PRODUCED BY APERTURE LABS LTD. IN PARTNERSHIP WITH CPNI

Automated Access Control System

Token Selection Guide

Draft V 4.0

Automated Access Control System

Token Selection Guide

Document History

Version	Purpose	Originator	Reviewed Aperture Labs	Reviewed CPNI	Date
1	Draft for review	Andy Ritchie Adam Laurie	Andy Ritchie Adam Laurie		31/03/09
2	2nd draft with CPNI comments, document split and glossary of terms added.	Andy Ritchie Adam Laurie	Andy Ritchie Adam Laurie		09/04/09
3	Inclusion of comments	Andy Ritchie Adam Laurie	Andy Ritchie Adam Laurie		10/6/09
4	Reclassified from restricted to not protectively marked	Andy Ritchie Adam Laurie	Andy Ritchie Adam Laurie		10/7/09

© Aperture Labs Ltd. 2009 info@aperturelabs.com

The text of this publication may not be reproduced, nor any talks or lectures based on material contain within this document be given, without written consent of Aperture Labs Ltd and the Centre for the Protection of National Infrastructure

Table of Contents

Introduction

The purpose of this guide is to provide a background into Access Control Token technologies and the implications they may have when used as part of an Automated Access Control system.

It is intended to inform you of the basics of how access control tokens work, and to help you understand the strengths and weaknesses of different token features.

Background

History

Early security solutions were all about protecting physical assets – whether in the form of valuable items such as crops, treasure, or personnel such as military forces or civilian populations.

Protection took the form of physical barriers such as moats, fences and gates, supplemented by armed guards. 'Locking' of gates or doors was performed from the inside, for example by raising a drawbridge or placing a bar across a gate, and so the security systems were reliant on activity from a trusted individual or group within the secure area. To gain access to a secure facility, a challenge/response, or some form of recognition would take place, whether in the form of a secret pass phrase exchanged between the guard and the visitor, or through visual confirmation of a friendly face or letter of introduction (usually supplemented by a seal or stamp of authority), which, when successful, would result in the barrier being moved and access granted.

The first to 'automate' this process, and provide a means of self-opening the barrier, are thought to be the Egyptians, who invented locks which used wooden pins that dropped into holes in the locking bolt that could be moved out of the way by means of a wooden 'key' with pegs that lifted the pins out of the bolt and allowed it to be slid clear. This is the same principal as that of the modern day 'pin-tumbler' lock.

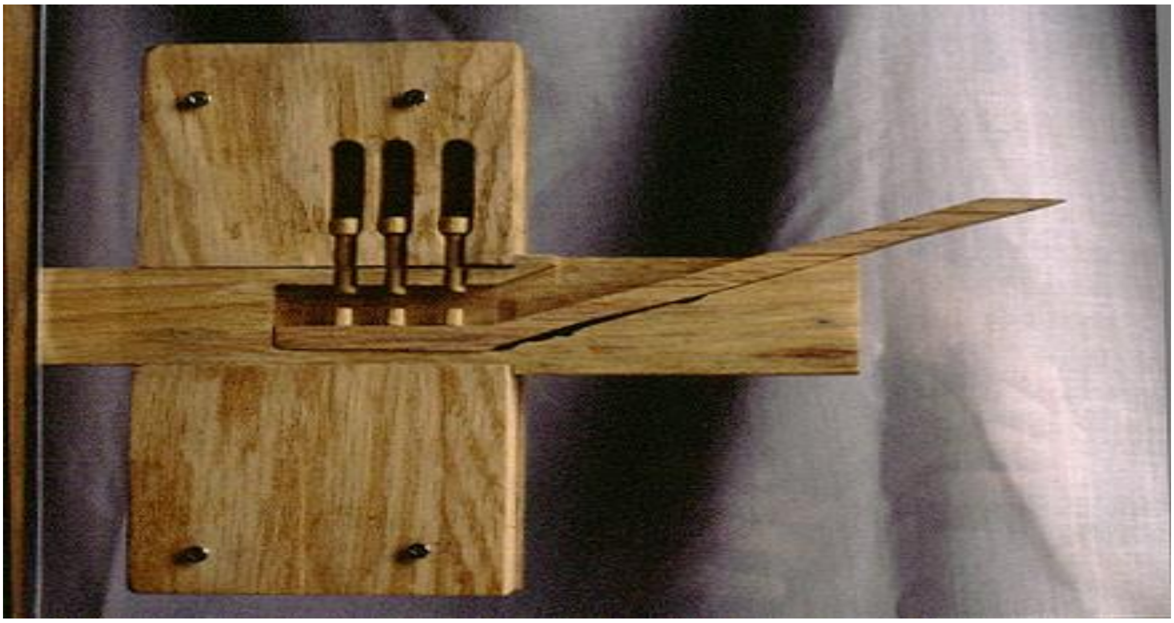


Illustration 1: Egyptian wood pin-tumbler lock

We can also see parallels between the challenge/response and modern access control systems using cryptographic or other token technologies that provide the 'recognition' or authentication of the visitor.

Authentication Methods

Authentication – the process of determining that an object or person is what it claims to be, can broken down into three areas:

- Something you know
- Something you have
- Something you are

Each can be used independently, or they can be combined for greater effectiveness.

PINs and Passwords – Something You Know

Sun Tzu, the ancient Chinese war lord said: “*a secret is not a secret if it is known to more than one person”*.

In this context, a genuine secret is of no particular use as it cannot be verified, but a 'shared secret' can, and can be utilised to confirm that the holder of a token or the person accessing a control is genuine. An example of this being the PIN number on your mobile phone's voicemail, which should be known only to you and the network operator.

Tokens – Something You Have

A door key is a common form of token that is verified by the very act of opening the lock. The correct token will cause it to open, whilst an incorrect one will not. An example of combining

'Something you know' with 'Something you have' can be found in the bank ATM card, with the card itself being the 'Something you have', and the PIN the 'Something you know'.

Biometrics – Something You Are

Finally, visual recognition of friendly forces or an individual would have traditionally provided the 'Something you are', but with the advent of Biometrics, we can now use fingerprints, iris scans, DNA or a number of other technologies to 'prove' you are who or what you claim to be. An example might be the fingerprint scanners used at Walt Disney World to ensure that season or multi-day tickets are being used only by one individual.

Automated Access Control Systems

Access Control 'Tokens' have long been used to automate the process of opening barriers, such as a door or a gate, or identifying an individual to a guard for inspection against previously stored credentials.

These tokens come in a variety of formats, and use a number of differing technologies to accomplish the task of 'reading' their contents and identifying the user. These technologies are as diverse as:

- Optical Barcode
- Wiegand Wire Code
- Mechanical Slot/Hole Punch
- Magnetic Stripe
- Smartcard Chip
- RF (Radio Frequency)
- RFID (Radio Frequency Identification) / NFC (Near Field Communications)

AACS Token Schemes

Tokens are simply a physical embodiment of a secret code. They are devices that when 'read' disclose the code, and some tokens are more secure than others. This is mainly due to the arms race between the security industry and the criminals and terrorists that seek to exploit flaws in security schemes.

Some of the tokens schemes may seem naïve by today's standards, but it's easy to forget that when they were conceived, many of these technologies were state of the art.

One of the critical parts of token security is exactly how the token gives up its secret code. Is it easy or hard? Does it give up the secret to anyone, or just those that have a need to know? How does it protect its secret and how does it authenticate those that require its disclosure?

Authentication Methods

There are many different types of authentication, some simple, some more complex. We will cover some base methods here to allow you to spot them when they are being used by tokens.

- Identifier
- Shared Secret

- Public Key Cryptography (also referred to as Public Key Infrastructure or PKI)

Identifier

This is the simplest method of authentication. The access control system and the token both know an identical piece of information, normally referred to as a 'UID' (Unique ID). When the token is presented/inserted/swiped through a reader, it gives up its UID to the reader, which transmits it to the access control system. The access control system compares the UID to its stored copy, and permits access if they match.

Shared Secret

This can be an effective method of authentication if used correctly. Both the token and the reader know the same secret information. But how do they authenticate each other without sending the secret which would allow it to be intercepted and read? A common method employed is known as a Challenge-Response. The reader generates a random number of 16 bits, for example. It then takes the random number and performs a mathematical function on it, which includes the shared secret. A good example of this is encryption: the random number is encrypted with the shared secret as the key. The result and the original random number are sent to the token. The token performs the same operation on the random number using its copy of the secret. If the shared secrets are the same, it will arrive at the same answer as the one sent by the reader.

A simple example is shown below. We will replace the encryption algorithm with simple multiplication.

Shared Secret = 5

Random Number = 4

Encrypted Random Number = 20 (5 * 4)

Challenge = 4, 20

This challenge is transmitted to the token, which performs the same operation. If the token ends up with the same 'encrypted' solution as the token, then it knows the shared secrets are identical without the secret ever being transmitted between the reader and card.

It is important to note that this mechanism allows both the reader to authenticate the token, and the token to authenticate the reader, so neither will be fooled into giving up its secrets to an unauthorised counterpart.

Public key cryptography

Public key cryptography solves two problems in one: It allows an encrypted conversation to take place without the secret keys being transmitted in plain text, and also provides a means of verifying the message originated from the original owner of the key.

This system uses asymmetric cryptographic algorithms, in which the key used to encrypt is not the same as the key used to decrypt, and one cannot be derived from the other. Each user has both a 'Public' and a 'Private' key, and anything encrypted with the public key can only be decrypted with the private key. The same also works in reverse – anything encrypted with the private key can be decrypted with the public key.

In practice, the user publishes their public key, and keeps their private key secret. When somebody wishes to communicate with the user, they encrypt the message with the public key, and only the user's private key can decrypt it.

This also allows the user to create a digital 'signature' for a message. The user writes a message and creates a 'checksum' of the message. The checksum is encrypted with the user's private key and appended to the message, which is sent to the recipient. The recipient also checksums the message, then decrypts the included checksum and compares the two. If they match, then it is proof that the message was sent by the user, and not tampered with en-route. This forms the basis for digital certificates, which are used to confirm the identity of on-line assets and users today.

Types of Tokens

Physical Key

The invention of the lock and key was one of the most important advents of security technology. For the first time, it was possible to rely on a security device and not a guard force. This was both cost saving, and did not rely on personnel that could be potentially subverted.

The most common modern lock is known as a pin tumbler lock, an example of which is shown below.

