# UNDERSTANDING THE CONFUSING WORLD OF RFID TAGS AND READERS IN ACCESS CONTROL

Wiegand, 120 kHZ, UHF, EPC, microwave, MIFARE, RS232, RS485, clock and data, AES, facility codes, client codes: The world of access control and vehicle identification is literally filled with concepts, techniques, acronyms and words that people outside our industry often find pretty difficult to understand and that sometimes seem very confusing. Also new entrants to this world often are overwhelmed by the number of techniques and concepts .

## Good news and bad news

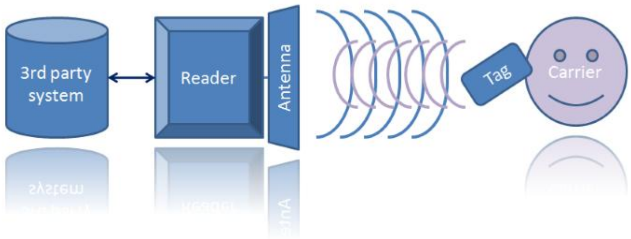
The bad news is that there really is a lot that can be learned when someone is getting involved in the procurement, supply or implementation of RFID based systems to identify people or objects like cars. The good news however is that the basic concept of RFID is pretty straightforward. Even when you really get involved with the details of programming and interpreting tags, the basic model is not too complicated. Understanding this basic concept will help you interpret a lot information that your are faced with in the right way. This article's objective is to help you on your way with understanding the most important concepts. It is not technically complete and it sometimes presents a simplified version of the related technology.

Underneath a model is presented that can be used as a framework to understand what needs to be done to have RFID tags and readers communicate successfully. It is a more detailed view on the principle of RFDI that was presented in the earlier insight with the title '[What is RFID?](#)'.

## The concept

As you may know a few things are needed to have an operational RFID system in place:

- A reader, that is connected to (or integrated with)
- An antenna, that sends out a radio signal
- A tag (or transponder) that returns the signal with information added



The reader usually is connected to a third party system that is accepting (and storing) RFID related events and uses these events to trigger actions. In the security industry that system might be a building access control system, in the parking industry it is most likely a parking management or vehicular access control system. In libraries it might be a library management system.

Let's have a closer look at access control systems. These systems usually consist of:

- RFID access control cards that, are read by
- Access control RFID card readers next to the door, that are connected to
- Access control panels (a physical controller), hardware that is able to open door locks and that is connected to
- An access control management system (software) that manages building access credentials and authorizations.

Many different access control systems exist worldwide. Most of these systems store access control rights for people (or vehicles) and also link those people to something that identifies them.

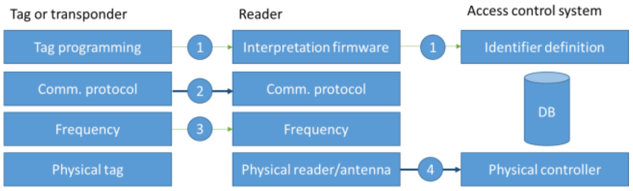
Usually a number that is stored on an access control card. When an access control card (the RFID tag) is shown to the access control reader next to the door (the RFID reader with RFID antenna), that specific number is sent to the access control panel (a physical controller). The control panel connects with the access control management software (at a server or in the cloud) to check who is connected to that number and if he/she has access to the door that is approached. When the person is authorized an event is stored at the server (for the event log book) and the access control panel is asked to open the door (by telling the physical lock to unlock).

The basic principle is easy. But a lot of software components and hardware devices are put to work to physically open the door when someone with the right access rights is showing their RFID card to the RFID reader.

You will probably know that RFID is a generic word for a wide variety of different systems that use radio frequencies to identify something. All that variation is the reason that RFID tags and readers are not always interoperable. And that again is the reason that RFID manufacturers and vendors ask so many questions when you try to purchase their systems: they would like to make sure that whatever RFID systems you procure, it is really working well.

## The model

The following model is an abstract representation of the access control system that was mentioned in the previous paragraph:



The model shows three columns with a few layers. The first column represents the tag. The tag is presented to the reader (center column) and the reader is connected to the access control system in the third column.

Each column is connected to another column at several virtual layers:

1. Tags are programmed with a number. That number needs to be in a format that is understood by the reader and that format should also be known in the access control system so that it can be processed. Tags usually have a facility code number (also called client code or facility code) and a card number. The facility code number links the tag to a specific installation, country or application. The card number should be unique for the installation with that facility code and is used to identify an individual carrier (like a person or car).

2. The number is encoded in a specific way so that it can be sent through the air. This communication protocol makes sure that tag and reader understand each other.

3. The encoded number is sent using radio waves at a specific frequency. The frequency of the reader and tag should be the same so they are able to communicate.

4. The reader is physically connected through wires in a cable with a controller that is part of the access control system. A reader communication protocol is applied to encode information sent over the physical line.

