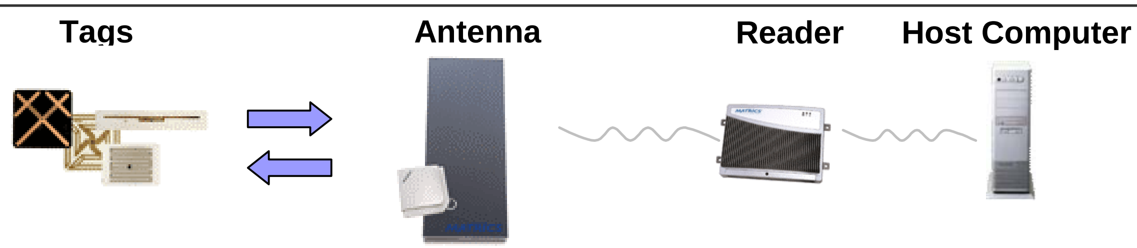
Attachment D: RFID Technology Overview

The following sections provide an overview to RFID technology, the applications in which they are currently used and other considerations of RFID technology as it might be applied to the US-VISIT Increment 2C problem. RFID technology was first used in World War II for identification, friend or foe (IFF) systems, and has been available in one form or another since the 1970's. There is no one definitive "RFID technology"; there is a wide range of technical solutions ranging from simple, inexpensive, and common to those with more functionality, performance and cost. RFID is part of our daily lives – in car keys, toll tags, access cards… This section will provide an overview of this technology and its applications.

1.1 RFID Tag Technology Description

In its simplest form in common use today, an RFID system consists of four elements, as shown in Figure 3-1. The RFID tag element consists of an antenna integrated with a microchip. The RFID reader and antenna transmit an electromagnetic RF signal. This signal is received by the RFID tag via the tag's antenna. The energy in the received signal provides the power to the tag that allows the microchip to operate. This is referred to as a "passive" tag.



Tags
- Device made up of an electronic circuit and an integrated antenna
- RF used to transfer data between the tag and the antenna
- Portable memory
- Read-only or read/write
- Hundreds of tag styles available

Antenna
- Receives and transmits the electromagnetic waves
- One or more antennae attached to a reader

Reader
- Communicates with the tag via antenna
- Receives commands from application software
- Interprets radio waves into digital information
- Provides power supply to passive tags

Host Computer
- Reads/writes data from/to the tags through the reader
- Stores and evaluates obtained data
- Links the transceiver to applications

Figure D-1 Components of a Passive RFID System

This data from the microchip is then added to an RF signal that is "reflected" by the tag back to the reader through the reader antenna. This process is referred to as passive backscatter. The reader contains the electronics to receive this signal from the tag, extract the RFID tag's code from the signal, and return it to its digital form, and provide that returned code to a host computer.

Passive tags systems are reader talk first. The tags are mute until a signal is received from a reader. Also, only one reader at a time can energize a passive tag; if more than one reader tries to "light up" a passive tag a condition known as "reader collision" occurs.

Passive RFID systems can read multiple tags at once. In a process called "singulation," the reader will rapidly cycle through tags and determine which ones are present. There are many methods of singulation, but the principle of identifying a single tag is the same. This is very important when trying to quickly identify all tags in the reader's field, and is also important when trying to speak to specific tags.

The simplest passive RFID tags have microchips that contain a single bit. These tags are referred throughout the world as electronic article surveillance (EAS) tags and are used to prevent shoplifting. Other tags contain a simple read-only numeric code or serial number. The code, which is stored in memory on the microchip, can be written to the tag at the time of first use or applied at the time the RFID tag is manufactured. The code is used to reference information stored elsewhere, such as in a database. Several tag coding standards exist, and are detailed in the "standards" section (Section 3.9).

