

RADIO FREQUENCY IDENTIFICATION (RFID)



IJIS Institute

EMERGING TECHNOLOGY WHITE PAPER

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following individuals and their sponsoring companies for their dedication and input on this document:

Fred A. Lengerich, *Information Builders* –
Primary Author

Matthew A. D'Alessandro, *Motorola* –
Committee Chair



John Crouse, *ACS Government Solutions* –
Committee Co-Chair



Iveta Topalova, *Analysts International*



Gigi Pereira, *SRA International*



This project was supported by Grant No. 2003-LD-BX-0007 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

INTRODUCTION

You are likely using Radio Frequency Identification technology (RFID) today. Maybe it is the toll road pass on your car windshield or the device you wave at the gas pump to pay. Each is an RFID device. The technology referred to as RFID is essentially a chip that automatically transmits gathered information to a detached receiving unit. RFID technology has evolved significantly in recent years. Manufacturers have been able to reduce the size, as well as lower the price of RFID “chips.”

“A form of RFID technology has been around since World War II.”

It is generally said that the roots of radio frequency identification technology can be traced back to World War II. The Germans, Japanese, Americans and British were all using radar – which had been discovered in 1935 by Scottish physicist Sir Robert Alexander Watson-Watt – to warn of approaching planes while they were still miles away. The problem was there was no way to identify which planes belonged to the enemy and which were a country’s own pilots returning from a mission.

The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back. This crude method alerted

the radar crew on the ground that these were German planes and not Allied aircraft (this is, essentially, the first passive RFID system).

Under Watson-Watt, who headed a secret project, the British developed the first active identify friend or foe (IFF) system. They put a transmitter on each British plane. When it received signals from radar stations on the ground, it began broadcasting a signal back that identified the aircraft as friendly. RFID works on this same basic concept. A signal is sent to a transponder, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system).

Since RFID technology has been around since World War II. Two main factors have resulted in the technological advancements and deployment of RFID since that time:

- The advent of computers enabling the processing of large volumes of information generated by thousands of RFID tags simultaneously
- Manufacturing techniques to lower the cost of the RFID to economical ranges.

The small, inconspicuous size of RFID chips and their ability to store, send, or receive data, provides for gathering information on any object or feature in the world.

WHAT IS RFID?

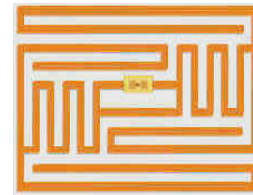
Figure 1. RFID technology common to most people (toll road device)



A basic RFID system consists of an electronic tag (the chip), a reader on the same radio frequency as the tag, and a computer with software to control the reader and manage the data received from the tag. An RFID system uses low-power radio waves to transmit information between the tag and reader. The radio power and chip capability define how far apart the reader can be from the chip, a few inches or many yards. The reader contains a transceiver (combination transmitter and receiver) and an antenna. The tag contains an antenna and a microchip. The chip has storage to contain the identifying data, an antenna, power source (on some types of active chips), and a transponder (which enables the tag to communicate with the reader). When the tag is within communication range of the reader, the readers' radio signal is picked up by the tag, causing the tag to send its data to the reader.

Once the reader has the data, that data is then transferred to computer software that can process it or start the integration of the data to other computer systems.

Figure 2. Examples of RFID chips



HOW DOES RFID WORK?

There are two types of RFID chips, or tags; *active* and *passive*.

An *active* RFID tag contains a power source (a battery) in addition to the obligatory chip technology described earlier (antenna, transmitter, and data storage). Active chips or tags are used where distance from the reader is generally 100 feet or more. The inclusion of the battery and its components makes the active tags very expensive. Currently, an active tag can be up to a 100 times more expensive than a passive tag (typical passive tag price is <\$0.50).

“There are two types of RFID chips: active and passive.”

A *passive* tag has no installed power source. The radio waves from the reader induce a small current in the tag that provides enough power to read the data on the chip and transmit the data back to the reader. Passive tags therefore have a lower cost per tag than active tags.

However, passive tags currently only have a range of a few inches or feet. Much of this is dependent on the “power” of the reader and environmental factors (e.g., are there obstructions between the reader and the tag). Most passive tags use a frequency of 13.56 MHz although no frequency has truly attained “standard” status.

