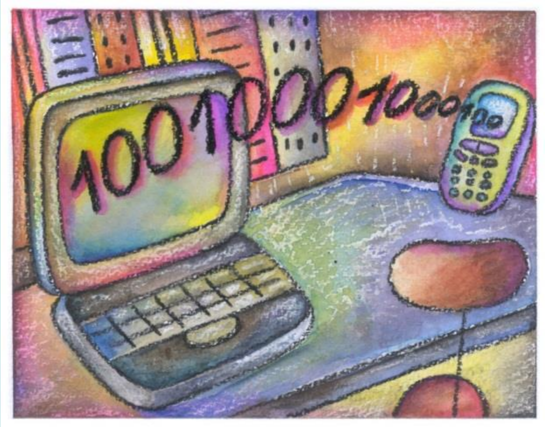
Singapore Polytechnic

Wireless Technology Applications
RFID Technology
Part II

Melvyn U Myint Oo
T16620
68970688
melvyn_oo@sp.edu.sg

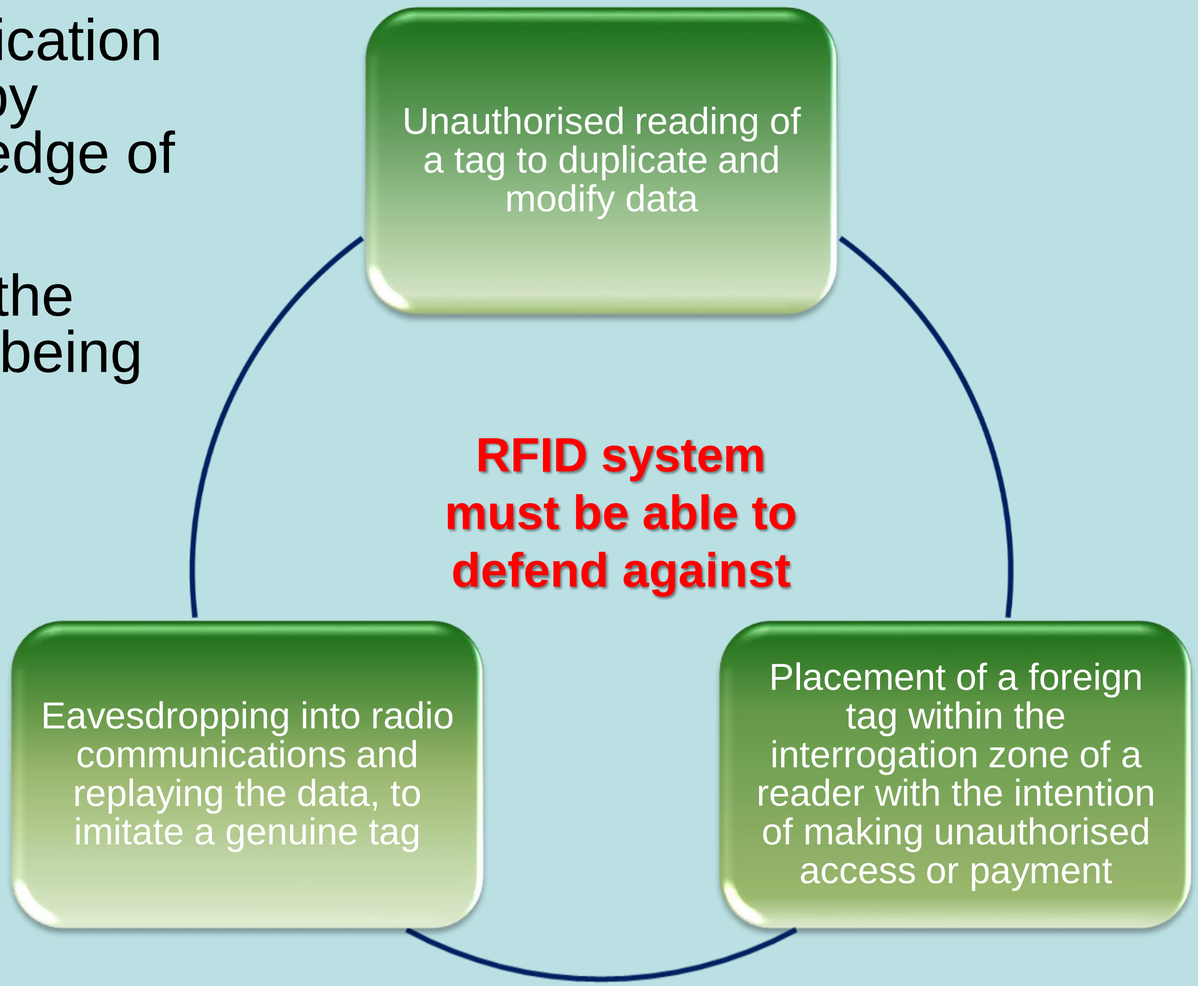


At the end of this lecture, you should be able to:

