# ACCESS CONTROL

## Introduction to Access Control

# What is Card Access?

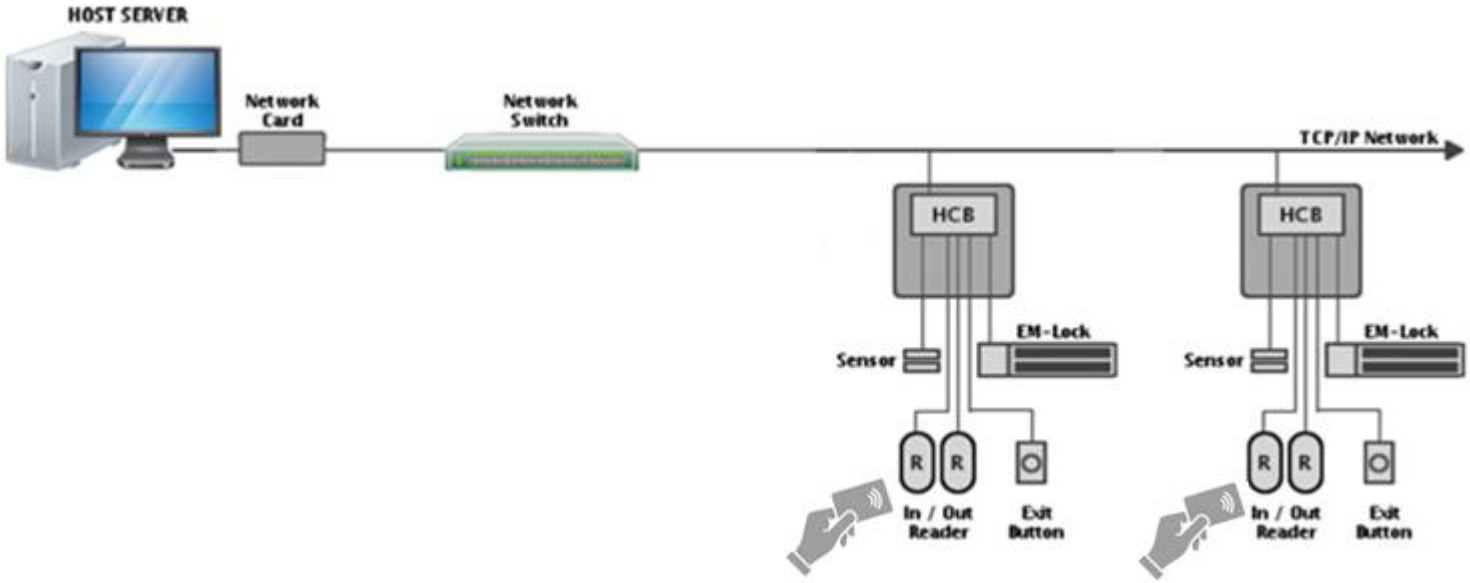
- Before we understand what electronic access control is, we need to know access control first
- Access control is a mechanism using which entry to certain areas and resources can be controlled
- Access can be controlled using several methods such as:-
  - ✓ Keys – car, house, safe deposit etc
  - ✓ Direct payment – pay per ride themepark, parking (some)
  - ✓ Tickets – movies, zoo etc
- Access control requires physical barrier. You cannot have access control without physical barrier, e.g: doors, boom gate, turnstile etc

# What is Card Access?

- The previous access controls are fine, but what if access should only be given to certain people? You can use key, but..
  - ✓ What if many door involved? Bunch of keys?
  - ✓ What if you want to know who access where? We need identification
- How do you grant access to these areas without compromising security yet flexible enough?
- Basically electronic access control is whereby access is gained by means of presenting a valid identification which enable a passage through the physical barrier
- Electronic access control requires
  - ✓ Identification
  - ✓ Authentication
  - ✓ Authorisation

# How?

- Summarised in diagram below;