Generally speaking, the more functionality embedded on a tag, the slower it is, the shorter the range and the higher the price. There are RFID tags that have greater amounts of memory, storage and functionality. For instance, some tags have separate areas for different users to access. Other tags have encryption and security features. Still other tags include microchips whose serial number is written to the chip by the user rather than at the point of RFID tag fabrication. This permits greater flexibility in the information that is written to the tag and when it is written. There are tags for almost every application – indeed, there are several thousand tag types in existence at this time. However, it is not possible today to get low cost, long range, high speed passive RFID tags with encryption and high security.

In terms of cost, passive RFID tags range from $0.25 up to $10.00, depending on functionality, packaging, and application. Serial number, read-only tags tend to be the least expensive. The prices of passive RFID tags are highly dependent on the volume of tags ordered – the prices mentioned here are for large orders (in the tens of millions). Lower volumes will generally lead to much higher per tag prices. There is potential for even lower prices for simple tags as standards solidify and as larger numbers of tags are used in the industry. Some preliminary research from sources such as Advanced Marketing Resources, Gartner and RFID Journal indicate that a passive tag with read-only serial number will approach $0.05 by 2008.

In a common application of RFID technology today, RFID tags are combined into an adhesive label that can be applied to packaging for products in the consumer packaged goods supply chain. As the products are moved from manufacturer to warehouse to retailer, the products can be tracked to aid in supply chain management and inventory control. Rapid uptake of RFID in the retail supply chain is driving standards across all industries and is also pushing the cost of RFID down.

More advanced tags are also available. These tags may include small batteries. These "active" tags, as depicted in Figure 3-2, allow them to broadcast a stronger signal that can be received at greater distances than the "passive tags" powered only by the signal received from the reader/antenna system. A key differentiator between active and passive tags is the style of communications. An active tag talks first – that is, it beacons. Since the tag is not depending on a reader to be energized, and because signal processing technology is so powerful, active tags can be read at much greater ranges than passive tags. Active tags can also be used for positioning – determining the XYZ location of the tag – through a process of triangulation.