1. Explain RFID security
2. Explain the advantages and limitations of RFID
3. Explain the passive, semi-active and active types of RFID system
4. Explain the various standards, performances and applications for RFID system

RFID Security

- Modern authentication protocols work by checking knowledge of a key
- How to prevent the secret key from being cracked?



Singapore Polytechnic

RFID Security

- RFID Security Methods
  - Mutual Symmetrical Authentication
  - Authentication using Derived Keys
  - Encrypted Data Exchange

SP Singapore Polytechnic

Mutual Symmetric Authentication

- Tags and readers contain same key K
- Reader issue GET_CHALLENGE command to tag
- Tag generates random number R_A and send to reader
- Reader generates random number R_B, computes and sends Token 1

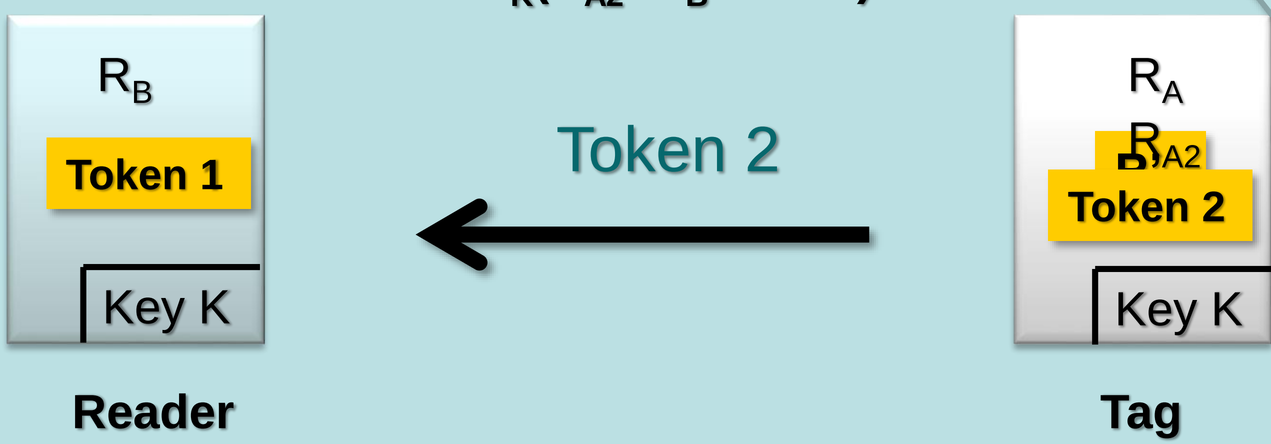
Token 1 = $e_K(R_B//R_A//ID_A//Text1)$

Mutual Symmetric Authentication

- Tag decrypts token 1 to get R'_A
- R'_A compared with R_A for tag to confirm that reader is authentic
- R_{A2} is generated in tag and used to encrypt t