# How (1) – Identification

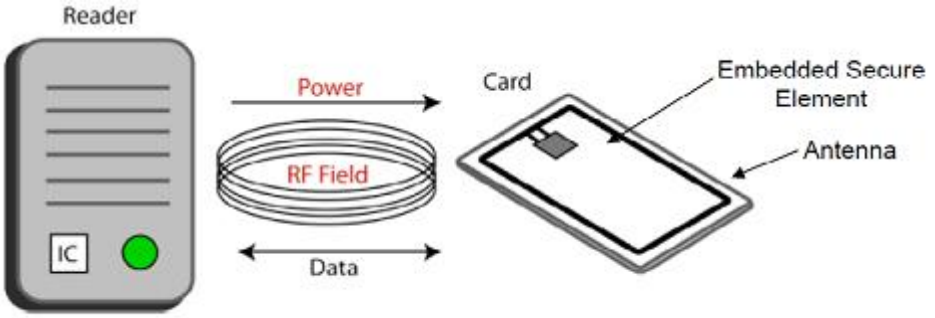
- Identification is required to start the access process. In this process we are identifying ourselves to the system using certain credentials. We will be using TV repairman analogy..
- Credential is something that verify who you are
- The credentials use for identification:-
  - ✓ Something you have – e.g: card, token, tag etc
  - ✓ Something you know – e.g: password, PIN etc
  - ✓ Something unique to you – normally biometric (e.g: fingerprint, eye scan)
- These concept represent the security level to be implemented. The security level can either be card only or card+PIN or card+PIN+biometric.
- Why these levels, and is it necessary to implement all these level?

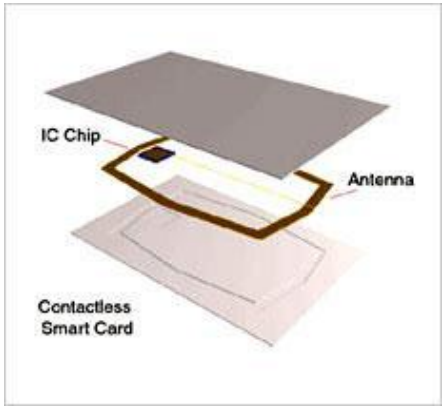
# How (2) – Identification

- Identification is done by presenting a card at the reader
- In this case the card represent the identity of the user (credential)
- The reader is the first interface in the card access system
- The card and reader communicate using RF technology
- So how the card communicate with the reader?

# How (3) – Identification

- Smatcard has built-in IC chip (memory) and antenna
- The reader always generate RF field. The RF field is pick up by the antenna inside the card
- The picked up field is enough to induce power inside the card IC chip and start transmitting data
- So now the card is in communication with the reader



# How (4) – Identification

- How the card communicate with the reader is determined by the card type or protocol or standards (TV repairman language..)
- In general card can be categorised into 2 major types:-
  - ✓ 125 kHz based technology
  - ✓ 13.56 MHz based technology
- 125 kHz technology card (not used anymore)
  - ✓ No ISO/IEC standards. Based only on industry standards
  - ✓ Sometimes known as proximity card (do not be confused with this!)
  - ✓ Mostly read only technology with only one application
  - ✓ Thus is good if the process only requires identification only
  - ✓ Weak security