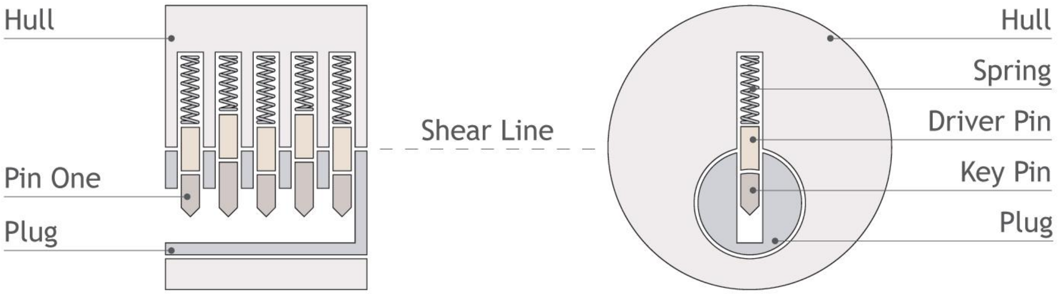


Illustration 2a: Pin Tumbler Lock in locked state

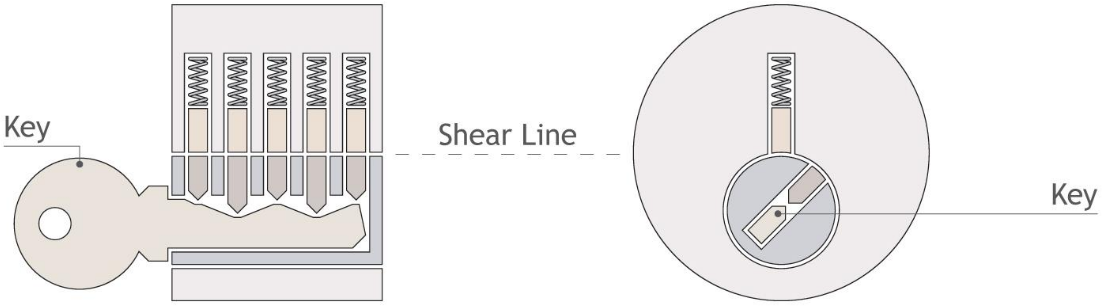


Illustration 2b: Pin Tumbler Lock in unlocked state

In the lower image you see the lock in the locked state. The driver pins are pushed down into the plug by the springs, preventing the plug from rotating. In the top image you see the key inserted. The cuts on the key's blade lift the key pins to the correct height, aligning the top of the key pin with the top of the plug and pushing the driver pins up into the cylinder. This point is known as the shear line. At this point all the driver pins are in the cylinder and all the key pins are in the plug (neither lie across the shear line), and the plug can be turned, opening the lock.

Security of a basic pin tumbler lock is provided by the profile of the key and the 'code' which is the number and depth of cuts on the key blade, which is known as the key's bitting.

The oldest form of copying a key's code involved pressing the key into a small box filled with wax or clay, to leave an impression of the key's cuts and profile.

Illustration 3: Key impression

Modern locks and keys come in a huge variety of different types, employing a large range of anti-duplication technologies. From the ineffectual “Do Not Duplicate” stamp, to special cuts, “restricted” blanks, and sliding components encased into the key blade.

Physical locks have a common disadvantage compared with electronic locking systems, in that there is no record of who has accessed the lock and when (audit trail).

Mechanical Slot / Hole

This type of card was used as the very first ATM card and is still used today in some hotel locking systems.

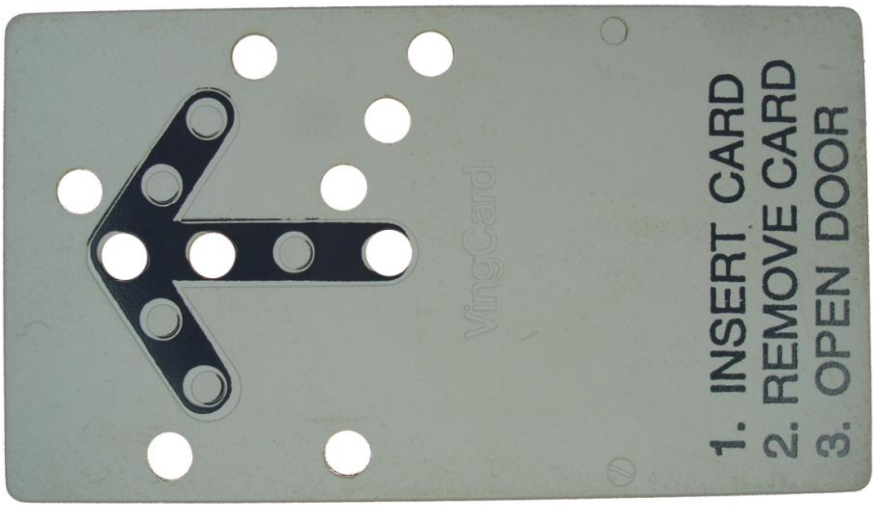


Illustration 4: Mechanical hole card

Like a computer punch card, data is represented by specific locations on the card and whether there is a hole or not in that location.

As you would expect, this card gives up its “secret” code to anyone who happens to glance at the card.

Barium Ferrite

Barium ferrite cards were the original 'Card Key', and consist of a compound (Barium Ferrite), which can be combined with a thermoplastic and magnetised. The cards have regions magnetised in a pattern to form a particular code, sometimes including different magnetic polarities. When inserted into or placed upon a reader, sensors detect the regions and decode the data to a specific user id, which is then passed to the access control system for verification.

Illustration 5: Barium Ferrite card

Using a magnetically sensitive film placed over the barium ferrite card, it is possible to view the magnetic regions encoded into the card:

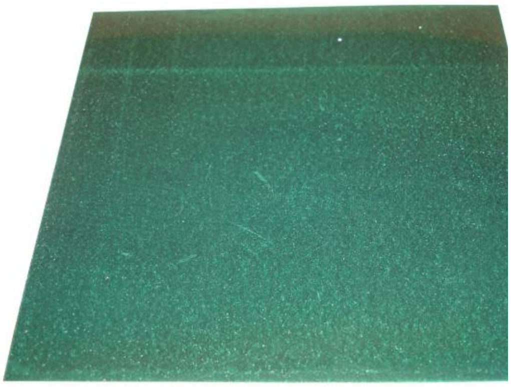


Illustration 7: Magnetically sensitive film

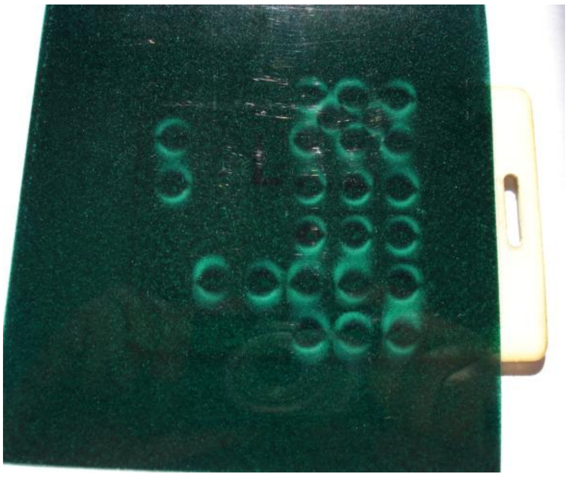


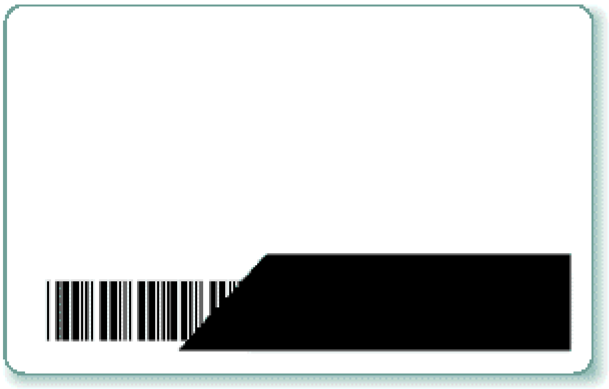
Illustration 6: Film over Barium Ferrite card showing encoded magnetic regions

Here the base technology is nearly identical to the Mechanical Slot/Hole card system, with just a different medium being used, and the similarity to the punch card shown above is obvious. The encoding here is 'hidden' by using magnets, and was therefore deemed more secure. In addition to the pattern of discrete magnetic regions, the regions themselves can be encoded with either North or

South magnetic polarities giving a greater number of potential combinations.

Barcode / Concealed Barcode

This type of card is printed with a simple Barcode, sometimes obscured by Infra-Red permeable, but visible-light blocking film.



This card provides little in the way of security, giving up its code to the casual viewer or, if concealed, a viewer with a powerful torch which can be shone through the plastic from behind, revealing the Barcode to the naked eye.

Magnetic Stripe

The magnetic stripe card was the first computer data storage card to gain wide acceptance, and is still in common use today, in banking and access control in the hotel industry. The card has a length of magnetic tape laminated into its fabric, which is used to store data. In most modern applications the data is laid out in three tracks, written along the strip by a read/write head similar to that used in a cassette recorder. The head consists of a ring of material with a narrow slot cut in it. Opposite the slot the ring is wound with wire that is connected to the electronics.

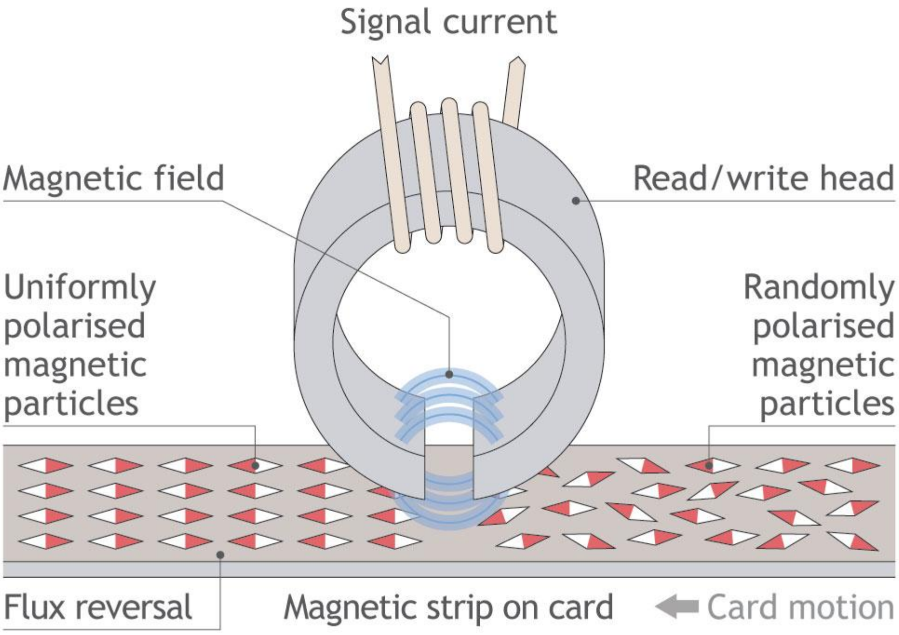


Illustration 8: Encoding a Magnetic Stripe

When the coil is energised, it creates a magnetic field in a particular polarity (North or South) across the gap in the ring. This gap is placed in contact with the tape, and the tape is moved across the gap.

The data is written to the tape by reversing the current flowing through the coil and therefore reversing the magnetic field across the gap. Such transitions are known as 'flux reversals', and it is these flux reversals that constitute the data being written to the tape.

There are a number of standards which define the layout of the data tracks on the tape and how that data is encoded onto the individual tracks:

ISO Number	Description of Standard
7810	Physical Characteristics of Credit Card Size Document
7811-1	Embossing
7811-2	Magnetic Stripe - Low Coercivity
7811-3	Location of Embossed Characters
7811-4	Location of Tracks 1 and 2
7811-5	Location of Track 3

7811-6	Magnetic Stripe - High Coercivity
7813	Financial Transaction Cards

There are three tracks on a standard ISO magnetic card:

Track 1 uses a recording density of 210 Bits Per Inch (BPI) and stores 79 alphanumeric characters using 7 bits per character.

Track 2 uses a recording density of 75 Bits Per Inch (BPI) and stores 40 numeric characters using 5 bits per character.

Track 3 uses a recording density of 210 Bits Per Inch (BPI) and stores 107 numeric characters using 5 bits per character.

These tracks can be visualised using a suspension of fine iron or magnetic particles in carbon tetrachloride. This substance was sold commercially under the name of 'Magnasee', and was used for checking the alignment of tape heads, but has now been discontinued as carbon tetrachloride has been identified as being a carcinogen. A safe alternative is now marketed under the brand name of 'QView'.