There are also many variations on the basic active or passive tag architecture. Some tags can support multiple radio frequencies while some can support read-write capabilities. The tag type used depends on many factors:

- Distance between the tag and reader.
- Speed at which tags will pass the reader.
- Environmental obstructions between the tag and reader.

These factors define the requirements of the RFID system and hence the cost of implementation and on-going support.

Unlike the first RFID units used in WWII, the current RFID tags take advantage of the advent of microchip technology that can allow today’s RFID tags to contain 100’s of kilobytes of data, allowing much more than a simple serial number to be stored. Such tags make it possible for military RFID applications to store the entire medical history of a soldier on a single RFID tag.

The data storage component of a tag typically supports one of the following read-write capabilities; read-only, write-once, or full read-write.

- **Read-only tags** are loaded with data once, typically in the manufacturing process of the RFID. In addition, this type of tag enables multiple read operations.
- **Write-once-read-many (WORM)** chips enable the user to customize the chip with information. Data can be loaded with a special write unit in the field that enables an entire box of chips to be coded with the same data. These, however, are a one-time write

operation that requires a special RFID writing device.

- **Read-write tags** allow repeated write and read operations to the tag. These are the most expensive type of tags, but are also the most versatile.

The type of tag, tag specifications, environmental issues, and usage method define the type of reader to use with the

tag. Must the reader be portable, or in a fixed location? Does the reader have obstructions between itself and the tags to be read? These factors and others help define what type of reader and tag is appropriate for the application.

RFID AND INFORMATION SECURITY

Information concerns

As described, RFID technology offers benefits of reading information from a tagged object wirelessly to a reader. This architecture could lead to information security issues from rogue reading devices or from physically taking the RFID chip and decoding it. In addition, RFIDs contain information and therefore need to be protected depending on the application. Obviously, data security for tags identifying characteristics of cattle in a feedlot differs greatly as compared to tags that would be used in the correctional system to relay medical information about a prisoner.

RFID Security Solutions

The most common form of RFID data security is the encryption of data on the RFID tag which would likely provide unintelligible data even if the contents of the tag were surreptitiously read and stolen by an individual. However, the difficulty in decrypting the information is largely determined by the level of encryption used

Some of the solutions outlined in the NIST Special Publication 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems April 2007, advised that in

addition to encryption, the amount of sensitive data on the tag be limited, physical controls be put in place for the readers, and training of operators, and hardware level authentication (specific linkage between tag and reader) be used among the many different approaches for RFID data security.

Real ID Act

The Real ID Act will require some type of electronic national identification card, most likely issued through state motor-vehicle agencies as a standardized driver's license. While the act does not require that the "machine-readable" technology will be RFID, all solutions currently being considered use RFID technology. The Real ID could be an information security maelstrom and as such it bears monitoring not just from a policy standpoint but from a technology standpoint as well.

The Real ID Act of 2005 was passed into law in May 2005 under the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief. The Real ID act will directly affect state government and court systems with the implementation deadline now being moved back to December 2009.

DOMAIN APPLICATION OF TECHNOLOGY

Passports and Citizen Identification

The U.S. government is developing electronic passports equipped with RFID tags for U.S. citizens, and also the visa-waiver program. Germany issued RFID enabled e-passports in November 2006¹. In addition to other identifying information, Germany's RFID chip will store a facial image initially and add digitized fingerprints by 2007.

Tracking Records, Evidence, Materials, and Prisoners

DeKalb County Juvenile Court

The DeKalb County Juvenile Court, the second-largest juvenile court in Georgia, is piloting an RFID record-tracking system for its approximately 12,000 manual files. Each file makes multiple trips to the courtroom, in addition to circulating among staff. The system uses a passive RFID tag on each file folder and includes handheld and desktop readers. Total costs were approximately \$42,000, plus \$4,000 in annual maintenance expenses. Court officials project that the system will pay for itself in less than two years through estimated annual savings of up to \$30,000 in lost productivity because of time spent searching for files throughout the three-story courthouse.