# How (5) – Identification

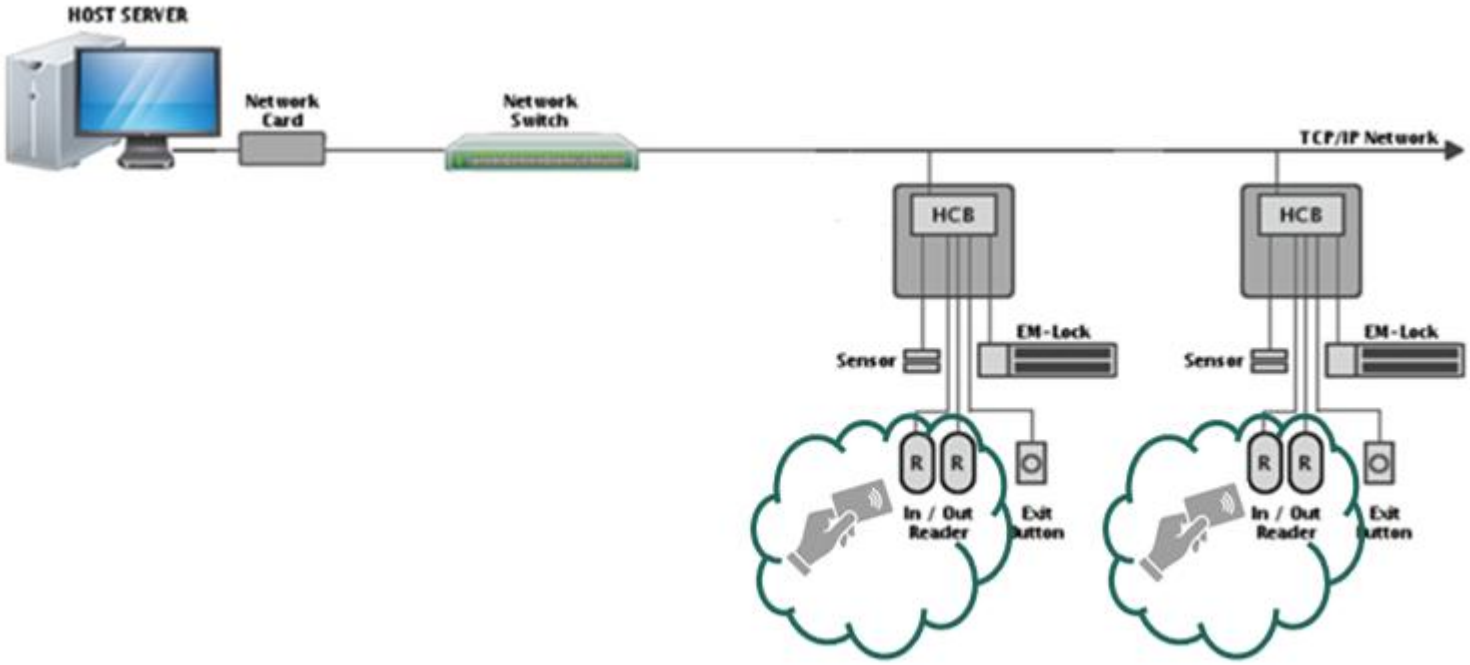

- 13.56 MHz technology card
  - ✓ Based on ISO/IEC 14443 & 15693
  - ✓ Communication between card and reader must be encrypted to avoid cloning etc
  - ✓ Minimum encryption required is Desfire
  - ✓ Mifare Desfire is an encryption/authetication protocol used with ISO/IEC 14443 type A (DES, AES)
  - ✓ Allow read/write process, thus good for fare collection. Touch 'n' Go?
  - ✓ Can hold many applications (e.g: access cards, parking cards, library cards, biometric templates etc)

# How (6) – Identification

- Combi-card
  - ✓ Normally the card has 13.56 MHz and UHF components
  - ✓ The UHF component is used for long range application, e.g: boom gate
  - ✓ 13.56 MHz component (Desfire) is used for normal door access
  - ✓ Requires special long range reader with UHF capability

# How?

- Let's recap again and see how far have we gone?
- So now the reader has captured the data inside the card, what's next?



# How (1) – Authentication

- After identifying yourself to the system, what next?
- If someone knock at your door and says he is coming to repair your TV, will you let him in straight away or will you do some checking first?
- That's is exactly the next process after identification
- Authentication is the process of ensuring you are what you are, what you can and cannot do, what is your access level, are you allowed in at that particular time etc
- So we need some sort of database where all these rights are stored and compared with

# How (2) – Authentication

- In card access this can be done either through a remote server or local database
- Remote server is normally centralised where the master database is kept
- Local database is inside the door access controller, as shown below. Each door normally have one controller (refer previous diagram)