The difference between layer 2 and 3 is that in layer 3 the reader can actually ‘hear’ the tag, but it does not understand it until they speak the same ‘language’ in layer 2. The specification of layer 2 enables basic compatibility between tag and reader. The ‘EPC Gen 2’ standard used in UHF (or RAIN RFID) is an example of a standardized air interface: a combination of a selected frequency with a specified communication protocol.

Level 4 is about the physical connection between the reader (with antenna) and the access control system. What type of cable should be used and what ‘language’ is spoken? An example of that is Wiegand, a standard that is used a lot all over the world and that specifies how to use two data wires and one ground wire.

## The Wiegand confusion

The word Wiegand can cause confusion. It can be used when talking about the wiring, but it can also refer to the coding format of the card. And to make it more confusing: many readers are capable of reading Wiegand formatted cards, but can then use other types of communication and wiring between the reader and the access control panel.

The *Wiegand* effect originally refers to magnetic effect in specific wires, named after John R. *Wiegand.* This magnetic effect is used to encode and decode information.
The *Wiegand* effect is used for security keycards. The plastic keycard has a series of short lengths of Wiegand wire embedded in it.

The *Wiegand* interface is a wiring standard commonly used to connect a card reader to the rest of an access control system. The *Wiegand* protocol prescribes how to connect the wires and how to send information (numbers) from the card reader to the access control system. The *Wiegand 26* format describes how the number on the card, the card data, is formatted (8 bits for the facility code and 16 bits for the card numbers).

Other vendors have adopted the Wiegand 26 format and have made changes to it to enable use of longer card numbers or longer facility codes. Many variations exist today. The physical Wiegand cards are not used anymore, but the Wiegand format is widely used nowadays when programming a variety of access control RFID cards (HID, UHF, etc.).

## Tag programming (1)

Let's have a more thorough look at each layer of the model and show some examples of technologies that are used in that specific layer.

We talked about the programming format, mentioned Wiegand as an example and addressed the existence of facility codes and card numbers. A wide variety of programming formats is available. A few common formats are:

- Wiegand 26 bit with or without facility code
- Wiegand 37 bit with or without facility code
- HID corporate 1000 with facility code
- Magstripe (Clock & Data) with several 'Decimal' versions
- Nedap XS with customer code (also see paragraph 'facility codes and variations')
- EM4200, 40 bit ID numbers

Many cards have a preprogrammed number that is usually unique. This number is called the CSN (Card Serial Number) or UID (Unique IDentifier). It usually is advised not to use this pre-programmed number. In some rare cases it might not be unique (like with the TID on UHF tags and the 4byte ID on current MIFARE Classic cards). But more importantly: the standard card number format is not very user friendly and is not linking the card to a specific installation.

Numbers are programmed at a specific location of the tag or card. UHF cards have several memory sections. MIFARE classic and HID iCLASS cards have specific sections. MIFARE DESfire cards is organized using a file structure. Java Cards use an application structure.

In short, to program any card you will need to know:

- The number (range) and potentially the facility code
- The location on the card (sector, file, application)
- The programming format

When combi cards are used, there are two parts of the card that need to be programmed. Nedap for example sell cards that combine long-range UHF with conventional card technologies like HID iCLASS or MIFARE.

Both the UHF part and the other part of the card can be programmed with the same number in the same or different formats. Many options are possible, but it depends on your situation what we would advise.

## Facility codes and variations

We talked about the use of facility codes: this first portion of the card number format is used to help the reader (and the access control system) decide if the card belongs to the installation or if that card should be ignored. If the selected facility code for an installation is for example '1', then only cards with facility code '1' will be read and interpreted. Cards or tags with other facility codes will be ignored.

So one could say that through facility codes cards are grouped and linked to a "facility". The number in the card format that is used to identify the 'carrier' (person, car, animal, etc.) should be unique within that group of cards or tags with the same facility code. It is a security measure and decreases chances of running into duplicate carrier numbers.

The word 'facility code' has some equivalents in the access control industry:

- Site code
- Client code
- Country code
- Customer codes

These words all refer to the same thing: the grouping of cards through a number that identifies that group. It is important to be aware about the existence of these codes, since it can cause problems when building access control installation. Readers, or the access control systems that they are connected to, often are configured to accept only one facility code (or the technical equivalents). When additional tags are procured for an existing installation chances are that a facility code is used. If the new tags have a facility code that does not match the facility code in the reader or the facility code on the existing cards, the newly procured cards will not work.

The 'Nedap XS' card format uses customer codes: cards are potentially linked to specific customers. Nedap tags with this format (TRANSIT transponders, uPASS UHF tags programmed in this format, Nedap XS cards) always carry a customer code. Readers that are manufactured by Nedap and that are configured to read Nedap XS formatted tags, will instantly filter out all cards that do not have a matching customer code. Reprogramming cards often is not possible for practical reasons. Therefore it is extra important to verify what customer code is used when the Nedap XS card format is selected.

