RADIO FREQUENCY IDENTIFICATION (RFID)

Working Paper

Table of Contents

1. Introduction

Radio Frequency Identification (RFID) is an efficient contactless identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is an object that can be attached to or incorporated into a product, animal, or person for the purpose of identification using radio waves.

The purpose of an RFID system is to enable data to be transmitted by a mobile device which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc.

2. RFID System

2.1 Components

A basic RFID system consists of following components

- A **tag** made up of a microchip which can either be powered or non-powered.
- A **reader** that communicates with the tag sending and receiving information
- **Reader antenna** is a mandatory component. Some current readers have built-in antennas
- **Controller** is a mandatory component. However, some current readers have built in Controller.
- **Middleware** that records and transmits the tag information to a central repository.
- **Sensor and actuator** are optional components, which can be used for external input and output of the system.
- **Communication infrastructure** is also a mandatory component. It is a collection of both wired and wireless network and serial connection infrastructure that is used to connect the previously listed components together so that they can effectively communicate with each other.

Block diagram of the operational RFID is shown in Fig 1:

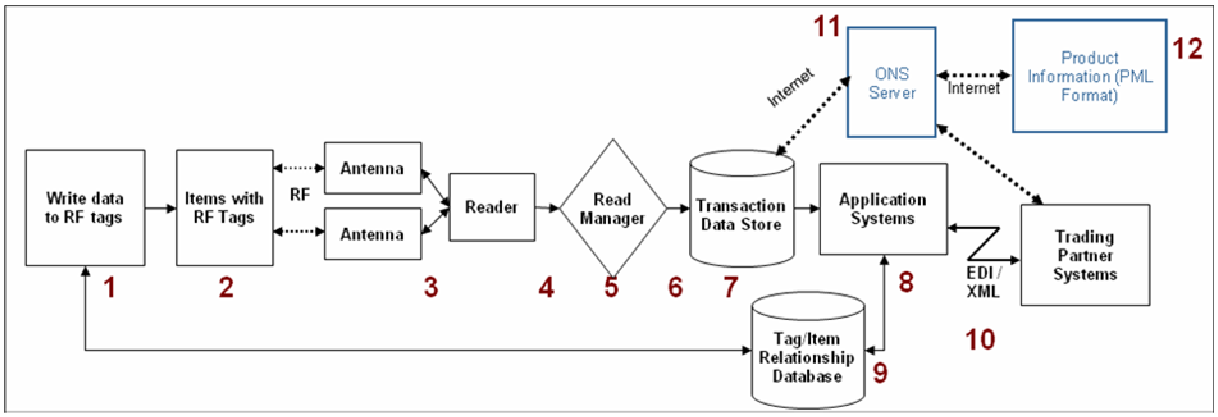

Figure 1: RFID Block Diagram

2.2 Classification of Tags

On the basis of on-board power supply tags can be following types

- Passive
- Active

Passive tags require no internal power source and they operate by gathering the energy transmitted by the reader.

Active tags, on the other hand, require a dedicated power source in the form of inbuilt battery. Consequently active RFID systems have larger range but lesser product life.

Detailed comparisons of the active and passive RFID devices are as follows:

	Active	Passive
Power Source	Internal Battery on TAG	Powered by Radio waves
Life	Limited by Battery	Unlimited
Operating Temp	More Limited	Wide Range(-40˚C, -185˚F)
Range	Longer (100m approx.)	Shorter (3 - 4m)
Memory capacity	Larger (up to 128 Kb or read/ write & search)	Smaller (128 bytes of read/write)
Multi-TAG	1000's of tags recognized – up to 100mph	Few hundred within 3m of reader

reading		
Feature Set	Additional Sensors, Alarms, GPS	Identity Basic Data
Cost	$10 - $100	$0.15 – $1
Multi-tag reading	1000's of tags recognized – up to 100mph	Few hundred within 3m of reader
Example Case	Track large assets, save info. to TAG	Single use tags, typically in open loop supply chains

Table I: Active v/s Passive RFID systems

2.3 Operation

In a typical RFID system, individual objects are equipped with a small, inexpensive tag. The tag contains a transponder with a digital memory chip that is given a unique electronic product code.

The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer. The application software on the host processes the data, and may perform various filtering operations to reduce the numerous often redundant reads of the same tag to a smaller and more useful data set.

The complete operation of the RFIS system can be understood from Fig 2.