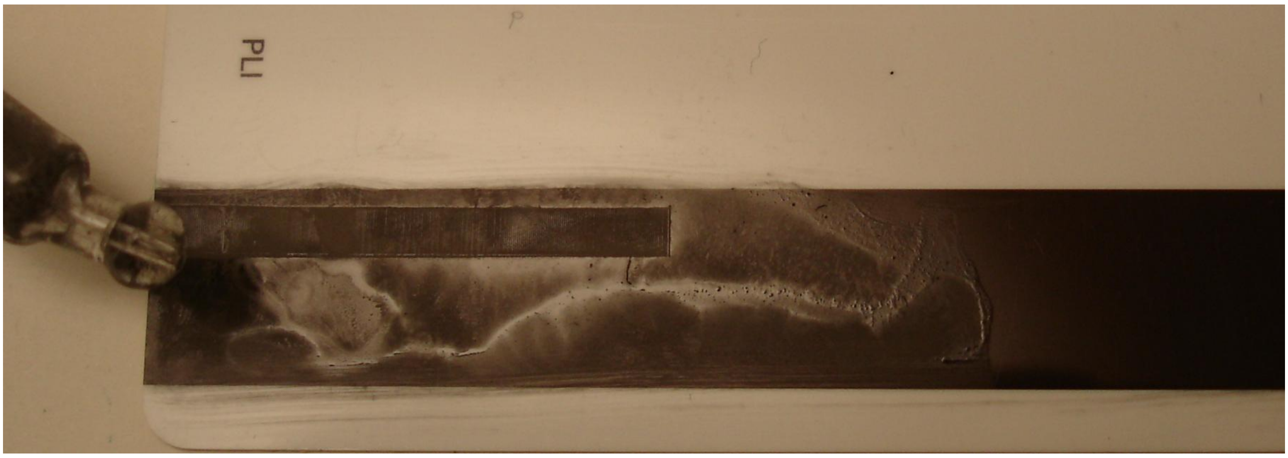


Illustration 9: Magnasee application

Here the Magnasee is being applied to the magnetic stripe on the card.

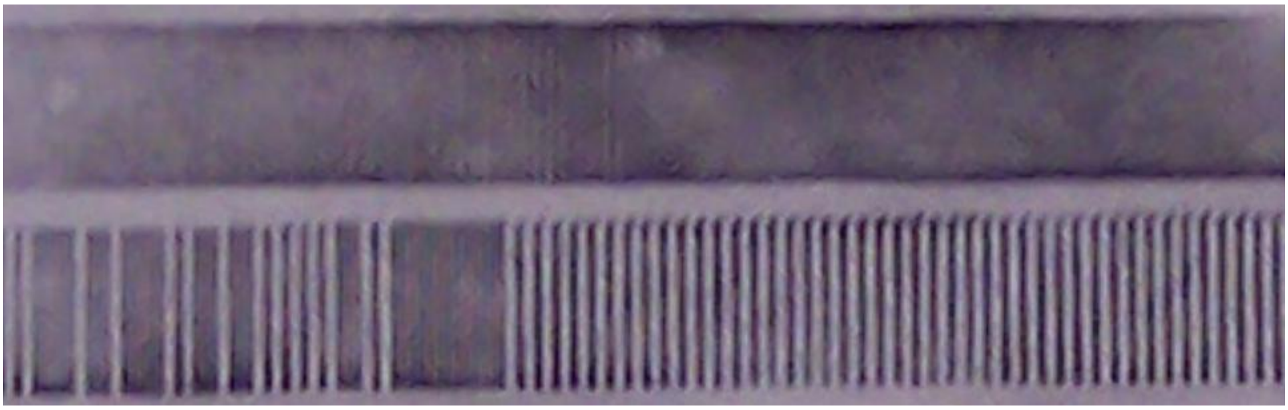


Illustration 10: Magnasee imprint

After the Magnasee has dried, it is possible to see the flux reversals clearly. The example above was removed from the card by placing a piece of clear sticky tape over the magnetic stripe, and then simply peeling it off and then affixing it to paper. In this example you see two tracks, the upper written at 210 bpi and the lower at 75 bpi.

As some manufacturers move the location, or even change the size of the tracks, as a so called "security feature", visualisation can provide important clues to an attacker. Such "security" features are easily defeated once they are known. Another more complex method of attempting to secure magnetic stripe cards is to create a magnetic image of the entire stripe, including natural imperfections, and a checksum of this image is stored on the card and checked each time the card is read. Further attempts at security include writing a code into the magnetic material during manufacture that cannot be changed by normal card writers.

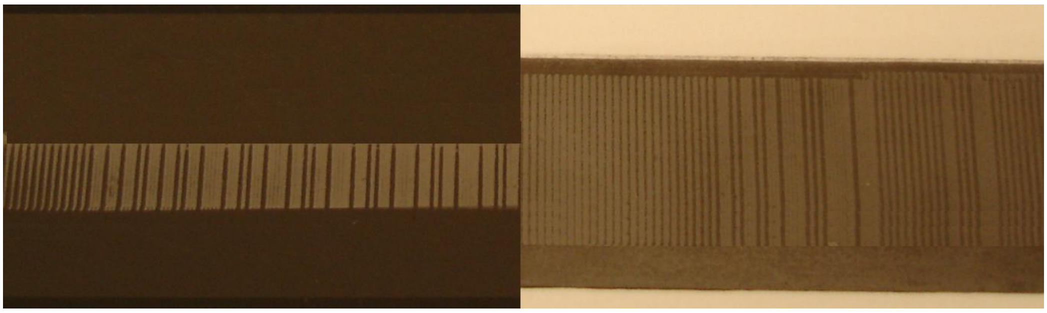
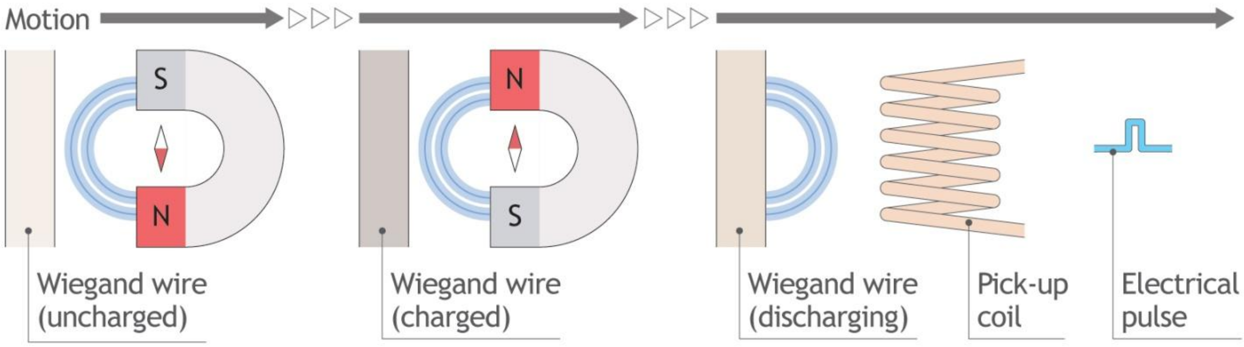


Illustration 11: Standard magnetic stripe width (left) and Non-standard stripe width (right)

Wiegand Card

Wiegand is a notable name in the security industry - not only is it the name of the magnetic effect (the Wiegand *Effect*) that is found in a specially made wire (the Wiegand *Wire*), it also refers to the cards using that wire (Wiegand *Cards*), the layout of the data encoded into the cards (Wiegand *Format*), and even the protocol used by the reader to signal the code back to the access control system (Wiegand *Electrical Protocol*).

The Wiegand *effect* is observed in wire that has been manufactured to create two separate magnetic regions within the wire itself: the core and the shell. Both regions react slightly differently to a changing magnetic field, and the wire will emit a short burst of magnetic energy when subjected to a change in an external magnetic field. This burst can be detected by a device similar to a magnetic tape head.



Here you see the uncharged Wiegand *wire* on the left being passed by a North-South polarised magnet. The Wiegand wire “stores” a magnetic charge, and releases it (discharges) as a short burst when it is moved passed an oppositely polarised magnet (South-North). This burst is picked up by a detector coil and transmitted as a pulse of electricity.

The Wiegand *card* contains short pieces of Wiegand wire, arranged in a pattern in the card. The pattern contains two rows of wire, with one row representing a binary one, and the other row a binary zero. The wires are interleaved so that when swiped through a reader with a separate read head positioned over each row, a stream of ones and zeros is detected.

An example of a Wiegand card is shown below.

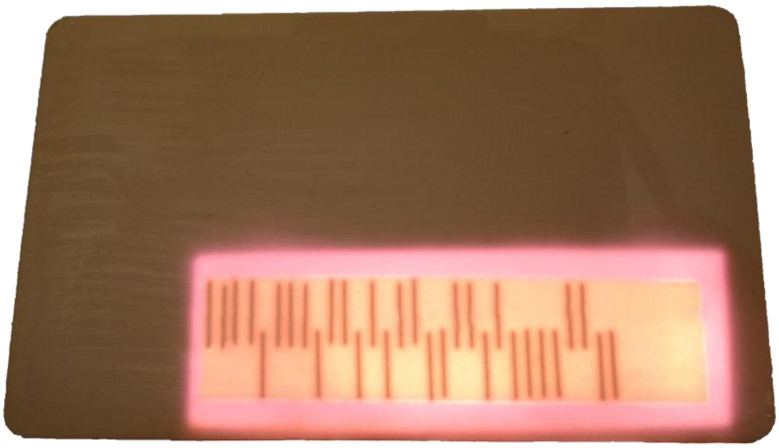
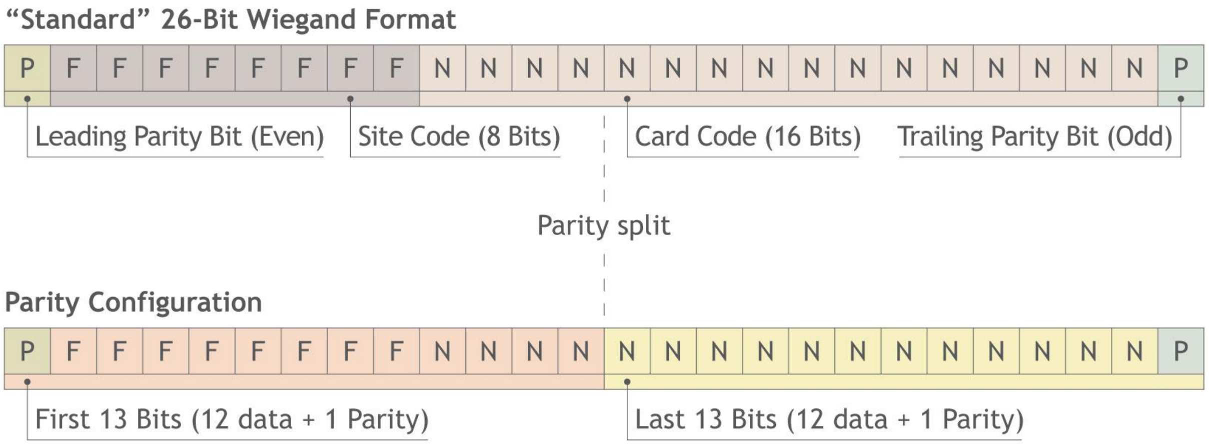


Illustration 12: Wiegand card

The card can be made to give up its secret code with the help of a torch shone through the plastic.

The Wiegand *format* is the layout of the data bits on the card. This can be specific to the manufacturer, however there is a standard format that is known as the 26-Bit Wiegand Public Format or Standard 26-Bit Wiegand Format.