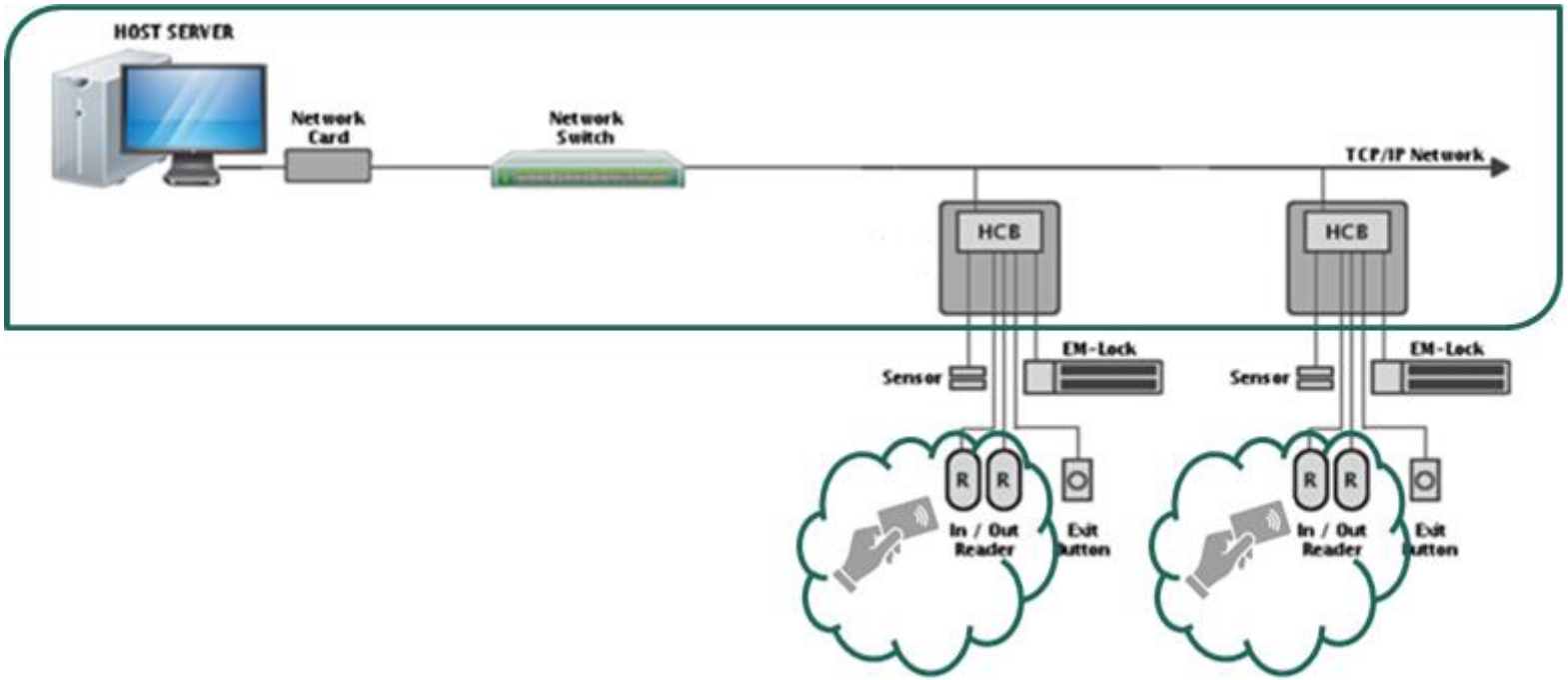
| Technical Specification | |
|---|---|
| MCU | 32bits @ 60MHz |
| Memory | • 256K Flash Memory<br>• 32K SRAM (Buffer)<br>• 64Mbits Non-Volatile SPI Flash Memory (Storage) |
| Card holder | 30,000 |
| Event Transaction | 80,000 |
| Digital/Supervise Inputs | Max. 8, User configurable |

# How (3) – Authentication

- Local database made cross referencing faster and quicker, but need scheduled updating from the master database. If the network is down door access is still possible because of the local database inside the door controller.
- New user data cannot be uploaded to the door controller if the network is down. So does the door transactions/events uploading to the master/server.
- What are the criteria normally associated with authentication?
  - ✓ Who you are & your access level
  - ✓ When are they expecting you (holiday mode, shift, weekend, after office etc)
  - ✓ Anti passback (global, hard, soft etc)
- Provides audit trail

# How?

- The user has been identified and authenticated by the system, so what's next?



