 3 configuration strings.

The string "Data format" specifies where which data is to be stored. The string format is as follows:

Checkmark	Description
X	Bit is irrelevant for the data format (typically the parity bits)
C	Credential type. When used, there must always be three consecutive bits. The credential type is coded as follows: 0b100 – Face 0b001 – PIN 0b010 – RFID
T	Terminal ID When used, it must be one to five consecutive bits. The terminal ID can be configured for each terminal via the WEB-GUI.
D	Data
1	is always sent as 1
0	is always sent as 0

The strings Parity1 and Parity2 determine the rules for forming parity bits. The string format is as follows:

Checkmark	Description
E	Even parity bit
O	Odd parity bit
D	Bit is used to calculate the parity bit
X	Bit is not used to calculate the parity bit

The DATA field transported in the Wiegand bit stream depends on the credential type:

- The card number is used for RFID identification (depending on the RFID configuration).
- Face recognition uses the Personal ID. The Personal-ID can be configured for each person via the WEB-GUI.
- The PIN code is used for PIN entry.

The data have LSB byte order. If the data field is longer than the number read, the data field is filled with zeros. If the number read is longer than the data field, the number is truncated.

2.3 Examples

For the standard 26bit Wiegand format the following string can be used:

Data format	„XCCCTTTTTDDDDDDDDDDDDDDDDX“
Parity 1	„EDDDDDDDDDDDDXXXXXXXXXXXXX“
Parity 2	„XXXXXXXXXXXXXDDDDDDDDDDDDO“

Assuming the terminal ID is configured with 26 (= 0x1A = 0b11010).

The PIN 1234 is entered (=0x04D2 = 0b0000010011010010):

Wiegand output:

```
|E|CCC|TTTTT|DDDD.DDDD.DDDD.DDDD|O
|0|001|11010|0000.0100.1101.0010|0
```

A card with the card number 51334 (=0xC886 = 0b1100100010000110) is recognized:

Wiegand output:

```
|E|CCC|TTTTT|DDDD.DDDD.DDDD.DDDD|O
|0|010|11010|1100.1000.1000.0110|1
```

Face is recognized. The personnel ID = 7654321 (= 0x74CBB1 = 0b11101001100101110110001)

Wiegand output:

```
|E|CCC|TTTTT|DDDD.DDDD.DDDD.DDDD|O
|0|100|11010|1100.1011.1011.0001|1
```

Only the lower 16bit 0xCBB1 are then output from the personnel number.