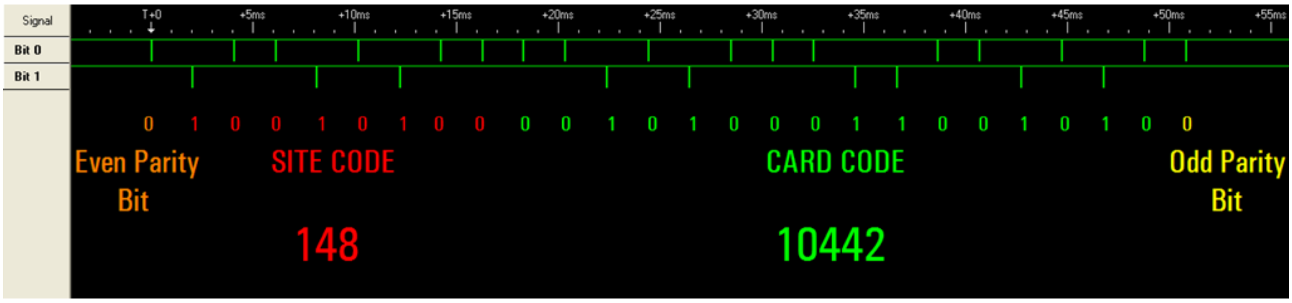
The 26-Bit format consists of an even parity bit, 8 data bits that define the facility or Site Code, 16 bits that define the Card Code, and an odd parity bit. The parity bits are used as a simple data integrity check. Even parity means that the parity bit will change to ensure all the bits it's checking will add up to an even number, and odd parity will do the same, but change to ensure an odd number is present.


"Standard" 26-Bit Wiegand Format
P F F F F F F F F N N N N N N N N N N N N N N N N P
Leading Parity Bit (Even)
Site Code (8 Bits)
Card Code (16 Bits)
Trailing Parity Bit (Odd)
Parity split
Parity Configuration
P F F F F F F F F N N N N N N N N N N N N N N N N P
First 13 Bits (12 data + 1 Parity)
Last 13 Bits (12 data + 1 Parity)

In this case the leading (even) parity bit protects the first 12 data Bits and the trailing (odd) parity Bit protects the last 12 Bits. This scheme has the added advantage that because the even parity section always comes first, the reading system can detect if the card was swiped "backwards", and automatically reverse the data stream to compensate.

As well as the 26-Bit format, there are many other formats created by different manufacturers, using different numbers of bits, and with different parity or checksum schemes, and often including different data in the code.

The Wiegand *Electrical Protocol* is used to connect most access control readers to the access control system, and is included here for completeness. Two wires carry the data read from the card back to the access control system from the reader. One wire handles all the “1” Bits and the other handles the “0” Bits. The wires are normally at 5 volts, and the presence of a Bit is signalled by the wire dropping briefly to 0 volts.



Above you can see the data that is transmitted by the reader down the wires to the access control system. As you can see, the ID is 26 bits, and is in the standard 26-Bit format. Removing the parity bits, the first 8 bits represent the number 148, which is the site code, and the next 16 bits represent the card number, in this case 10442.

Incidentally, you will notice that the arrangement of bits in the image above is almost identical to the physical layout of the Wiegand wires embedded into the card.

Contact Smart card / Chip Card

The smart card contains a small microprocessor and memory device implanted directly into a standard plastic card. The microprocessor unit can perform a variety of functions including authentication using strong cryptographic algorithms.

Illustration 13: Smart Card

Contact smart cards have not been seized on by the physical access control industry, but they have found their uses in other security applications. They have now entered our daily lives as the ubiquitous Chip & PIN cards issued by banks and credit card companies, and as the Subscriber Identity Module (SIM) for GSM mobile phones and subscriber access cards for Satellite TV.

There are many types of contact smart card available, each with a different level of security.

Like all security solutions, correct implementation is key. It is easy to take a collection of secure components and integrate them in a fashion that destroys the overall security of the system.

iButtons

An iButton is a small metallic capsule which contains a small integrated circuit. This circuit communicates via a '1-wire interface' (in reality two wires: a signal wire and a ground wire).

Illustration 14: iButton

Here you see an iButton connected to a small plastic carrier suitable for attachment to a keyring.

Like smart cards, there are several different types of iButton, some simply transmitting an ID (the A variants), and others with encryption capabilities (the S variants).

Although used for access control, they tend to be low end or standalone systems.

You will also find these devices used as data loggers, identification devices in point of sale applications (e.g. Pub tills), and, most notably, for the security industry in guard tour products.

Illustration 15: iButton Door Lock

Infra-red

One of the oldest electronic access tokens, often used to open garage or car doors, or to disable alarm systems. These devices work by sending a 'carrier' signal when the button is pushed, which is 'pulsed' to modulate the data stream, with a short pulse representing a '0' and a long pulse a '1'.

In the early days, this technology relied heavily on the fact that the data being sent was invisible to the naked eye, and was therefore supposedly "secure" as it could not be observed. As a result, the codes sent were often very simple, and could be as little as 8 bits.

Illustration 16: IR Token

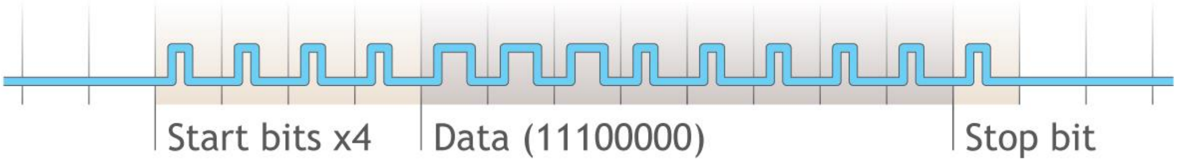


Illustration 17: IR Data Pulses

In the illustration above, the data is sent with 4 'start bits', and 1 'stop bit', with 8 data bits in-between (the data here is '11100000'). The automotive industry soon found that vehicle immobiliser/central locking keys were being cloned and so moved to "rolling code" systems, in which the data being sent by the key changed each time it was used, following a pattern recognised by the vehicle. This prevented simple cloning as a code that had already been used would be ignored by the vehicle. The code was allowed to get several steps out of sequence to allow for accidental key presses whilst the keys were being carried in pockets.

RF (Radio Frequency)

The move to RF from Infra-red was merely a medium change, with the data staying the same, but transmission being sent via RF instead. This had the advantage of providing potentially greater range, as well as removing the necessity of "pointing" the remote at the vehicle to ensure that the signal could be seen.

RFID / NFC

Devices that are commonly referred to as RFID are, in many cases, not actually strictly speaking RFID, but are in fact NFC or 'Proximity' devices. RFID has become a catch-all term for 'Contactless' technologies – i.e. those devices that do not require a physical interface to transfer data, but do so via other means when in proximity to a reader. True RFID devices actually transmit data using RF and none of the devices examined for this publication used such technology, but in keeping with common vernacular we will refer to proximity and NFC devices as RFID throuought this document.

An NFC Token is typically made up of three main components:

- A coil to energise the electronics through induction from the reader's coil and to provide communications between reader and Token
- A capacitor to tune the coil to become a resonant circuit
- A microcontroller to interpret commands from the reader and signal responses

There may be other supporting components such as transistors and resistors, but the three above are the most important ones.

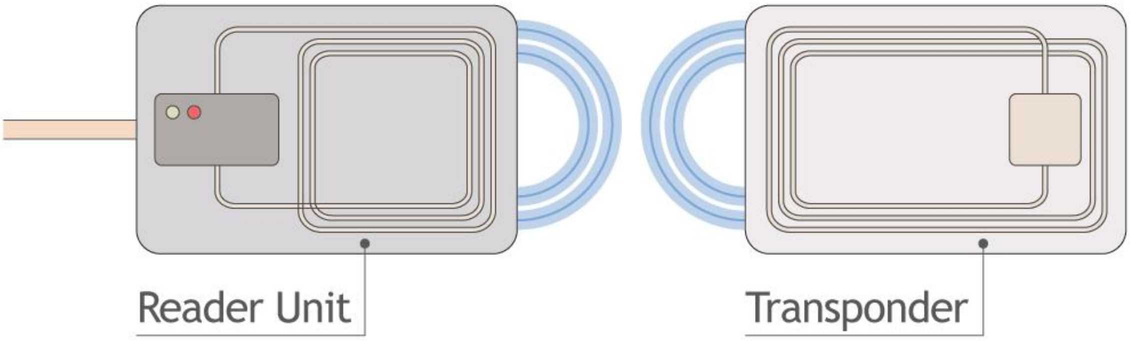


Illustration 18: NFC Reader and TAG

NFC devices are passive in that they do not have a power supply of their own, nor do they 'transmit' any data unless activated by a reader, and, even then, only by affecting the reader's magnetically coupled "field" that is being used to activate the device.

In its simplest form, an NFC reader will be made up of similar components, and will be generating a 'carrier' signal which emanates from its coil, for example at 125KHz, as used in many common systems:

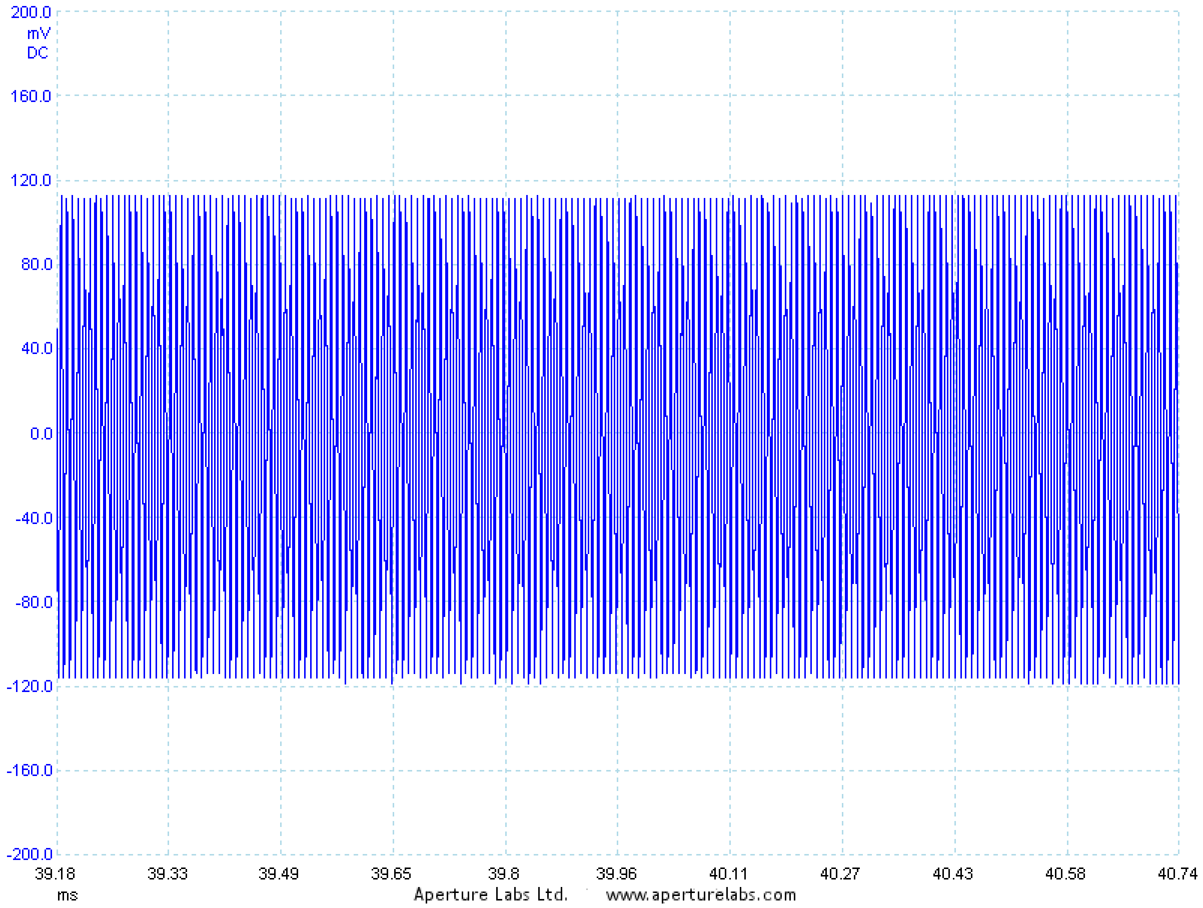


Illustration 19: 125KHz Carrier Signal

When placed in this field, the Token will be energised by induction through its own coil, and can begin the process of identification.