# How (1) – Authorisation

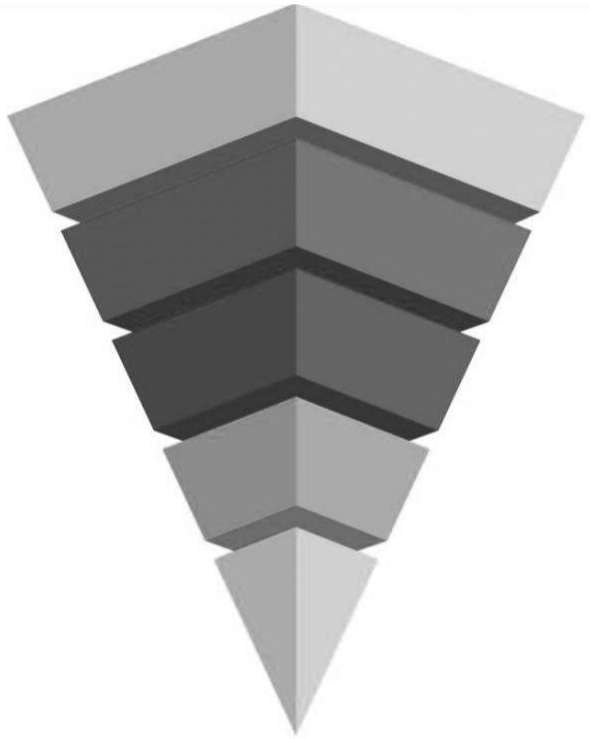
- Let suppose that now you've been rightly identified, your credential checked out and authenticated, what's next? So what happen to the TV repairman? You open the door and let him in..
- Well in card access the authorisation process in similar but in a different way
- The components related to door access for authorisation is:-
  - ✓ EM lock
  - ✓ Door sensor
  - ✓ Exit button
  - ✓ Breakglass

# How (2) – Authorisation

- After valid identification and authentication, the relay at the controller will de-energise the EM lock and door is released
- Exit button is used for exiting without authentication
- Door sensor monitors door ajar status (time out) and after certain preset delay the relay energise the EM lock so the door is locked again
- Emergency breakglass is to provide fail-safe exit during emergency by cutting the power to EM lock independent of the controller


# How (1) – Placement

- Understand the purpose and concept of access control
- Where to put the electronic access control? (Similar to camera placement)
  - ✓ Need to limit access to the complex/premise? (boomgate?)
  - ✓ Limiting access to certain building? (access control at entrance, e.g: Flap barrier, turnstile, door access etc)
  - ✓ Limit access to certain office / floor in the building? (access control at lift, office area etc)
  - ✓ Limited access to certain area/room? (e.g: server room, control room etc)

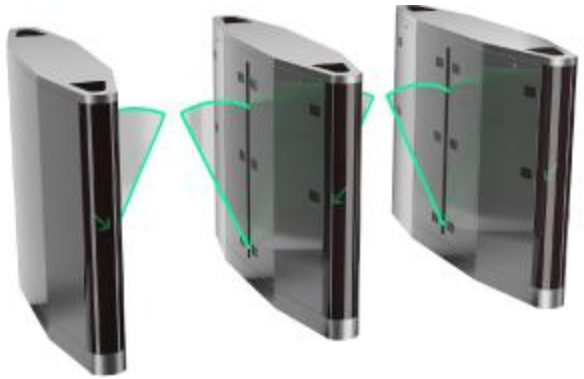


# What (1) – Application

- By now you should have understand the fundamental theory and concept behind card access system
- You should see that the same concept can be applied to other type of electronic access control such as:-
  - ✓ Time attendance
  - ✓ Turnstile
  - ✓ Boom gate system
  - ✓ Door monitoring
  - ✓ Guard tour etc