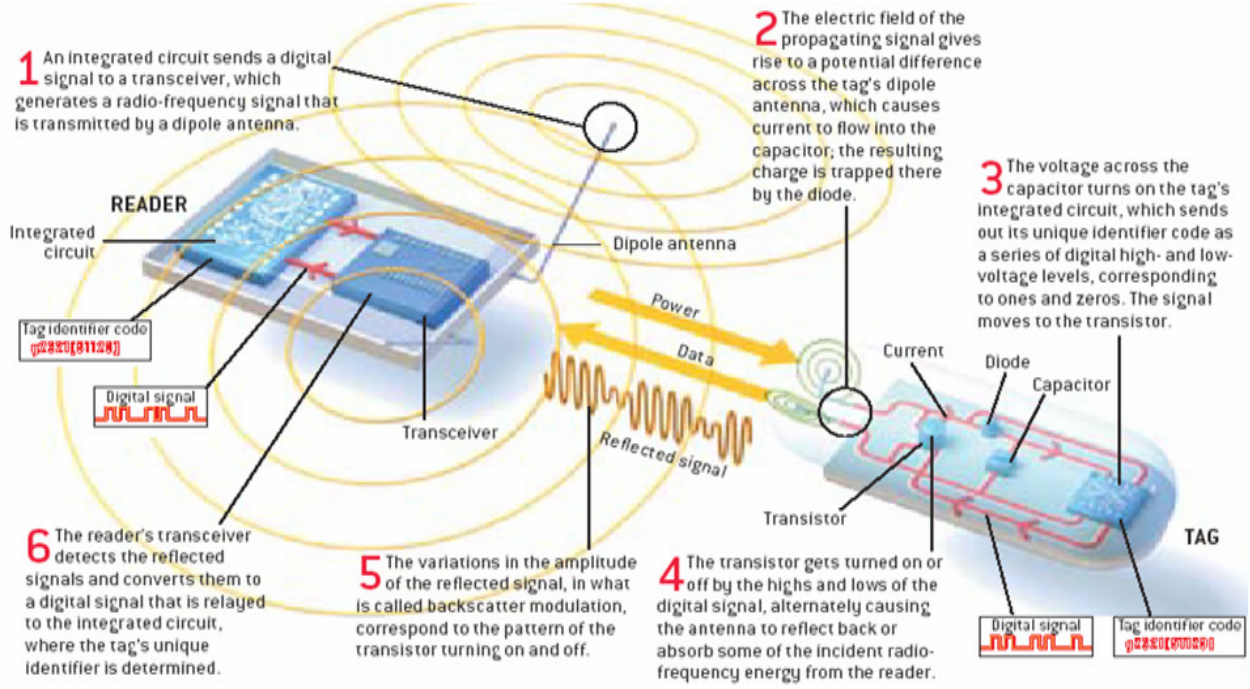

Fig 2: RFID during operation

2.4 RFID Issues

Several security and privacy issues exist with RFID applications that are related to federal and commercial use of RFID technology. The security of tags and databases raises important considerations concerning the confidentiality, integrity, and availability of the data on the tags. Most privacy and security concerns about RFID involve the use of RFID at the individual customer level at the point of sale and after the point of sale.

Privacy concerns involves, what information is given to customers when RFID is used; whether options are provided to customers to disable the tag, what data is collected and how it will be used or shared and how long and for what purpose the data will be retained.

2.4.1 Security Issues

Data security issues can arise by direct interceptions of RFID transmissions or by indirect access to networks where transaction data is stored. The information collected by the readers by querying tags is transferred to a middleware. Security concerns may arise regarding the collection of data during wireless transmissions, the storage of the data, and the physical security of the data storage site. Without effective security controls several security issues can like

- Any compliant reader can read data on the tag.

- Data transmitted through the air can be intercepted and read by unauthorized devices.
- Unauthorized users can access data stored in the databases.

2.4.2 Privacy issues

RFID technology used in businesses and industry helps in understanding critical business processes by collecting and analyzing business relevant information. But such data collections can also lead to the accessibility of personal information. It is very vital to maintain a balance between the utility of the technology and the privacy protections. Privacy issues associated with RFID implementation include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of information.

Most personal privacy threats arise from the fact that tags with unique IDs can be easily associated with a person's identity. Once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual.