In its simplest form, this consists of simply sending its ID to the reader. It will do this by grounding its own antenna for brief periods, thus causing a micro-fluctuation on the reader's magnetically coupled coil, which the reader will detect as a voltage drop. The process of creating these fluctuations in an orderly manner, such that they can be interpreted by the reader, is known as 'modulation', and the exact manner of the fluctuations (period, intensity, number of changes etc.) determines the modulation type or 'scheme'. Typical modulation schemes include:

- FSK – Frequency Shift Keying
- ASK – Amplitude Shift Keying
- PWSK – Pulse Width Shift Keying
- Manchester code (also known as Phase Encoding or PE)
- Biphase mark code

More than one scheme may be used in a single system.

In addition to this, the data itself will be further encoded for reliability and interoperability. Typical encoding schemes include:

- ASCII - American Standard Code for Information Interchange
- BCD – Binary Coded Decimal
- EBCDIC - Extended Binary Coded Decimal Interchange Code

and, again, more than one scheme may be used in a single system.

A Token in the reader field 'transmitting' its ID might look like this:

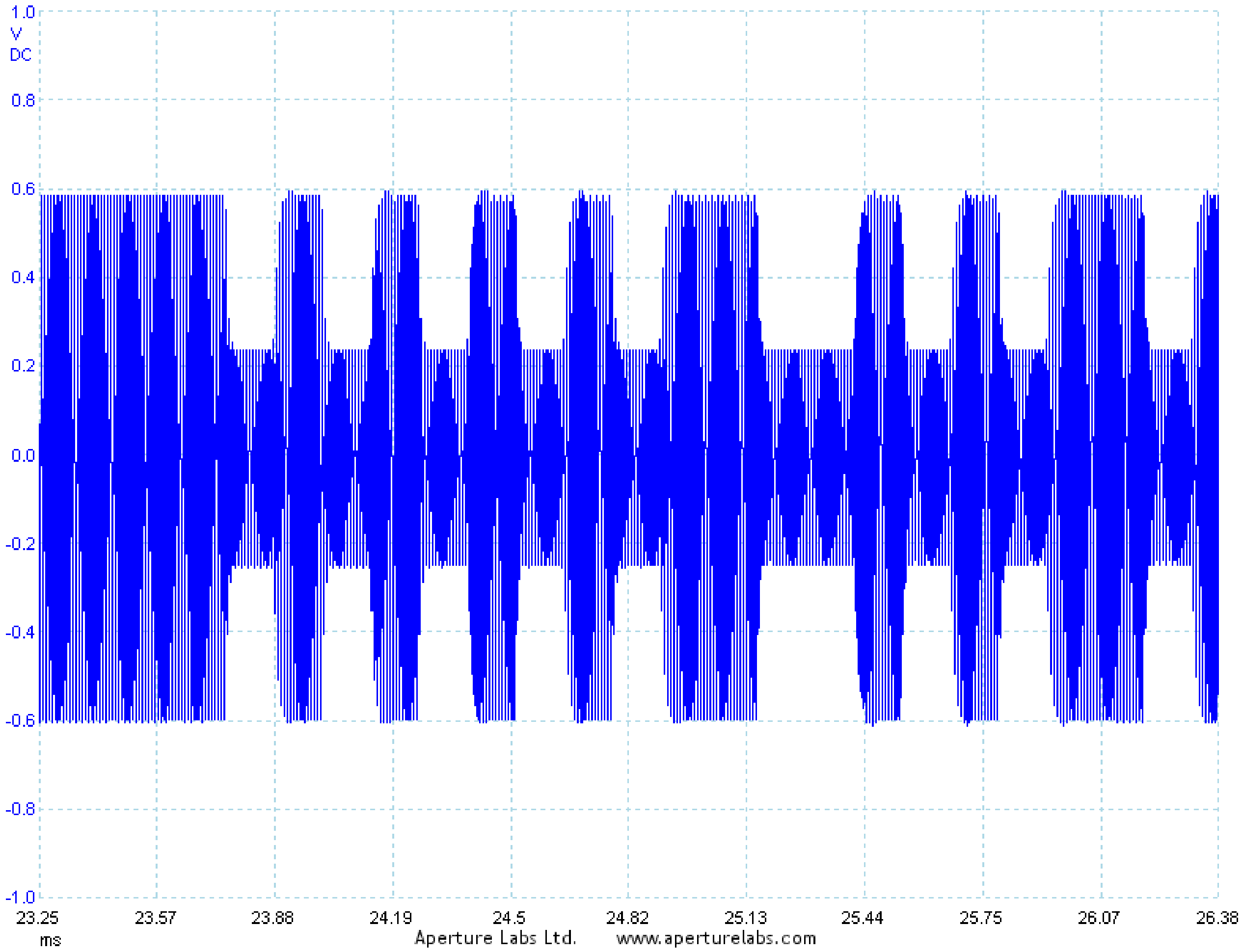


Illustration 20: 125KHz TAG message to reader

Data is sent as a stream of binary 1s and 0s, a '1' being signalled by damping the coil and causing a dip in the voltage for a short period, and a '0' by NOT damping the coil for the same length of time.

Once the data stream has started, the reader can simply determine ones and zeros by checking the voltage on its coil at specific intervals, known as the 'period', or by looking for transitions between low and high voltage, depending on the modulation scheme. It can then interpret the data according to the data encoding standard being used, apply any CRC checksums (Cyclic Redundancy Check) etc., and thus determine the Token's ID.

Similarly, the reader can send signals to the Token by switching the carrier field off and on. This can be done for short periods even though it is supplying power to the Token as the Token's capacitor circuit will store enough energy to keep it powered until the reader field is switched back on. A message being sent by the reader to the Token might look like this:

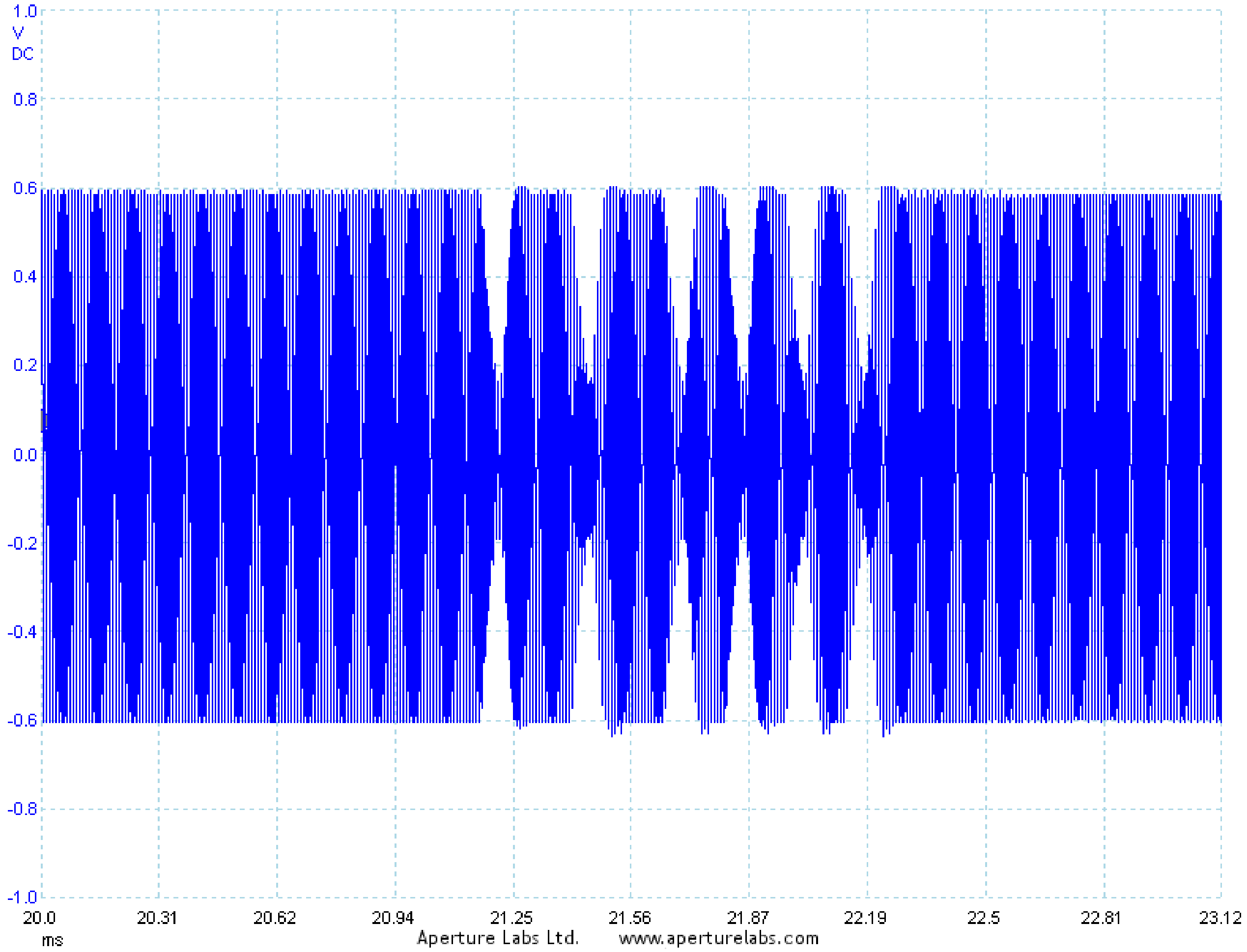


Illustration 21: 125KHz Reader message to TAG

In this case, PWSK is being used - the length of the signal 'pulse' between momentary shutoff of the carrier indicates a '0' or a '1'. A long burst being a '1', and a short a '0', so here a message of '11000' was sent.

Now that we have two-way communication between Token and reader, more complex interactions are possible, including authentication and/or encryption, and we will look at those topics in more detail later in this document.

For now, however, it is important to understand the different levels of conversation that occur between reader and Token, and the implications that has on security of the system as a whole. These roughly break down into:

- UID only (Unique ID)
  - No AUTHENTICATION or ENCRYPTION

The Token simply transmits a 'Unique' number or ID in the clear.

- UID plus DATA
  - No AUTHENTICATION or ENCRYPTION on Token

The Token transmits an ID and also has storage space for data, which the reader can request on a per-block basis. The contents of the data field and the UID are transmitted in the clear, without any form of authentication on either side, but the data stored in the Token may be encrypted or otherwise verifiable by an external process.

- UID plus AUTHENTICATION protected DATA
  - DATA only available after successful AUTHENTICATION

The Token transmits its UID in the clear, but then requires some form of authentication before access to the data blocks is granted. This may take the form of providing a correct password with the read request, which could also be transmitted in the clear.