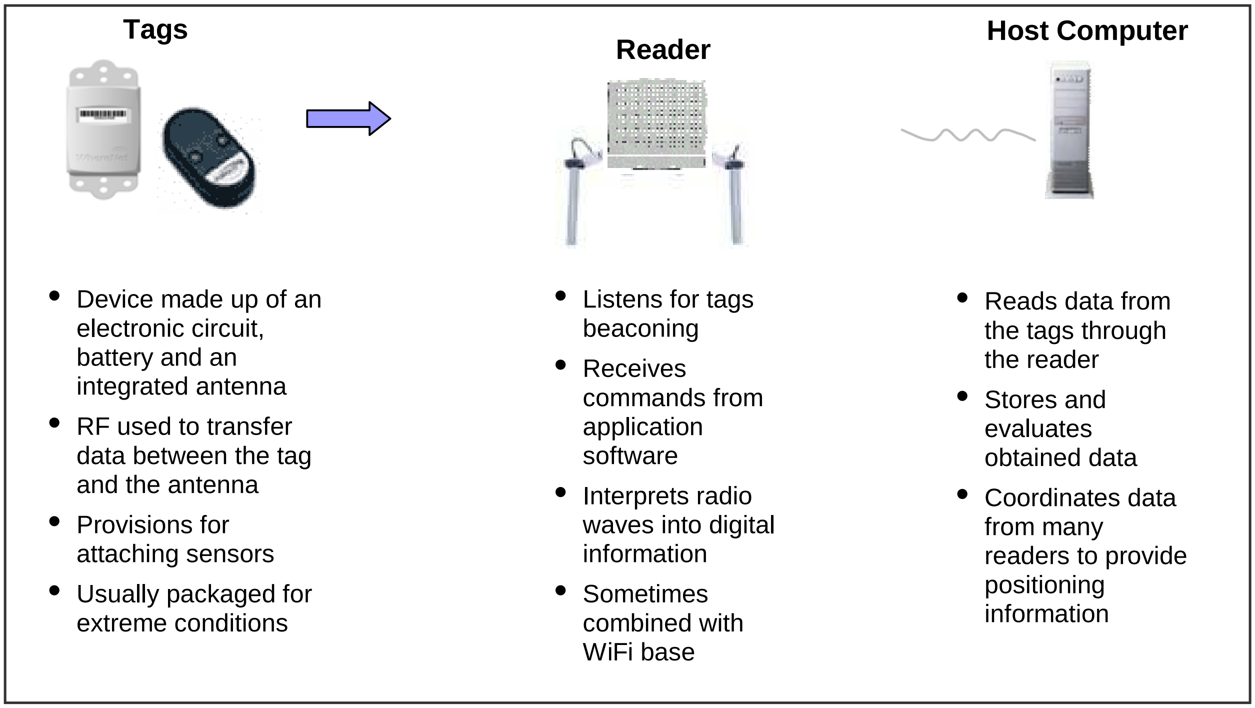


Figure D-2 Components of an Active RFID System

Since there is a communications channel involved, active tags can be integrated with sensor devices, such as temperature, location or motion sensors. These devices can take samples from the sensors, store them, and send them back to the reader along with the standard beacon signal.

A third class of tags exists, alternately referred to as semi-active, semi-passive, or battery assist tags. These tags are akin to passive tags in that they are reader talk first. A battery is present though for one of two reasons. Either it is providing a "boost" for the tag, allowing it to be read and respond in difficult RF environments, or it is used to power a sensor. Such sensors can collect data even when the tag is not powered. This data is then transmitted back to the reader when the tag is read. This is a much slower read process than standard tag reading. The battery and sensor portions of semi-passive tags can drive costs into the $5.00-10.00 range.

1.2 RFID Reader Technology Description

The second major component of RFID systems is the reader. For passive tags, readers energize the tags with energy, receive the results and frequently handle the low-level anti-collision algorithms that allow readers to read more than one tag at a time. For active tags, readers are responsible for listening for the tags' beaconing, and for communicating with other readers to determine positioning.

Readers are generally controlled via a software application programming interface (API) that is provided by the reader manufacturer. Generally, the API also allows for configuring the reader's read cycle, power or other settings. The API software libraries for a given reader may be priced separately for the reader, although many providers bundle the software.

1.3 RFID Antennae Technology Description

Antennae are the third major component of and RFID system. These can range greatly in cost, depending on functionality, application and base operating frequency. Whether it is a shelf, mat, portal, wand or directional antenna, different antennae are required for different applications.

Depending on how many antennae are required, one or many multiplexers may be necessary. A multiplexer allows many antennae to be physically connected to a reader. A configuration using multiplexers may also require an additional communications card such as an RS-485. Many readers contain built in multiplexers, and external varieties are also available.

Cabling for the systems is an important aspect of performance. Although there are generally fewer limits on the distance between reader and host computer, there are signal degradation effects in the cables connecting readers and antennae. High-grade RF cables for this purpose can be expensive, and can have distance limitations.

The combination of the reader, antennae, and multiplexer setup is sometimes referred to as a "read point."

1.4 Host Controller

The host controller is generally a desktop or laptop computer, positioned close to the readers. This controller serves two main functions. First, it is receiving data from the readers and performing data processing such as filtering and collation. Secondly, it serves as a device monitor, making sure the reader is functioning properly, securely and with up to date instructions. Host controllers are connected to readers through networking technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP) or sometimes through serial connectivity. Generally speaking, one controller can manage several readers, with the ratio being dependent on the data volume from those readers.

1.5 RFID Middleware

RFID middleware is software that facilitates communication between RFID readers and enterprise systems. It collects, filters, aggregates and applies business rules on data received from readers. Middleware is also responsible for providing management and monitoring functionality - ensuring that the readers are connected, functioning properly, and are configured the correct way. Middleware may also contain a localized data store for archival of read events.