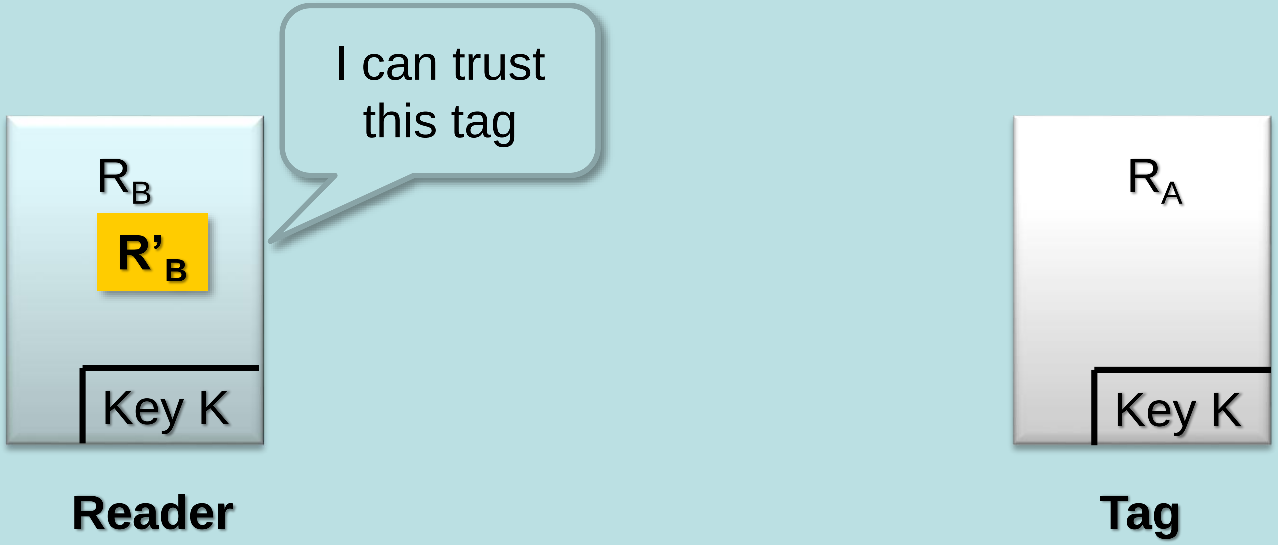
I can trust this reader

Token 2 = $e_K(R_{A2}//R_B//Text2)$



Mutual Symmetric Authentication

- Reader decrypts token 2 to get R'_B
- R'_B compared with R_B for reader to confirm that tag is authentic



Advantages of mutual authentication procedure

- Keys never transmitted over the air
- Two random numbers are encrypted every time. Cannot obtain secret key from inverse transforming R_A to get token 1
- Token can be encrypted using any algorithm
- Recording an authentication sequence for playback later would fail
- Random key can be calculated from random numbers generated, to secure subsequent data transmission

But…

Disadvantage

- All the tags/transponders belonging to an application are secured using the **same key K**

RFID Security

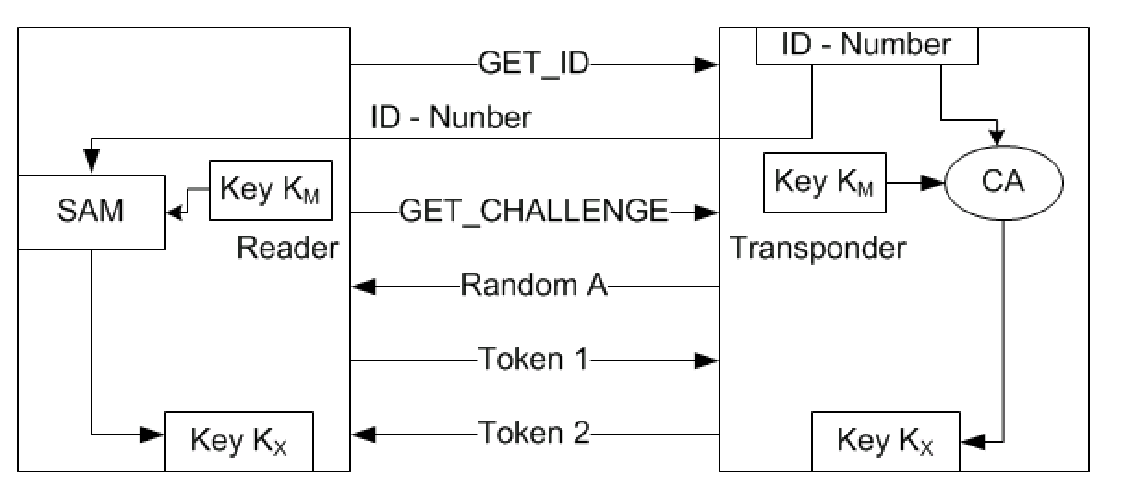
RFID Security Methods

- Mutual Symmetrical Authentication
- Authentication using Derived Keys
- Encrypted Data Exchange