- UID plus AUTHENTICATION plus ENCRYPTION
  - DATA only available after successful AUTHENTICATION
  - Communications between Token and READER are ENCRYPTED
  - DATA may be encrypted by Token
  - Token has secret KEY store
  - READER may have secret KEY store

The Token transmits its UID in the clear, but then requires a cryptographic handshake, which both authenticates the reader and establishes session keys to encrypt the following conversation. All data other than the UID and the cryptographic challenge/response is transmitted in encrypted form.

RFID Threats

Threats to RFID devices include the following:

- Unauthorised reading
  - Disclosure of Credentials
  - Disclosure of Monetary Value

Tokens running in 'UID only' or 'UID plus DATA' mode should be considered extremely insecure as they provide no mechanisms that prevent reading by unauthorised users. This means that simple 'Drive-By' attacks are possible: an attacker can read the target's credential by walking past them or standing next to them in a queue with an active reader.

Tokens running in AUTHENTICATION mode prevent this by requiring knowledge of a shared secret or PKI (Public Key Encryption) before allowing access to the content. However, it should be noted that the Token having that capability is no guarantee that the system is actually using it. Many systems are configured to use the UID only, despite the Token having cryptographic capabilities, in which case the system as a whole should be considered as insecure as a non-crypto capable system whilst it is in that configuration.

- Emulation / Cloning
    - Duplication of Credentials

Again, Tokens running in 'UID only' or 'UID plus DATA' mode are vulnerable, as they have no defence against emulation/cloning. Any device that presents the correct UID or returns the expected DATA will be recognised and accepted as genuine, and either blank un-programmed Tokens or purpose built emulator devices can be easily configured to present any UID and/or data blocks required.

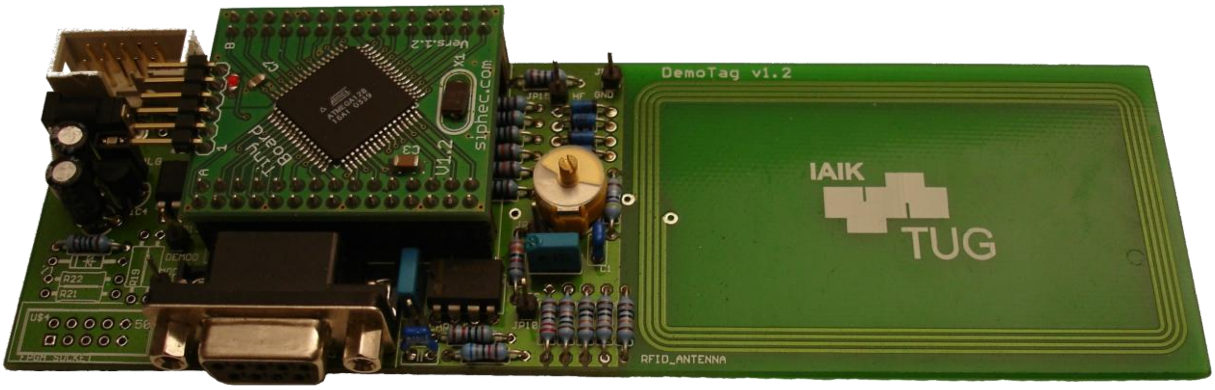


Illustration 22: RFID/NFC emulator

- Relaying (Man-In-The-Middle)
    - Unauthorised remote use of genuine Credentials

In this attack, a reader and an emulator are used to relay the messages between a system's reader and a target Token, which may be near or far away, depending on the technology used to transfer the data between the attacking reader and emulator. Even fully encrypted conversations can be relayed in this way, as the data is passed between the two devices unmodified, and no decryption is necessary for the attack to succeed. The attacker is only interested in satisfying the reader and the Token that they are talking to each other, which, in effect, they are, albeit via a 3rd party. For example, to relay e-Passport credentials, the attacker's reader would be held up against the target passport, and the emulator against the official reader. Any read commands issued by the genuine reader are intercepted by the emulator and relayed (say via TCP/IP over The Internet) to the remote reader, which issues them to the genuine Token. The Token's response is relayed back to the emulator in the same way, and so the conversation proceeds to completion, after which access may be granted to the attacker if no further verification takes place (such as Biometrics).

- Sniffing (interception of conversation)
  - Disclosure of credentials (unencrypted)
  - Disclosure of passwords
  - Disclosure of cryptographic handshakes
  - Disclosure of encrypted conversation

Introducing another coil into the field between reader and Token may allow a 3rd party to intercept the signals as they are passed between the two devices. These signals can be demodulated and interpreted just as the genuine reader and Token are able to do, and, depending on the level of encryption deployed in the system, some or all of the data could be recovered. At the very least, it should be possible to determine the UID of the Token, and, if running in password or non-authenticated mode, both the password and data will also be accessible. Even if running in encrypted mode, as the handshake will have been captured, it may be possible to run a cryptographic attack against the system and recover the secret key, thereby allowing the full conversation to be decrypted, and possibly enabling further attacks against the system such as cloning or modification of genuine credentials.

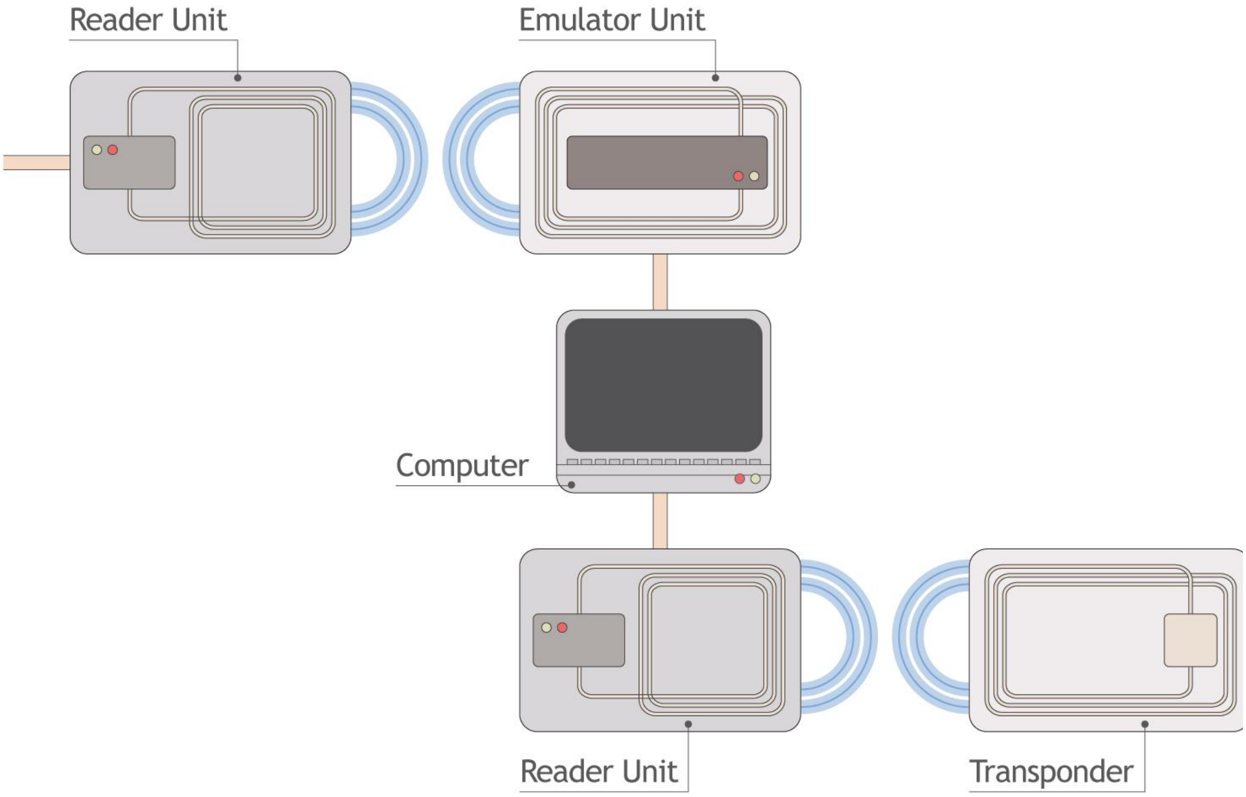


Illustration 23: RFID Man-in-the-middle attack

- Unauthorised Writing
  - Modifying Credentials
  - Modifying Monetary Value storage

Cryptographic keys recovered through a sniffing attack may allow a genuine credential to be updated, possibly changing access rights through modification of data blocks, or increasing or re-instating value blocks. Tokens running in 'UID and DATA' mode which have not been set to Read Only can be attacked in this way without the need to recover any cryptographic keys. A common example of devices vulnerable to this kind of attack can be found in hotels using ISO15693 Tokens as room keys, which are normally left as re-writeable so that the keys may be returned by the guest and re-used by the hotel.

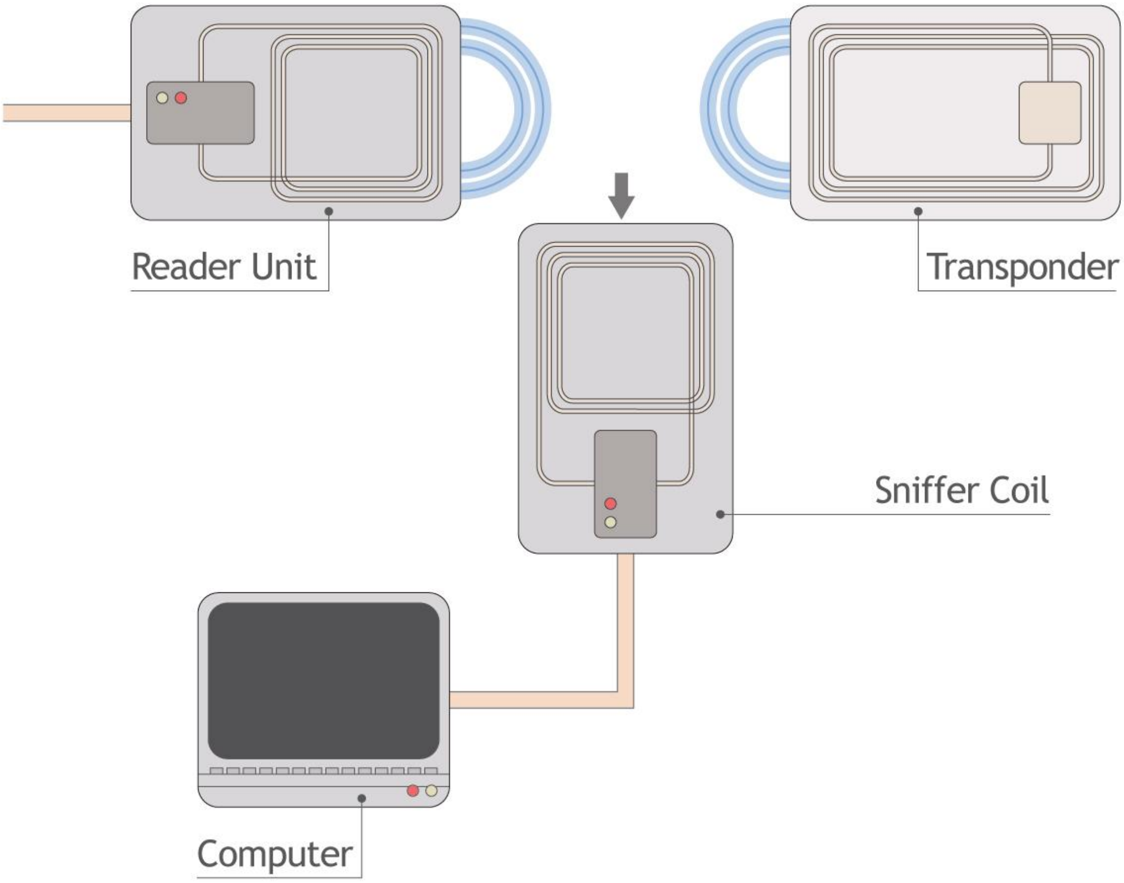


Illustration 24: RFID Sniffer

RFID Tokens

RFID tokens come in a variety of form factors, and careful consideration should be given as to what style is appropriate for the application.