Host computers and readers may communicate with each other via the EPCglobal Reader Protocol 1.0 standard, although this is not common as of yet. Each middleware vendor must provide firmware for all supported readers. Deployed either centrally or locally, middleware can be managed through user-friendly interfaces, similar to a standard software application. Also, middleware differs in its implementation style - middleware may be implemented on a host computer, a central server, or on intelligent readers.

1.6 Other RFID Technology Considerations

1.6.1 Frequency

RFID systems operate in several regions of the RF spectrum. Differing regions of the RF spectrum tend to be used for specific applications. No one frequency is good for all applications, geographies, or types of operating environments. Within the U.S., the FCC regulates the frequencies and their associated characteristics. These frequencies generally fall into FCC's Part 15 rules, which govern the use of unlicensed radio transmitters (such as cordless phones, baby monitors, or garage door openers) but there are also Part 90 regulations, which allow for higher power transmissions as specific physical locations. There are power, bandwidth and gain regulations associated with all of these frequencies. So even though a common frequency may be available, the power levels allowable at that frequency may not be the same. This section focuses on those frequencies generally in use for passive RFID. Active RFID systems use slightly different standards, but for Entry/Exit purposes we do not cover those.

A frequency used in very early RFID implementations was the low frequency (LF) band of 125-133 kilohertz (kHz). This frequency is in wide use for pet recovery, cattle tagging and access cards. Most LF tags now are sold for car immobilization systems – an RFID chip in the key lets a reader in the steering column know it's OK to start the car. Another popular use for LF systems is timing for marathons, triathlons and bike races. Ranges for LF systems are fairly low, on the order of inches up to two feet.

The closest thing to a common, worldwide frequency today is the 13.56 Megahertz (MHz) band, also known as high frequency (HF). This is available in most parts of the world, albeit with variations in restrictions. HF systems are very frequently used for smart shelf applications, access control, and smart-cards. Related technologies such as near-field communications also use the same HF band. HF has the advantage of a very tunable field shape so that its read pattern can be precisely controlled. It has the disadvantage of a relative short read distance (three feet at most). This limitation makes HF less suitable for vehicle-based exit.

More useful to Entry/Exit in terms of read range and speeds are tags operating at roughly 915 MHz, or ultra-high frequency (UHF). UHF has a higher range and faster data transfer rate than HF. The UHF spectrum is not universally available at the same frequency and power levels worldwide. However, in the U.S., it is available at a power level that allows for read ranges of up to 30 feet with good data transfer speeds.

Finally, microwave frequencies are also used in the RFID realm. The main frequency is 2450 MHz or 2.45 Gigahertz (GHz) although there are some systems available in the 5.8 GHz band. 2.45 GHz is the same band as wireless LANs (or WiFi), and Bluetooth.

Microwave tags have the advantage of being smaller than UHF tags, but generally have shorter ranges. Microwave tags are not in general use in the U.S., but are more prevalent in Japan.

1.6.2 Accuracy

RFID readers and tags do not have 100% accuracy in all instances. Environmental issues, the make-up of the items being tagged and the volumes of tags to be read, all impact read accuracies. Accuracy can be improved by applying a layered approach to acquiring the RFID data.

RFID offers many advantages over manual or semi-automated data collection processes. Any shortcomings in accuracy can be mitigated through the use of redundant readers, information auditing and process redesign. Additionally, minimizing the numbers of tags in a reader's field of view increases accuracy – thousands of tags will not be read as well as dozens or hundreds.

The environmental influence of metal can definitely impact readability of RFID tags. Metal reflects radio waves, so that in a highly metallic environment, the RF signal will be reflected and confuse both readers and tags. However, with proper design and tuning, the presence of metal can be used to *increase* accuracy and performance.

Water also has a deleterious effect on RFID read accuracy. Water absorbs radio waves, and the human body is mostly comprised of water. The most common approach is to add some spacing between the tag and the liquid. This gives the radio waves room to maneuver, so to speak, and get to the tag. A little airspace goes a long way. For Entry/Exit scenarios, we have tested a number of conditions that involve water absorption such as placement of the tag near a body, or holding of the tag inside a hand.