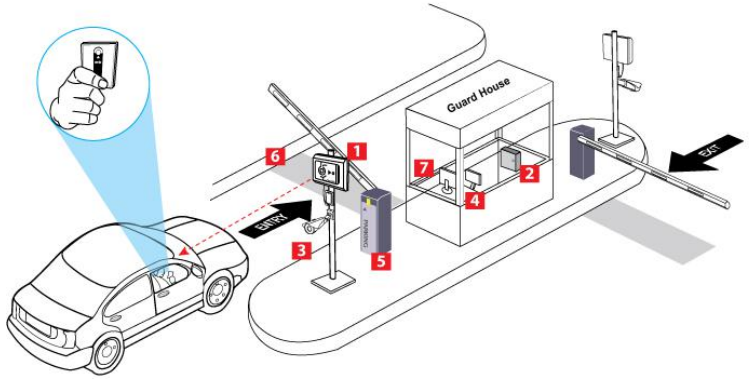
# What (2) – Application

- Time attendance
  - ✓ Only used the identification and authetication process
  - ✓ Reader and controller at main entrance
  - ✓ Rules created in the software
- Flap barrier/turnstile
  - ✓ Similar to door operation
  - ✓ Only reader and controller used



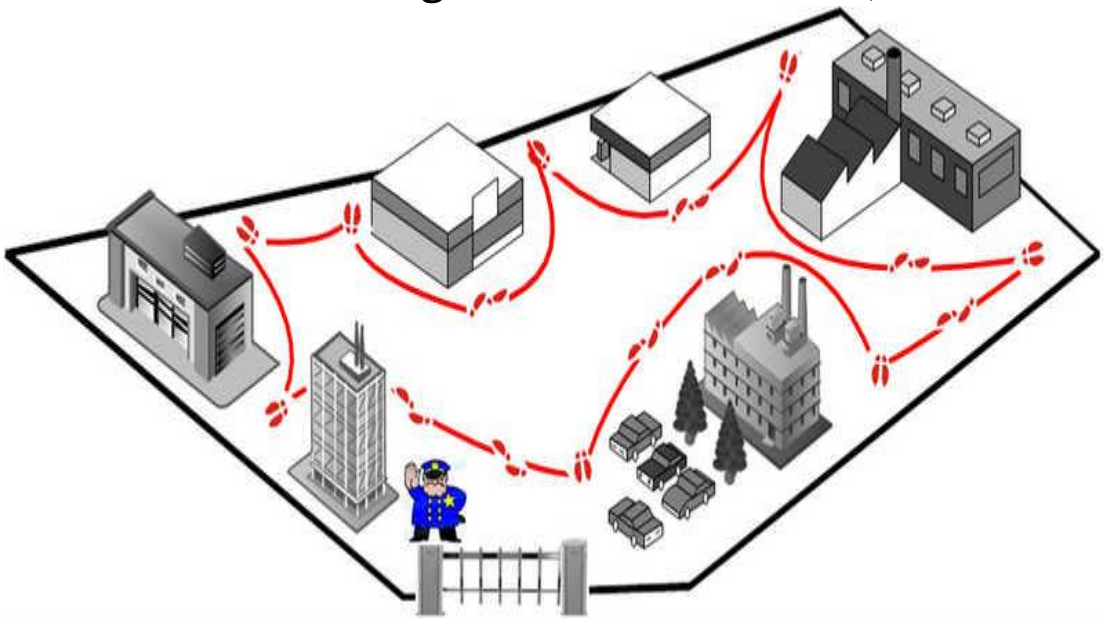
# What (3) – Application

- Boom gate
  - ✓ Normally road entrance to building, parking etc
  - ✓ Same concept as flap barrier
  - ✓ Used loop detector for safety
- Door monitoring
  - ✓ Used where soft monitoring is required
  - ✓ Use controller and door sensor
  - ✓ Normally used to minitor suspicious activity, yet maintaining easy access



# What (4) – Application

- Guard tour
  - ✓ Similar to time attendance system
  - ✓ Use reader and controller
  - ✓ Combined with guard shift or rotation, schedule check in etc



Unit Perunding Akustik

# Thank You For Listening