For example, if the token is a supplement to a physical lock, as would be the case for an alarm system disarming Token, it is bad practice to use a keyfob style as that is likely to be attached to the key ring, which would mean that anyone finding a lost set of keys would not only be able to open the door, but also to disarm the alarm.

Common styles include:

- Clamshell
  - For use with lanyard
- ISO Card
  - Credit card style for carrying in wallet
- Keyfob
  - Attach to key ring
- Disc
  - Insert into envelope or pocket
- Sticker
  - Attach to physical device
- Glass capsule
  - Human / Animal implant

Illustration 26: Clamshell

Illustration 27: Disc

Illustration 25: Glass Capsule

Illustration 28: Sticker

Illustration 29: ISO Card

Illustration 30: Keyfob

RFID Readers

RFID readers will normally be placed by the door or gate and may be 'plain' or with PIN Pad and/or confirmation LED/Buzzer. Size and form factor will vary, but in general, the longer the read range, the larger the device. The maximum practical read range for passive Tokens is around 70cm. Readers should always be fitted with tamper detect circuits and the output of those tamper detect circuits should be monitored so as to sound an alarm should that tamper circuit be activated.

Illustration 32: RFID Reader with PIN Pad

Illustration 31: Long range RFID reader

RFID Writers

RFID writers are normally only required if tokens are going to be created or modified on-site, and will usually be supplied as part of the overall access control system. However, stand-alone devices are available for most systems that will allow credentials to be created outside of the access control system's audit trail.

Illustration 33: Proprietary 125KHz Reader/Writer

Illustration 34: OmniKey 5321 ISO standard 13.56MHz Reader/Writer

Cabling

Although this guide is primarily about tokens it should be noted that the readers, their installation and cabling can adversely affect the security of the system. Most readers are easily removed from the wall and access to their cabling can weaken the security of the system as in general that communication is not encrypted. It is recommended that all cabling be run in the protected area, tamper detect switches leading to monitored alarms be installed on all readers and if possible cabling is fastened on the secure side of the door to prevent reader removal due to short cable length to the reader.

The Human Condition

Human beings are most creative when they are looking for an easy way to do something.

A human being will ALWAYS TAKE THE EASY OPTION, no matter how many rules are laid down, even if those rules are initially adhered to, the easy option will always prevail in the long run.

This is a factor that many managers have a real problem with. They attempt to force staff into difficult ways of working, simply because they have the authority to do so, thus causing the staff to look for the easy way around the problem. In a security context this almost always leads to security being compromised.

For example:

- failing to put an access control reader on a rear door, for seemingly sensible budgetary reasons, that is used by staff to visit an adjacent building.
- Telling the staff that they must use the front door which has a reader and is secured properly, will almost certainly result in that rear door being propped open, or to avoid obvious detection have its striker plate taped up so it appears closed and locked but is neither.
- It is important that in your implementation that you embrace the human condition and implement a system that is easy to use, and workable for the staff.

This will enhance your security more than you could imagine.

Glossary Of Terms

TERM	DESCRIPTION
1-Wire Interface	The electrical interface used by iButtons, which is actually two wires – one for ground and one for power and data.
26 Bit Wiegand Format	A commonly used data format in which 26 bits representing two parity bits and 24 data bits are used to carry a Site Code and Card Code which together form a UID.
AACS	Automated Access Control System.
Aperture Labs Ltd.	A security research company that focusses on physical and electronic locking systems such as access control systems. For more information please contact info@aperturelabs.com
ASCII	American Standard Code for Information Interchange. The code used by most computer systems to map printable and control characters to a numerical value that can be stored and manipulated by a computer. E.g. The letter 'A' is represented by the hexadecimal value 41 and a Carriage Return by the value 13.
ASK	Amplitude Shift Keying. A modulation scheme in which the amplification level of the signal is varied to signal data.
Algorithm	A mathematical or cryptographic formula.
ATM card	ATM stands for Automated Teller Machine, commonly known as a 'Cash Machine', and an ATM card is a plastic card with a Magnetic Stripe or embedded Contact Chip (Chip & PIN) .
Audit Trail	A list of transactions pertaining to the device in question, kept for the purpose of tracking usage.
Authentication	The process of establishing the identity of a party in a transaction.
Barcode	An optical machine-readable data representation usually consisting of parallel lines of black on white. The spacing and thickness of the lines represent the data.
Barium Ferrite	A magnetically sensitive compound ($BaFe_2O_4$) used in Magnetic Stripes and other tokens such as Barium Ferrite cards.

TERM	DESCRIPTION
BCD	Binary Coded Decimal. A method of representing Decimal values within binary data. The Hexadecimal representation of the binary data is read as Decimal, so, for example, the data characters 'A' and '0' would be interpreted as their Hexadecimal representation '4130', which in turn would be read as 4,130 – four thousand, one hundred and thirty.
Binary	A counting system in which the value is either 0 or 1. When used in conjunction with the word data – i.e. 'Binary Data', it is referring to 'raw' data in the form it is stored or transmitted by the system.
Biometric	The term 'Biometric' is taken from the ancient greek 'Bois' meaning 'Life' and 'Metron', meaning 'Measure', so it literally means 'Life Measure', or a system for creating a pattern or representation that can be compared to that of a real living thing, to determine its Identity.
Biphase Mark Coding	A modulation scheme in which '0' and '1' are represented by two consecutive phases of the signal. If they are both the same – i.e. Positive/Positive or Negative/Negative - then a '0' is being transmitted, and if they are different – i.e. Positive/Negative or Negative/Positive – then a '1' is being transmitted.
Bit	A single Binary element of data. I.e. A '0' or a '1'.
Bitting	The pattern of cuts in a physical key.
Blade	The section of a physical key containing the bitting.
Blanks	Un-programmed electronic tokens or un-cut physical keys.
Bow	The 'handle' end of a physical key.
BPI	Bits Per Inch. The number of Data Bits that can be stored per inch of storage medium. Usually referring to Magnetic Stripes.
Brute Force Attack	An attack in which attempts are made to guess a code by trying every possible combination, either randomly or in sequence. Remember when your children reset the combination on your briefcase? You opened it an hour and a half later, after starting at 000 and incrementing the code until it opened. They were irritatingly smart and set it to 997.
Byte	Eight bits. A single data character is normally represented by a Byte, and larger numbers by multiples of Bytes or 'Words'.

TERM	DESCRIPTION
Capacitor	An electronic component that stores electrical energy.
Carbon Tetrachloride	A solvent compound (CCl_4) which is now known to be hazardous to health (carcinogenic, amongst other things), so is no longer in general use.
Carrier Signal	A signal such as an audio tone or radio wave which forms the basis of a transmission. This carrier Signal is Modulated which forms the basis for data transmission.
Challenge Response	An authentication method whereby a challenge is issued which requires a correct response. This will usually incorporate some form of cryptography to protect a Shared Secret.
Checksum	A value calculated by performing a mathematical function which incorporates every data bit in a body of data to determine if any of them have been lost or corrupted. The checksum is stored or transmitted along with the data, and by re-calculating and checking that the same value is obtained, the integrity of the data can be determined.
Chip	A microprocessor with a 'Contact Interface' – i.e. One that requires insertion into a reader to enable contact pins within the reader to interface with the microprocessor e.g. Chip & PIN. Can also be used to refer to the microprocessor itself.
Chip and Pin	A government backed initiative in the UK to implement the EMV standard for secure payments using smart cards.
Chip Card	*See Contact Smartcard.*
Clamshell Card	A clamshell card consists of two halves and has a small depression in one half for a RFID chip and coil which is then sealed in by the application of the other half.
Cloning	The act of creating a token that appears to a reader to be an original existing token. This can be as simple as copying a magnetic stripe.
Coercivity	The amount of magnetic energy that is required to re-orient magnetic particles in a magnetic substrate such as a magnetic stripe on a credit card. The higher the Coercivity of the magnetic material the less likely it is to be affected by other magnets, such as the magnet in the speaker of a mobile telephone for instance.
Coil	A coil of wire that has an exact set of dimensions and with a capacitor is used to form a resonant circuit.

TERM	DESCRIPTION
Computer Punch Card	One of the very first ways of storing data for processing by a computer. It consisted of a 187.325 by 82.55 mm card which has holes punched in it at set locations to represent bits and bytes of data.
Contact Smart Card	An ISO standard card with a small microprocessor embedded into the card structure. This microprocessor has a set of connectors on the surface of the card. When the card is inserted into a read/write device its contacts mate with a set of contacts on the read/write device, the contacts are used to power the chip and provide a means for data transfer.
Contactless Smart Card	An ISO standard card with a small chip embedded into the card structure. This chip may or may not have a set of connectors on the surface of the card similar to a contact smart card. It will however have a coil embedded in the card structure that will enable the embedded chip to receive power and communicate with a read/write device.
CPNI	Centre for the Protection of National Infrastructure. The United Kingdom government authority which provides protective security advice to businesses and organisations across the national infrastructure. Their advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services secure.
CRC	Cyclic Redundancy Check. A type of Checksum.
Credential	An object or item of data that is used by an individual for the purpose of identification.
Crypto	Abbreviation of 'Cryptographic'. Used to refer to any element of a system that is cryptographic in nature.
Cryptographic	Pertaining to an algorithm used for hiding secret information by encoding it with another piece of data known as a key.
Cylinder	The non-rotating part of a physical pin-tumbler lock.
Data Logger	A device that records data.
Decrypt	The reverse of Encrypt. The process of decoding an encrypted message.
Demodulate	The process of extracting the data from a modulated signal.
Denial Of Service	A form of attack designed not to break into a system, but to prevent if from operating normally, i.e to slow it down or to prevent it from operating at all.

TERM	DESCRIPTION
	For example, by injecting Superglue into a physical lock to prevent a key being inserted.
Digital Signature	A cryptographic checksum of a body of data designed to demonstrate that the data has not been tampered with and/or that it came from a particular origin.
DNA	DeoxyriboNucleic Acid. A Nucleic acid that contains the genetic instructions for all living organisms. It is unique enough between individuals to be used for the purpose of Biometrics.
DOS	*See Denial Of Service.*
Drive-By	A random or opportunistic attack. One that requires no specific knowledge of the individual target in order to succeed.
Driver Pin	A component of a Pin Tumbler lock. It is the top pin in the stack and is pushed into the plug by a spring when the lock is in its locked state.
EBCDIC	Extended Binary Coded Decimal Interchange Code. A data representation method developed by IBM that has been largely superseded by *ASCII*.
Emulation	The act of pretending to be something else. I.e an RFID emulator would appear to a reader to be a real card, when in fact it is an electronic device responding in an identical manner to a real card. *(see also Cloning)*
EMV	Europay Mastercard Visa Standard for authenticating credit/debit card payments and ATM transactions.
Encrypt	The act of taking a message and and encoding it with a key causing it to become unintelligible to anyone apart from the holder of the appropriate Decryption Key.
Energised	This is the state where a circuit has enough electrical energy to become active.
E-Passport	A passport that conforms to the Machine Readable Travel Document standard (ICAO 9303).
Even Parity	A checksum method in which the positive bit count is Even. I.e. If all '1' data bits are counted, the resulting number is Even.
Facility Code	*See Site Code.*
Ferro-Magnetic	The property and mechanism by which certain materials can become magnetised.