Authentication using Derived Keys

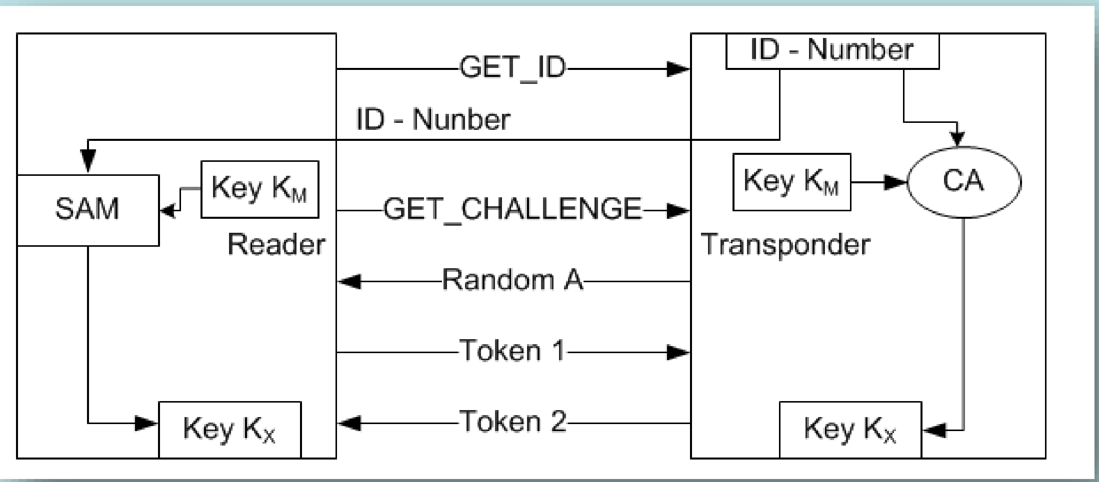
- Secure each transponder with a different cryptological key
- Each tag have a unique ID number which is read out during its production.
- A key K_x is calculated (→ derived) using a cryptological algorithm (CA) and a master key K_M

$$CA(ID, K_M) = K_X$$



Authentication using Derived Keys

- Transponder is initialised
- Each transponder receives a key linked to its own ID number and the master key K_M
- The SAM (Security Authentication Module) normally takes the form of a smart card with contacts incorporating a cryptoprocessor
- The stored master key can never be read.



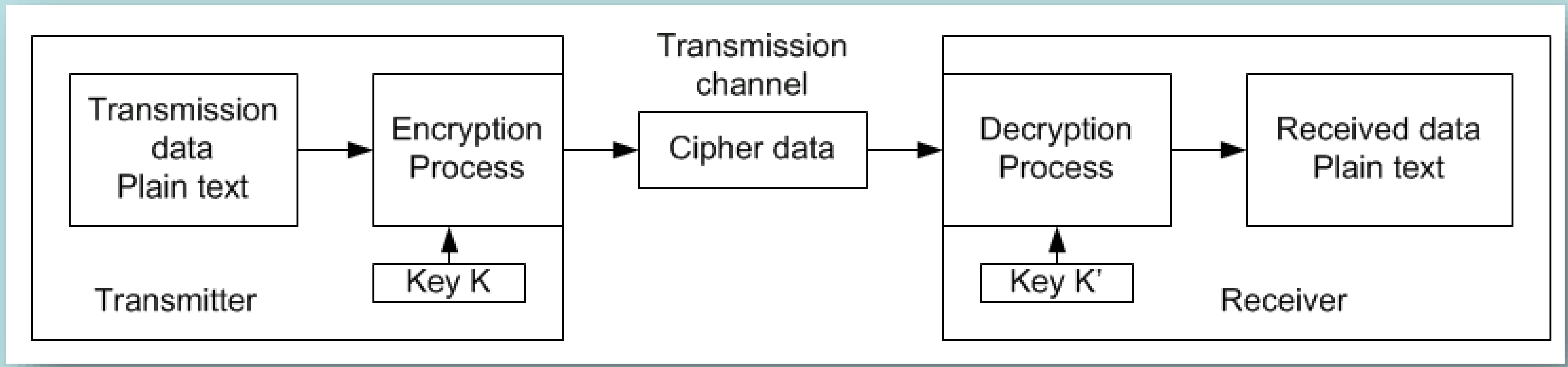
RFID Security

RFID Security Methods

- Mutual Symmetrical Authentication
- Authentication using Derived Keys
- Encrypted Data Exchange

Encrypted Data Exchange

- Data encrypted prior to transmission
- Potential attacker cannot interpret recorded data or recreate transmission data from the cipher data
- Enforce security



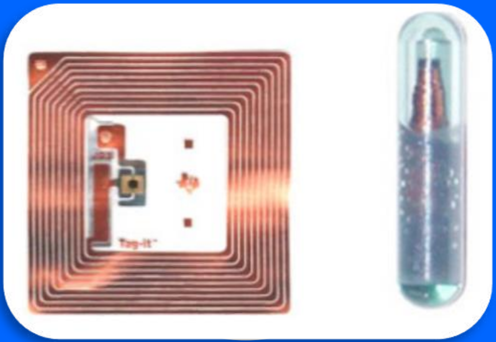
Advantages of RFID

- Contactless
- Writable data
- Absence of line of sight
- Varity of read ranges
- Wide data-capacity range
- Support for multiple tag reads
- Rugged
- Extreme read accuracy
- Perform smart tasks