1.6.3 Interference

As RFID systems proliferate, more occurrences of interference will be experienced. Depending on the frequencies and powers used, devices such as phones, wireless handsets and industrial equipment may be affected. Since widespread implementation of RFID technology has not been undertaken before, it is difficult to state what will be impacted. Good engineering and proper tuning will be required.

The perceived health concerns of RF may also come into play. While there is no evidence that there are any negative effects at the power and frequency levels associated with RFID, no one has deployed large-scale implementations yet. More research and monitoring will be needed to address the public's concerns in this matter.

1.7 Current RFID Applications

There are several areas in which RFID technology is being applied today. These are summarized in the following sections.

1.7.1 SENTRI/NEXUS

DHS currently uses RFID technology on the northern and southern borders in support of three separate programs: NEXUS on the northern border, SENTRI on the southern border, both part of the DCL program, and the FAST program for commercial vehicles on both borders. Historically, each has used a unique combination of active transponders and passive RFID tags and readers to meet its identification goals.

NEXUS is an implementation of the DCL program that allows prescreened, low-risk travelers to be processed with little or no delay by United States and Canadian border officials. Approved applicants are issued photo-identification and a proximity card, and make a declaration. They are then released, unless chosen for a selective or random secondary referral.

The NEXUS/DCL program utilizes RFID cards to query Global Enrollment System (GES) to validate the enrollment of a vehicle's passengers for border travel. The NEXUS Intermec RFID system has very limited data, constrained to reading a 64-bit Identification (ID). The GES database uses the 64-bit ID as a key into the GES system to retrieve data that is returned to the Officer client workstation. Although the NEXUS RFID system has the capability to write up to 110 bytes to the RFID, that capability is limited by the GES database. Video surveillance images are also captured in the NEXUS lanes, although this information is only stored locally.

Both SENTRI and NEXUS are using tags in the UHF band.

1.7.2 E-Passport

The U.S. Government Printing Office (GPO) is testing electronic passports (e-passports) embedded with RFID chips that the agency hopes to make standard within the next year. To carry out the tests, the GPO awarded four companies with contracts to provide 13.56 MHz RFID chips to test the e-passport system. The chips comply with the ISO 14443A and 14443B standards.

The eight-week-long testing program, which began in October 2004, involves the National Institute of Standards and Technology (NIST). The GPO will manufacture test passports embedded with RFID chips. NIST will test the passports for durability as well as ensure they meet security and electronic requirements. Some of these tests verify that the chips can withstand 10 years' of normal wear and tear and stamping by customs' officers and still remain functional.

1.7.3 Toll Collection

In many states, toll collection for vehicles traveling at or near highway speeds is accomplished through the use of active RFID tags. There are many systems available today: EZPass (West Virginia, Maryland, Delaware, Pennsylvania, New Jersey, New York and Massachusetts), I-PASS (Illinois), SunPass (Florida) and FasTrak (California). These systems may run at any number of frequencies, but 915 MHz and 5.8 GHz are frequently used. These systems are often linked to a credit card, allowing for stored values to be replenished without need for manually handling the tags. Some card types store value as well.

1.7.4 Payment Systems

Sony's Felica card and Philips ViVOTech are examples of Near Field Communications devices (essentially HF RFID with improved data speeds) used for payment systems. An emerging application of this technology is to use a mobile phone enabled with an RFID chip for payments. Still other payment systems use a small key fob (e.g., ExxonMobil's SpeedPass) linked to a credit card account for payment. This style of RFID application tends to involve heavily encrypted tags with more functionality and memory and generally use the HF band with greatly reduced ranges.

1.7.5 Supply Chain

A popular, emerging application of RFID is in the area of supply chain visibility. The trend is to attach an RFID tag containing a unique identifier to an object at its point of manufacture. This tag would then be read at various intervals up to its point of sale. Manufacturers, retailers and third party logistics providers are in differing states of pilots on products, with the major target benefits being reduction in inventory, a decrease in material handling time, safer and more secure supply chains, and potential post sale applications.