Corporate builds an items database associated with the people identity in corporate information systems. When they discard these electronic breadcrumbs, the association between corporate and the items isn't broken. The threat arises when discarded breadcrumbs are used, for example, to commit a crime or some other malicious act.

In addition to issues about the planned uses of such information, there is also concern surrounding the possibility that organizations could develop secondary uses for the information; that is, information collected for one purpose tends over time to be used for other purposes as well. This has been referred to as "mission-" or "function-creep."

Placing covert readers at specific locations can also lead to privacy threats as the individuals carrying unique tags can be monitored. The cloning threat Researchers at Johns Hopkins University and RSA Laboratories demonstrates that RFID tags could have security consequences beyond merely tracking or profiling consumers. They identified a serious security weakness in the RFID tag in Speed-pass devices and many automobile immobilizers systems. The researchers revealed the possibility of payment fraud and new modes of automobile theft by such tags cloning.

The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated. As the uses of technology proliferate, consumers have raised concerns about whether certain collected data might reveal personal information such as medical predispositions or personal health histories and that the use of this information could result in denial of insurance coverage or employment to the individual. For example, the use of RFID technology to track over-the counter or prescription medicines has generated substantial controversy.

2.4.3 Addressing Privacy & security Considerations

Employing a mechanism that can deactivate, or "kill," a tag at the point of sale can prevent tracking of the individual and item once the tag leaves a store. This feature would still provide the supply chain tracking benefits to the retailer without providing additional information about the consumer beyond the point of sale. However, enforcement may be a challenge, as a tag may inadvertently be deactivated or remain dormant with the potential to be reactivated. Additionally, consumers opting to have the tags deactivated may have to undergo additional procedures that may cost time or money.

Another solution proposed is the introduction of a disable/enable mechanism that would disable all tags by default as part of the shopping check-out process and provide consumers with a password enabling them to re-enable their objects' tags if needed**.**

To prevent consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing, several privacy-enhancing technologies (PETs) have been proposed. "Selective blocking", involves using a cheap passive RFID device that locally jams RFID signals by interrupting a standard collision avoidance protocol, allowing the user to prevent identification if desired. Other PETs include shielding RFID tags from scrutiny using what is known as a Faraday Cage—a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies) as well as active jamming of RF signals Further details regarding all privacy-enhancing technologies can be obtained from detailed report.

Government and industry groups have also proposed using an opt-in/opt-out framework. This framework would provide consumers with an option to voluntarily participate in RFID transactions that gather data about them.

Consumers would be informed of the existence of the tags and the type of information that would be collected and could then decide whether to participate in the transaction or opt out. A concern of this hybrid system is the potential disparity in benefits received between consumers who opt in versus those who opt out, similar to customer loyalty cards, and the notion that this framework might penalize consumers who articulate their privacy preferences. Also, a study has suggested that organizations using RFID workplace access devices should implement "fair information practices" and communicate those policies to employees. As in other contexts in which personal information is collected from consumers, a company that uses RFID to collect such information must implement reasonable and appropriate measures to protect that data.

3. RFID around the world

Following Frequency Spectrums and their corresponding maximum power limits are being used world wide for RFID operations:

Frequency bands	Characteristics	Applications
LOW **100-500 KHz**	• Short to medium read Range (<0.5m) • Low read speed	• Access control • Animal identification • Inventory control
HIGH **10-15MHz** **850-950MHZ**	• Short to medium read Range (<1.0m) • Potentially inexpensive Medium reading speed	• Access control • Smart cards, • Item level tracking
ULTRA-HIGH **860-930 MHZ**	• Long read range (<0.30m) • High reading speed • Line of sight required	• Supply chain management • Pallet tracking
Microwave **2.4-5.8 GHZ**	• Long read range (the range of a passive 2.45 GHz tag is in the order of one meter. • Active tags used in road toll applications have a range in the order of ten meters.) • High reading speed	• Railroad car Monitoring • Toll collection Systems • Vehicle Identification

- Line of sight required

Table II a: RFID Worldwide

S.No	Band	Frequency	Power
1.	LF	<135KHz	72 db UA/ m
2.	HF	13.56MHz	60 db UA/ m
3.	UHF	433, MHZ	10 – 100 m W
		865-868 MHz	10 – 100 m W
		902-928 MHz	2 Watts
4.	Microwave ISM Band	2.40 - 2.483 GHz	2 Watts
		2.446 - 2.454 GHz	2 Watts
		5.725 – 5.875 GHz	2 Watts

Table IIb: RFID Worldwide: Frequency Spectrums

Study of various countries has revealed that mostly 865-868 MHz band is in use for RFID applications in Europe and 902 to 922 MHz in Latin American countries. In most European and Asia-Pacific countries, 865-868 MHz band is most popular for the RFID applications. This indicates that RFID equipment for this band is adequately available and we may get various cases for type approval.