Limitations of RFID

- Poor performance with RF-opaque and RF-absorbent objects
- Limited penetration power of RF energy
- Environmental factors
- Hardware interference
- Limit of number of tags read
- Immature technology

Types of RFID tags



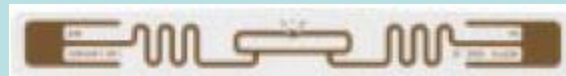
Passive

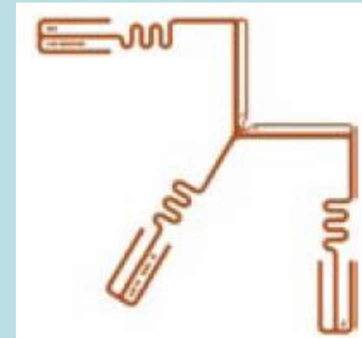
Semi-passive or Semi-active

Active

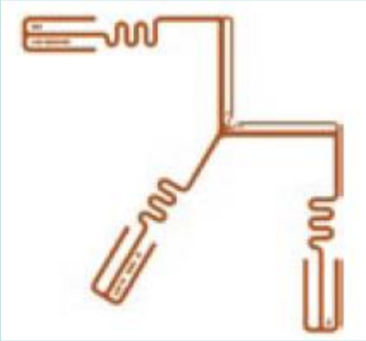
Passive Tag

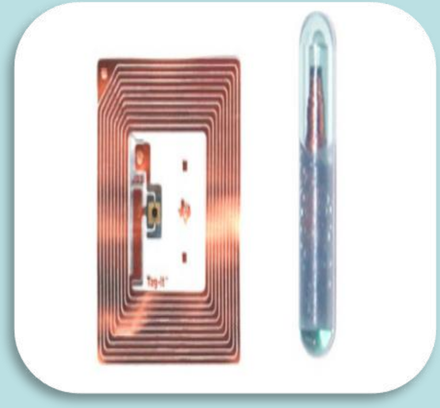
- Requires no batteries
- Backscattering the carrier signal from the reader
- Much smaller, unlimited life span
- Antennae can be manufactured using printing process
- Cheaper to manufacture
- Read distances – 2mm to few metres
  - Reader
  - Frequency Band
  - Power of reader signal
  - Sensitivity of receiver





Passive Tag





- Cheaper to manufacture and have no battery → the majority of RFID tags in existence are of the passive variety.
- Current demand for RFID integrated circuit chips is expected to grow rapidly.
- Two classes of passive tags:

Relatively short read range	Relatively long read range
Less expensive, relatively easy to design and build	More expensive and difficult to build

Semi-passive Tag

- Addition of small battery
- Tag IC is constantly powered
- Antenna need not be designed to collect power from reader signal
- Antenna optimised for backscattering signal
- Faster in response

Singapore Polytechnic

Active Tag

- Own internal power source to power ICs and generate outgoing signal
- Longer range and larger memory
- Can store additional information
- Beacon used to conserve power

Active RFID Tag

Major advantages of active RFID tag

- It can be read at distances of one hundred feet or more, greatly improving the utility of the device.
- It may have other sensors that can use electricity for power.
- It may have the capability to perform independent monitoring and control.
- It may have the capability of initiating communications.
- It may have the capability of performing diagnostics.
- It may have the highest data bandwidth.
- Active RFID tags may even be equipped with autonomous networking; the tags autonomously determine the best communication path.

Active Tag

Problems and Disadvantages

- The tag cannot function without battery power, which limits the lifetime of the tag.
- The tag is typically more expensive, often costing $20 USD or more each.
- The tag is physically larger, which may limit applications.

RFID Standards

Why?