TERM	DESCRIPTION
Fingerprint	In computer related security, a fingerprint generally refers to a cryptographic checksum used to verify the integrity or authenticity of a body of data.
Flux-Reversal	An event in which a magnetic stripe write head reverses its magnetic polarity. This causes the magnetic particles within the stripe to reverse their polarisation. For example if particles were being aligned north-south north-south north-south, a flux reversal would cause an ongoing polarity change and you would end up with north-south south-north south-north. The point where two particles had their south poles adjacent would constitute a flux reversal. This would be the case until the next flux reversal in which case the polarity would change again.
Frequency	The number of occurrences of an event within a given time period. In this context, normally referring to carrier wave frequency of RFID devices, which will usually be measured in Hertz, which is the number of cycles per second. 125KHz is normal for 'Low Frequency' devices – 125 thousand cycles per second, and 13.56MHz for 'High Frequency' – 13.56 million cycles per second.
FSK	Frequency Shift Keying. A modulation scheme in which the frequency of a signal is modified to signify data. For example, F2F (Frequency Twice Frequency) might use two short pulses to send a '1' and one long pulse to send a '0'. The total time to send each bit would be exactly equal, so the two short pulses are exactly half the length (or twice the frequency) of the long pulse.
Glass Capsule	In this context, a small glass capsule containing an RFID transponder, designed to be implanted under the skin of a human or animal.
GSM	Global System for Mobile communications (originally Groupe Spécial Mobile). The most commonly used mobile phone communication standard.
Guard Tour	A system designed to check that security guards are performing their rounds. Devices will be located at strategic points around the perimeter that they are supposed to be checking, and as they pass each one they will interact with it to prove that they were there and create a timestamped entry in a log. This will typically be achieved by carrying a hand-held reader and swiping a Token affixed to the wall, but can also done by carrying a Token and presenting it to a fixed Reader.
Handshake	The process of two-way authentication and exchange of keys.
Hex	*See Hexadecimal.*
Hexadecimal	A counting system using base 16. Numbers 10-15 are represented by the characters A-F In general number are represented in multiples of two with leading zeros where necessary . For example the decimal number 10 would be

TERM	DESCRIPTION
	represented as 0A, 15 as 0F and 255 would be FF
iButton	A microprocessor encased in a small metal can that communicates via a 1-wire interface.
ID	*See UID.*
Identifier	*See UID.*
Immobiliser	A device designed to prevent the engine electronics in a car from functioning in the event that the vehicle has not been properly unlocked.
Impressioning	The process of taking a physical image of a door key in a wax (or other soft medium) block. It can also refer to a method of 'picking' a physical lock.
Induction	The process by which electrical current is transferred without physical contact from one circuit to another, via adjacent coils of wire.
Infra-Red	Non-visible light commonly used in remote controls such as for TV, but also found in some security applications, for example garage door openers or, on older vehicles, immobiliser key fobs. It can also be used for CCTV lighting.
Integrated Circuit	A miniaturised electronic circuit, typically formed on a small piece of silicon wafer, commonly referred to as a 'Silicon Chip'.
Iris Scan	A biometric method in which an image of an Iris is taken and an index generated that uniquely identifies that Iris.
ISO	The International Organization for Standardization. A body that coordinates the creation of International standards across many industries.
ISO 15693	ISO standard for “Vicinity Cards”, operating at 13.56 MHz. This standard is specifically designed to increase the readable range of previous “Proximity Cards”.
ISO 7810	ISO standard defining Physical Characteristics of Credit Card Size Document (85.60mm × 53.98mm).
ISO 7811	ISO standards for recording of information on identity cards. This is broken down into the following sections:
ISO 7811-1	Embossing
ISO 7811-2	Magnetic Stripe - Low Coercivity
ISO 7811-3	Location of Embossed Characters
ISO 7811-4	Location of Tracks 1 and 2
ISO 7811-5	Location of Track 3

TERM	DESCRIPTION
ISO 7811-6	Magnetic Stripe - High Coercivity
ISO 7813	ISO standard for Financial Transaction Cards
ISO Card	A plastic card conforming to *ISO 7810.*
Key (cryptographic)	Data used in conjunction with a cryptographic algorithm to encrypt data. The key is exactly that and is required to read or decrypt encrypted data
Key Pin	The lowest pin in a pin-tumbler lock stack that makes contact with the key when it is inserted in to the lock. At its other end it presses against the Driver Pin to lift it to the Shear Line when the correct key is inserted.
Laminated	A material that consists of thin layers glued or fused together.
LED	Light-emitting Diode. A semiconductor diode that emits visible light when current is passed through it, commonly used as indication lights.
Magnasee	Very fine colloidal iron in a fast-evaporating liquid (Carbon Tetrachloride) used to visualise magnetic fields recorded onto magnetic medium such as Magnetic Stripes. *See also Q-View.*
Magnetically Coupled	Two devices that are connected together using a magnetic field.
Magnetically Sensitive Film	Plastic film which contains a slurry of fine nickel particles, which will group together when exposed to a magnetic field, making it possible to visualise it.
Magnetic Polarity	The property of being either magnetically North or South.
Magnetic Stripe	A strip of Ferromagnetic material Laminated into a plastic card to provide a medium for storing data.
Manchester Coding	A modulation scheme in which each bit contains both a positive and a negative component, switched at its mid point. For example, a '1' would start with a positive voltage and then switch to negative at its mid point, and a '0' would start negative and switch to positive. This has the added advantage that it is 'self-clocking', as the bit transmission period can be determined by measuring the time between transitions, which makes it very useful in systems such as Magnetic Stripes, where the swipe speed (and therefore the length of the data pulses) will vary, particular when being performed by human hand.

TERM	DESCRIPTION
Man In The Middle	An attack method in which the attacker places themselves between two components of a security system and relays messages between them. This gives them the opportunity to read and/or modify the messages before passing them on.
Microprocessor	An integrated circuit semiconductor that performs complex processing functions and may incorporate some memory capacity.
Modulation	The process by which a signal is altered in order to convey information.
Mutual Authentication	The process of confirming the identity of both parties in a transaction.
NFC	Near Field Communications. The correct term for magnetically coupled contactless devices commonly refered to as “Proximity” or “RFID” devices.
Odd Parity	A checksum method in which the positive bit count is Odd. I.e. If all '1' data bits are counted, the resulting number is Odd..
Parity Bit	A redundant bit which is added to data bits in order to force the positive bit count to be Odd or Even.
Password	A secret word or number that is checked for the purpose of verification.
PIN	Personal Identification Number. A secret number known only to an individual and the system they need access to. A common form of this is the PIN on an ATM card which is checked when attempting to withdraw cash.
Pin (lock)	A component of a Pin Tumbler Lock that prevents the plug from rotating unless the correct key is present.
PIN Pad	A keypad that is used to enter PIN numbers. Normally built into an access card reader.
Pin Tumbler	A type of physical lock in which pins prevent a plug from rotating within the lock cylinder. Insertion of the correct key lifts the pins out of the way, allowing the plug to turn.
PKI	Public Key Infrastructure. A system for exchanging encrypted messages using two encryption keys – a private one which is kept secret and a public one which is published. Message encrypted with the public key can only be decrypted with the private one and vice-versa.
Plug	The centre part of a pin tumbler lock that rotates as the correct key is turned.

TERM	DESCRIPTION
Polarised	Magnetised to either North or South polarity.
Private Key	The secret key in a PKI system.
Proximity	*See RFID*
Public Key	The published key in a PKI system.
PWSK	Pulse Width Shift Keying. A modulation scheme in which the duration of the pulse signifies a '0' or a '1'. The factor would normally be two, so if a '1' was signified by a pulse of 1 millisecond, a '0' would be 2 milliseconds.
Q-View	A combination of tiny magnetic particles suspended in a clear solvent liquid used to detect flux reversals on magnetic stripes. S*ee also Magnasee.*
Read Only	A device or memory location that can only be read and not written.
Relay	To receive some information and then pass it on.
Resistor	An electronic component that resists the flow of current in an electrical circuit.
Resonant Circuit	A combination of a coil and a capacitor that responds to a specific frequency.
RF	Radio Frequency. A transport mechanism that utilises a radio transmitter and receiver system to send messages between two devices.
RFID	Radio Frequency Identification. Devices that use contactless technologies to exchange credentials or data. Also commonly known as Proximity or NFC.
RO (R/O)	*See Read Only*
Rolling Code	A secret code that is used once and then discarded. A new code is generated according to an algorithm that is known to both the sending and receiving devices, and is synchronised such that a repeated code will be ignored but a new one in the correct sequence will be recognised.
Shared Secret	A secret that is known to two or more parties for the purpose of verification.

TERM	DESCRIPTION
Shear Line	The boundary between the plug and the cylinder in a pin tumbler lock. This boundary has pins across it when the lock is in its locked state, thus preventing the plug from turning. When the correct key is inserted, it lifts the gap between the key pins and the driver pins such that they align with the Shear Line, allowing the plug to turn.
Short Circuit	The interconnection of two wires that causes electrical current to flow along a different path than originally intended.
SIM	*See Subscriber Identity Module.*
Site Code	In systems that break their UIDs down into two parts – User and Site, the Site Code is the code that identifies the building or organisation. It is normally 1 byte in a *26-Bit Wiegand* system, and has 256 possible values: 0-255.
Smart Card	A card with an embedded microcontroller. This may have a Chip or contactless interface.
Sniffer	A device to facilitate the listening-in of data transmissions.
Sniffing	The act of listening-in on a data transmission, usually in an unauthorised manner.
Start Bit	A bit that precedes the actual data bits in a binary transmission.
Stop Bit	A bit that succeeds the actual data bits in a binary transmission.
Subscriber Identity Module	A card containing a microprocessor which holds the subscriber details for a GSM phone.
Tag	An RFID/NFC transponder which is the active component of an RFID/NFC Token.
Tamper Detect	A device for detecting interference with a physical device such as an access control token reader– e.g. Removing the cover.
TCP/IP	Transmission Control Protocol/Internet Protocol. A set of protocols for transmitting data over networks such as The Internet.
Thermoplastic	A type of plastic that turns to a liquid when heated and returns to a solid state at room temperatures.

TERM	DESCRIPTION
Token	A physical device used to identify, and, optionally, to authenticate a person.
Transistor	A small electronic component that acts as a switch or amplifier.
Transponder	An electronic circuit which transmits and receives.
UID	Unique Identifier. A number or data sequence that is unique to that entity.
Wiegand	John R. Wiegand discovered a magnetic effect which has been adapted to a number of applications in the field of security, as follows:
Wiegand Card	An access control token which contains small pieces of Wiegand Wire arranged to convey a bit pattern typically arranged in the Wiegand Format.
Wiegand Effect	An effect which occurs when a specially produced wire is moved by two oppositely polarised magnets. The wire will emit a small magnetic pulse when moved past the second magnet which can be detected by a small coil of wire.
Wiegand Electrical Protocol	The electrical protocol defining voltages and timings which is used by most access control readers to communicate with the access control system over a physical cable.
Wiegand Format	An arrangement of bits that indicate a Site Code and Card ID together with parity bits to ensure the data is not corrupted.
Wiegand Wire	Specially manufactured wire which exhibits the Wiegand Effect.