Major retailers such as Wal*Mart, Best Buy and Albertsons are leading the charge, mandating usage of RFID tags on cases and pallets inside the next two years. Furthermore, the U.S. Department of Defense (DoD) has issued similar mandates for its suppliers, also at the case and pallet level. These retailers and the DoD are all specifying the use of UHF band chips in the EPCglobal standard (see Section 3.8)

1.7.6 Access Control

A very common application for RFID is access control. Contactless badges are in use in almost every office and facility. This style of RFID badge tends to work in the LF or HF band, and generally have very low read ranges. These systems tend to utilize very proprietary formats, networks and protocols. The tags are generally packaged in a sealed ID card format. Some ID tags have thin film batteries as well for encryption and information storage.

1.7.7 Animal Tracking

RFID has a long history of being used for animal tracking. From livestock management (for animal movement, feeding, health, and market visibility) to pet tracking, RFID is relatively mature in this field. Animal tracking can be considered one of the largest implementations of asset management using RFID. Generally speaking, low frequency tags are used for animal tracking.

1.8 Security, Privacy, and RFID Technology

An RFID Security/Privacy study has been conducted in concert with the 2C RF Feasibility Study and has resulted in an SBA Security and Privacy white paper, which is included as Attachment H to this document. This white paper discusses all known security and privacy issues that arise from the proposed use of RFID technology in US-VISIT and assesses the capability of available technology to resolve those issues. This security/ privacy study also provides the basis for the subsequent security analysis and evaluation of individual RFID products.

1.8.1 Security

The RFID back-end tag database and the associated network can and certainly will use existing security mechanisms. Depending on the design of the readers and tags, these devices can leverage the security mechanisms already in place in the network and database. A number of RFID security "models" have been postulated. For example, RSA

Security, Inc. has developed a set of RFID Security and Privacy "Attributes" that include tag privacy, tag authenticity, reader security, and tag database security. Authorization and authentication can be supported with certain types of RFID tags but there are cost/benefit tradeoffs.

It is possible that the nature of the interconnection or the interaction between the RFID reader and the existing infrastructure could introduce an exploitable vulnerability, but if security best practices and requirements are observed in integrating the product with the network, this can be minimized.

1.8.2 Privacy

The amount of information gathered about individuals is growing through the proliferation of surveillance cameras and sensors; microchips and RFID tags embedded in devices and products; wireless devices that provide location data; and smart cards and interactive TV that can track viewing and buying preferences. Advances in electronic technologies allow companies and government agencies to store and process large amounts of information about individuals. The Internet provides the ultimate copier device, making this information easily available to millions. Due to the commercial value of personal data, governments and companies have considerable financial incentives to take the time to gather information and to use machine-learning technologies and data-mining techniques to infer customer preferences based on this information

Although the number of organizations using RFID is increasing, resistance from privacy groups to tagging technologies at the consumer level suggests the challenges ahead. As a result of consumer resistance, several retailers have decided to forego the use of RFID tags at the retail level at this time. In April 2003, clothing retailer Benetton Group announced that it was postponing plans to embed RFID tags in one of its clothing lines. In March 2004, METRO AG, the fifth largest retailer in the world, decided to abandon the use of RFID chips in its loyalty cards after protests from privacy groups. METRO continues to use RFID tags in supply management applications. These decisions signaled to many companies that they needed to do more about privacy than just understand relevant legislation. They need consumers to trust them to protect their personal information.

On November 20, 2003, a group of 45 consumer privacy and civil rights organizations from around the world issued a position statement on RFID[1]. These groups identified privacy and civil liberties threats posed by RFID tags, and called for the application of Fair Information Principles, such as those codified in the Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD). The groups also called for a flat prohibition on human tracking or on the use of RFID tags in any way that would reduce anonymity.