4. RFID in Pakistan

PTA, being the regulator of Pakistan telecom market, realized the utility of RFID applications in various sectors. It undertook a thorough study on the subject with the help of a consultant and later after analysis of the whole report did consultation on the topic with Government Ministries and concerned security agencies. Following the consultation process below mentioned frequencies have been identified for RFID systems in Pakistan:

S. No.	Frequency Band	Maximum effective Radiated Power / Field Strength	Distance	
			Active	Passive
1.	125 – 134 KHz	72 dBuA/m	100m	10m

2.	433.05 – 434.79 MHz	100 mW	-do -	-do -
3.	865 – 868 MHz	100 mW	-do -	-do -
4.	2.4735-2.4835 GHz ISM Band **(Indoor Use Only)**	2 W	30m	2-5m
5.	5.725-5.850 GHz ISM Band (Region 3) **(Indoor Use Only)**	2 W	30m	2-5m

Table III: RFID Spectrum Recommended in Pakistan

Note: *FAB has no concern for the usage of this frequency chunk for RFID stand alone applications.*

2.4 & 5.7 GHz bands are Industrial, Scientific and Medical (ISM) bands and are strongly recommended for RFID which have most of its application in industrial domain. The point to be considered is the amount of bandwidth which will be permitted in the said bands. Recently, FAB has cleared 2.4 GHz band earlier being used for military applications. Moreover, FAB has no reservation in providing 125-134 KHz, 433.05 – 434.79 MHz, 865 – 868 MHz and 5.7GHz ISM band for Region3, for RFID *stand alone* (un-networked) applications.

5. PTA Recommended Framework

ID division of PTA after thorough technical study of the subject is currently working on drafting recommendations for the formal approval from the authority. In this respect following is criteria is recommended for use of RFID applications in Pakistan:

Sr.	RFID Type		Recommended distance	PTA proposal
a.	Indoor Active	-	Distance upto 10m (Standalone)	No Type Approval No Licensing
b.	Indoor & Outdoor Passive	-	Distance <= 0.5m (Standalone)	No Type Approval No Licensing
c.	Indoor Active	-	Distance > 10m (Standalone)	Type Approval No Licensing.
d.	Outdoor Passive	-	Distance > 0.5m (Standalone)	Type Approval No Licensing.
e.	Outdoor Active	-	Upto 3m (Standalone)	No Type Approval No Licensing
f.	Active & Passive	-	Upto 100m	Type Approval

	with Networking (Domestic use only)		Data limited to Pakistan	Licensing
g.	Active & Passive	-	Upto 100m, through satellite Connectivity (Domestic use only)	Type Approval Licensing & on case to case basis
h.	Indoor Passive	-	Greater than 0.5m	Not allowed

i. All RFID system networked will require Class Value Added Licensing (CVAL).

j. RFID should only be used for terrestrial applications and services.

k. Satellite based RFID system may be allowed on case to case basis subject to clearance

l. RFID data transfer outside Pakistan is not allowed.

m. Permissible Power Ratings to be provided by FAB against Frequencies cleared by FAB and discussed in PTA presentation during the meeting.

PTA wants to make RFID proliferation process in Pakistan as industry friendly as possible. In this regard this working paper is being placed at the PTA website for comments from concerned people of the industry. You are encouraged to comment, suggest or criticize on any of the above stated recommendation in order to improve the said. Please provide solid reasons as to how your proposal would benefit the **entire** industry. It would be appreciated if you could provide your comments on the following issues within **15** days of posting of this document on the website.

Q.1 Do you agree with the proposed framework of PTA? If **NO** improvements you think are further required!

Q.2 What advantages or disadvantages to Pakistani market and public do you foresee due to implementation of this proposed framework?

Q.3 Should specific protocols be allowed in implementation of RFID system or technology neutrality should be followed in RFID as well?

Q.4 Is there a serious demand of RFID applications in market? i.e. How do you see scope of RFID applications in Pakistani market

Q.5 Do you want to be part of any such study group in future?