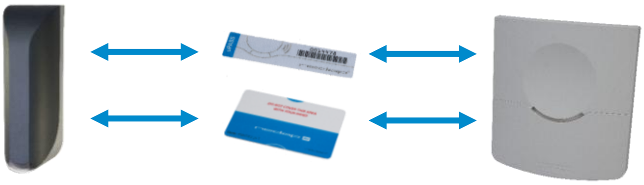
## Communication protocol (2)

The communication protocol prescribes how the content of a card or tag is sent to the reader and how it should be interpreted. It is a definition of rules for communication between two devices.
Modification of the radio signal is used to encode information but also to distinguish the radio communication from other radio signals. Commands are specified to make sure it is clear who is sending and who is listening. Algorithms are defined to make sure the right tag or card is read when more than one card or tag might be in the range of the reader (anti-collision). Many systems use proprietary air interfaces. This implies that cards/tags and reader will always have to come from the same vendor.

Nedap's TRANSIT reader for example will only work properly with Nedap TRANSIT tags. The good thing is that there is only one vendor responsible for the fact that the reader reads those tags well. The ordering process usually also is more straightforward, since clients do not have to worry about the programming format of the tags or cards.

The downside of proprietary air interfaces is that it prevents interoperability with devices from other manufacturers. Once you buy a reader with a proprietary air interface, you will have to buy cards or tags from that same manufacturer. Readers and cards/tags that fully comply with a standardized air interface are very likely to be interoperable. Of course they need to operate on the same frequency (see next paragraph) and they need to comply with the same version of the standard.

ISO144443-A for example is a famous standard for smartcards communicating at 13,56 MHz. Since many vendors have adopted (portions of) this four part standard you can find readers that support basic reading of Legic cards, HID iCLASS cards and MIFARE cards.



Another well-known standard is RAIN RFID, also known as EPC Gen 2, the standard for readers and tags/cards that operate at the UHF frequency (appr. 900 MHz). The RAIN alliance (http://www.rainrfid.org) promotes the use of ISO/IEC 18000-63 and GS1 EPC(TM) UHF Gen 2. A wide variety of readers and tags comply with these standards, which makes them interoperable.

Tags (or cards) and readers may be interoperable, it is still important to consider how to program tags. UHF tags can be programmed for example with Wiegand formatted numbers. The standard identifier on UHF tags (the so called TID) is not guaranteed to be unique and is not really fit for use in access control systems.

## Frequency (3)

RFID systems use a wide range of frequency bandwidth. The antennas on both the reader and the tag are tuned to one specific frequency to enable basic interoperability. You can however define different air interfaces for one frequency. 13,56 MHz for example is a frequency that is used in access control systems, but also in library management systems. The standardized air interfaces for these two application areas are very different. The same applies for example to low frequency access control cards (120-125 kHZ): HID Prox cards, Nedap Nexs cards and EM cards all operate in that frequency range, but they are not interoperable.
Frequencies that are often used in access control are (examples in brackets):

- LF: 120-1355 kHz - (HID Prox, EM, Nedap NeXS)
- HF: 13.56 MHz - (MIFARE Classic, DESfire, HID iCLASS, Legic)
- UHF : 860 - 980 MHz - (RAIN RFID/EPC Gen 2)
- Microwave : 2.45 GHz and above - (Nedap TRANSIT)

It is important to realize that local radio regulations prescribe specific requirements for use of the frequency. UHF for example is not globally harmonized, which means that you will need to look out for readers (and tags) that are complying to radio regulations in your country.

## Reader Communication (4)

The access control reader is physically connected to the access control system. This physical connection is called the interface. A reader communication protocol is applied to encode information sent over the wires.

Common interfaces and reader communication protocols are:

| Interface | Protocols supported: |
|---|---|
| RS232 | CR/LF, DC2/DC4 |
| RS485 | CR/LF, DC2/DC4, OSDP, Profibus |
| Èthernet | TCP/IP |
| Wiegand | W26-bit, W32-bit |

These connection methods often can be made wireless.

OSDP is a standard that is managed by SIA (Security Industry Association) that is about to be widely embraced by the security industry as a standard (based on RS485) for connecting readers with access control panels (controllers). Information about OSDP can be found here: http://www.siaonline.org/Pages/Standards/OSDP.aspx

Nedap's uPASS Access reader is an example of a reader that is ready for OSDP deployment.

## Keep it simple!

We do hope this insight helps you to understand the basic concepts of how to get access control cards, readers and controllers to work.

The basic model is simple. And although many variations exist, this basic model should help you understand how to relate all these words and concepts to each other.

Need additional information or help? Do not hesitate to contact us.