[1] RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, November 20, 2003, available at <http://www.privacyrights.org/ar/RFIDposition.htm>.

The SBA long-term vision includes the use of a Self Verifying Device (SVD) that will utilize the same RFID infrastructure, but will add the ability to biometrically verify an individual and send a single, encrypted number for identification purposes. Several near-term strategies can be used to mitigate privacy concerns raised by RFID tags:

- label tags and readers so that the public is aware that they are being used
- discuss the operation of tags in the privacy policy
- provide security safeguards for the data gathered through the tags
- publicize that no personal information is stored on the RFID tag and that tag serial numbers are unique
- make available shielded sleeves that prevent eavesdropping
- educate the public on RFID technology, including the potential for eavesdropping and how to prevent it, for example with shielded sleeves. This would complement current EPCglobal outreach efforts of this kind.
- make known to the public that personal information associated with the RFID tag number is secure stored behind firewalls

Additionally, EPCglobal, which includes a security working group, and other standards groups are aware of security and privacy issues, and are expected to introduce more security features in the standards in the future. It can be expected that encryption of data on tags will appear as prices of tags come down.

Government agencies have a particularly delicate balance to achieve – maintaining privacy whilst protecting our nation's borders and people. The Security and Privacy white paper discusses known security and privacy issues that arise from the proposed use of RFID on US-VISIT and assesses the capability of available technology to resolve these issues.

1.9 Standards

There are several areas of standards that need to be reviewed for a complete understanding of RFID technology. These standards frequently align with applications such as toll collection or animal tracking. This section will discuss the various standards bodies and their relative contributions to the available standards.

1.9.1 ISO

One of the major standards bodies in the world is the ISO. ISO is an organization of the national standards institutes of 146 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO is a non-governmental organization: its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

Therefore, ISO is able to act as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

ISO manages several standards related to the area of RFID. ISO 11784/11785 relates to animal tracking. ISO 14443A/14443B relates to proximity style RFID while ISO 15963 relates to vicinity tagging. ISO 18000 pertains to radio frequency identification for item management, and contains six subsections covering differing frequency ranges. There are many other ISO standards relating to test methods, APIs and conformance standards.

1.9.2 INCITS

The International Committee for Information Technology Standards (INCITS) is the primary U.S. focus of standardization in the field of Information and Communications Technology (ICT) encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as the American National Standards Institute's (ANSI) Technical Advisory Group for ISO/IEC Joint Technical Committee 1 (JTC 1). JTC 1 is responsible for international standardization in the field of information technology. INCITS is accredited by ANSI and operates under its rules, designed to ensure that voluntary standards are developed by the consensus of directly and materially affected interests.

1.9.3 ICAO

The International Civil Aviation Organization (ICAO) is another standards body creating RFID related standards. In 2003, ICAO specified the technical requirements for RFID technology used in electronic passports. These specifications were published in ICAO Doc 9303, and are the focus of the ePassport activities taking place within Department of State.

1.9.4 NIST

The NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is currently working on RFID technology in the construction industry, and has ties into smart card technology through its encryption standards.

1.9.5 EPCglobal

Another very visible standards body applicable to RFID devices is EPCglobal. EPCglobal was formerly known as the Auto-ID Center, originally started at Massachusetts Institute of Technology (MIT). The Auto-ID Center originally sought to bring users of RFID together with technology providers to create an item identification standard as well as to promote technologies to carry the identification. This identification standard, known as the Electronic Product Code, can be thought of as a serialized version of the common Universal Product Code (UPC) found on many consumer goods. However, a key distinction is that while the UPC designates a class of items (i.e., all copies of a certain product sold in the U.S. will have a common barcode) the EPC designates an instance of an item (e.g., each copy of that CD will be identifiable from others).

The EPC, a 96 bit number, is expected to provide an address space of roughly 30 trillion trillion unique identifiers. All users of the EPCglobal system will also have control over their address space – no repeating will be allowed.