- Communication is determined by original designer
- Protocols vary, e.g. modulation, encoding, commands, security
- Standards needed to assure compatibility

RFID Standards

(Technology/Application/Conformance/Data content)		
Application	**Standard**	**Name**
Animal Management	ISO 11784	Code/Data Structure
	ISO 11785	Technical concept
	ISO 14223	Expand Code Structure & Encoding (Data Security)
Freight Containers	ISO 10374	Automatic Identification
	ISO 18185	Electronic Seals for Security
	ISO 23389	Read Write RFID
Near Field Communication	ISO 18092	Near Field Communication Interface & Protocol

RFID Standards

Application	Standard	Name
Identification "Vicinity" Card (cm to 0.7m)	ISO 15693-1	Physical Characteristics
	ISO 15693-2	Air Interface & Initialization
	ISO 15693-3	Anti-Collision & Protocol
Identification "Proximity" Card (mm to cm)	ISO 14443-1	Physical Characteristics
	ISO 14443-2	Radio frequency and power
	ISO 14443-3	Initialization & Anti-collision
	ISO 14443-4	Transmission Protocol

RFID Standards

Item Management Application

Standard	Name
ISO 18000-1	Reference Architecture that provides Generic Parameters
ISO 18000-2	Air Interface below 135 kHz
ISO 18000-3	Air Interface at 13.56 MHz
ISO 18000-4	Air Interface at 2.45 GHz
ISO 18000-5	Air Interface at 5.6 GHz
ISO 18000-6	Air Interface at UHF; 860 MHz to 960 MHz
ISO 18000-7	Air Interface at 433 MHz

RFID Standards

Item Management Application

Standard	Name
ISO 15961	Data Protocol: Application Interface
ISO 15962	Data Protocol: Data Encoding/Syntax Rules
ISO 15963	Unique ID
ISO 18001	Application Requirements Profiles
ISO 18046	Tag and Reader Performance Test Method
ISO 18047	Device Conformance Test Method

RFID Standards

Frequency ranges used for RFID systems

- 125/134KHz or low frequency (LF)
- 13.56MHz or high frequency (HF)
- 433/869/915MHz or ultra-high frequency (UHF)
- 2.45/5.8GHz or micro-wave (µW)

RFID Standards

Typical relative performance of RFID systems

LF 125 KHz

Max Read Range (Passive Tags) < 0.5m

General Characteristics

- Relatively expensive, even at high volumes.
- Low frequency requires a longer more expensive copper antenna.
- Additionally, inductive tags are more expensive than a capacitive tag.
- Least susceptible to performance degradations from metal and liquids, though read range is very short.

RFID Standards

Typical relative performance of RFID systems

LF 125 KHz

Tag Power Source

- Generally passive tags only, using inductive coupling

Typical Applications

- Access control, animal tracking, vehicle immobilizers POS application including SpeedPass

RFID Standards

Typical relative performance of RFID systems

HF 13.56 MHz

Max Read Range (Passive Tags) < 1m

General Characteristics

- Less expensive than inductive LF tags.
- Relatively short read range and slower data rates when compared to higher frequencies.
- Best suited for application that does not require long range reading of multiple tags.

RFID Standards

Typical relative performance of RFID systems

HF 13.56 MHz

Tag Power Source

- Generally passive tags only, using inductive or capacitive coupling

Typical Applications

- "Smart Cards", Item-level tracking including baggage handling (Non-US), libraries

RFID Standards

Typical relative performance of RFID systems

UHF 868 - 915 MHz

Max Read Range (Passive Tags) < 3m

General Characteristics

- In large volumes, UHF tags have the potential for being cheaper than LF and HF tags due to recent advances in IC design.
- Offers good balance between range and performance - especially for reading multiple tags.

RFID Standards

Typical relative performance of RFID systems

Microwave 2.45 GHz & 5.8 GHz

Max Read Range (Passive Tags) < 1m

General Characteristics

- Similar characteristics to the UHF tag but with faster read rates.
- A drawback to this band is that microwave transmissions are the most susceptible to performance degradations due to metal and liquids, among other materials.
- Offers the most directional signal, ideal for certain applications.

RFID Standards

Typical relative performance of RFID systems

Microwave 2.45 GHz & 5.8 GHz

Tag Power Source

- Active tags with internal battery or passive tags using capacitive, E-field coupling

Typical Applications

- SCM (Supply Chain Management) , electronic toll collection

SP Singapore Polytechnic

Performances of RFID Frequency Ranges

Frequency Range	LF 125kHz	HF 13.56 MHz	UHF 868 - 915 MHz	Microwave 2.45 GHz & 5.8 GHz
Data Rate	Slower			Faster
Ability to read near metal or wet surfaces	Better			Worse
Passive Tag Size	Larger			Smaller

Summary

1. RFID security
2. Advantages and limitations of RFID
3. Passive, semi-active and active RFID
4. RFID standards