In October of 2003, the AutoID Center formally closed up operations and transferred activities to a non-profit entity known as EPCglobal. EPCglobal is a joint venture between EAN International and the Uniform Code Council (UCC). EAN International is a trade organization founded in the 1970's that was established to coordinate the "European Article Numbering" system for identifying products, similar to the UPC managed by the UCC. MIT and other worldwide universities continue to be involved with EPCglobal as part of "Auto-ID Labs."

EPCglobal is somewhat unique in that it is an organization that is promoting de facto specifications compared to a formal standards organization. It follows standards development methodologies from the World Wide Web Consortium (W3C) but is not directly creating standards. The plan however is to merge the specifications created within the EPCglobal process to ISO for formal standards ratification.

EPCglobal has a number of specifications for RFID, namely Class 0/Class 1 UHF and Class 1/HF. The latter is equivalent to the ISO 15963 standard. A new specification known as UHF Generation 2 (commonly referred to as "Gen2") has been moved to candidate specification status and is expected to move to ISO draft standards immediately upon final ratification.

EPCglobal's UHF Gen2 is the specification that the U.S. DoD and most retailers around the world are coalescing around. Since it is becoming a de facto standard, and because so many technology providers are planning or have announced production of Gen2 products, the RF Feasibility team is favoring this standard as the key guideline for technology selection.

1.10 Resources

RFID is a hot technology topic, and there is tremendous hype, disinformation, and general noise on the web. Below are several websites with good information for reference.

- http://www.incits.org
- http://www.iso.org
- http://www.epcglobalinc.org/index.html
- http://www.aimglobal.org/
- http://www.rfidjournal.com
- http://www.rfid-handbook.de

On EPCglobal security and privacy topics see:

- http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

1.11 Summary

The following table summarizes key RFID frequencies, standards, applications and decision criteria:

Frequency Bands	Data & Speed	Read Range	Typical Usages	Strengths/Challenges	Applicable Standards
Low Frequency (LF): 125 – 134 KHz	Low read speed Small amounts of data	Very Short: inches	Access Control Animal Tagging Inventory Control Car immobilizer	▪ low tag costs ▪ small read range ▪ small data amounts ▪ low data transfer speed ▪ No singulation	ISO 11784/11785 ISO 18000/2
High Frequency (HF): 13.553 – 13.567 MHz	Medium read speed Small to Med amounts of data	Short to Med: 1 to 3 Feet	Smart Cards Item or case level tagging	▪ sufficient data amounts ▪ most standards in place ▪ less suseptible to interferance	ISO 15963 ISO 14443A ISO 14443B ISO 18000/3 EPC Class 0/1
Ultra High Frequency (UHF): 433 MHz	Good data speed Medium to large amounts of data	Long range 50 -300 Feet	Active tags Container seals Container tracking for DLA	▪ read speed and range ▪ costs ▪ potential interference with certain devices	INCITS 371 .2 ISO 18000/7
Ultra High Frequency (UHF): 900-950 MHz	High read speed Small to Med amounts of data	Medium: 2 to 10 Feet	Pallet or case level tagging SENTRI/NEXUS	▪ better vicinity read range ▪ more suseptible to interferance ▪ high data tranfer speed ▪ high tag costs	EPC Class 0/1 EPG UHF Gen 2 ISO 18000/6
Microwave Frequency: 2.45 GHz	High read speed Med amounts of data	Med to Long: 3 to 20 Feet	Container or rail car Toll collection Pallet level tagging	▪ long read range ▪ high data tranfer speed ▪ high tag costs	ISO 18000/4 INCITS 371 .1
Microwave Frequency: 5.8 GHz	Very high read speed High data rates	Long range 50 -300 Feet	Toll tags	▪ long read range ▪ high data tranfer speed ▪ high tag costs ▪ battery replacement	ISO 18000/5 (rejected)

Figure D-3 RFID System Characteristics