Marin County District Attorney's Office

The Marin County District Attorney's Office in San Rafael, California implemented a new file-tracking system using two-inch-square RFID labels with adhesive backing that are applied to the inside of a file folder. The readers include

stationary tracking pads that plug into the office computer system and are capable of reading a pile of file folders as much as 12 inches thick. The battery-powered handheld scanners can be carried to offices or other locations to scan files being used there. The 40-attorney office anticipates saving approximately 2,500 person-hours of time spent searching for active and misplaced files within its 120 different work and filing areas and performing related data-entry activities.

Maricopa County Attorney's Office

The Maricopa County Attorney's Office in Phoenix, Arizona, has been piloting an RFID-based tracking, inventory, and archiving system for its records and files. With an annual volume of approximately 100,000 case files and 45,000 to 50,000 prosecuted cases, tracking files scattered among staff in a half-dozen buildings has been a significant challenge. The office estimates that 10 to 40 percent of all files were misplaced at some point in their life cycle – sometimes permanently. The new RFID system captures a complete file history as records move from file rooms and offices to other locations. From any computer on the network, staff can easily view the movement and current location of a particular file.

State Arson Investigators in Indiana

Since late 2003, state arson investigators in Indiana have been using an RFID-based evidence-tracking system on a trial basis to replace an existing barcode system. The system includes around 1,500 passive RFID tags to track materials stored in a number of buildings. Successful read rates have been 98–99% with RFID, compared with about 80% for the old barcode system.

¹"RFID Passports take off." October 26, 2006, CNET News.com
(http://news.com.com/RFID+passports+take+off/2100-7348_3-6130016.html?tag=item)

Correctional Facilities

Correctional facilities in Michigan, California, Arizona, Illinois, and Ohio already are using or piloting RFID-tracking systems. These typically use a tamper-evident wristband for inmates and a belt-mounted tag for officers. Both are equipped with RFID chips and antennas, but the system design may be passive or active. Either can detect when an inmate or officer moves through a portal

equipped with a reader and can be read with a handheld reader at any time to confirm an inmate's identity. Active systems have the added advantage of periodically (e.g., every few seconds) emitting a longer-range signal that can be picked up anywhere in the facility, thus providing nearly continuous prisoner counts in each area plus the ability to locate a particular inmate or officer at any time and record the location in a database.

HARDWARE OR SOFTWARE REQUIREMENTS

Companies that offer RFID units will also generally provide software to read and if appropriate programming services to the device. An RFID reader is another form of input device, like a paper scanner. Just as the rate of paper scans dictates the hardware "horsepower," the same is true of RFIDs. How many tags over what unit of time will be processed is needed information for sizing computing hardware, antennas, readers, and network connectivity. An area often missed is the impact of RFID data on back office systems, like a "Hot Files System" or a "Criminal History System". If these back office systems are configured to accept data at a slow rate of input, they will likely slow down—or worse—under the real-time input stream from RFID devices. The hardware and software requirements for RFID need to be evaluated through the entire data path.

STRENGTHS, WEAKNESSES & POSSIBLE RISKS

Some general considerations when looking at RFID solutions:

- Privacy almost more than cost, is a major consideration of RFID systems. At both the local and national level the courts and legislation are actively involved in addressing the privacy issues of implementing RFID. The main focus on securing RFID focuses on how a person's behavior can be tracked by an RFID enabled device. For example, if a person knows the frequency of the RFID device attached to a certain DVD, someone with an unusually strong receiver could drive down your street and know what DVDs you have. California has passed legislation that forces RFID devices to be deactivated once they leave the store. The privacy policy for personal data on RFID tags is tied to general privacy laws such as those affecting banking and health information. There is on-going work from both a policy and technology standpoint regarding how to protect RFID information. The area of privacy legislation is also a very active topic and as such both local and national legislation, should be closely monitored as privacy concerns are a major concern.
- It is important to note that RFIDs are not GPS devices. An RFID tag must be within a few hundred feet of the reading device in the case of active RFID tags, and less than 100 feet for passive RFID tags. The ability to track an individual's location outside of an RFID-enabled environment (like a prison in the above examples) is the domain of GPS devices.
- The current standard for RFID is UHF Gen 2 which has been widely adopted for readers and RFID tags. The standard however does not support encryption, in order to keep tags low cost. The standard does support a strong "kill" capability so that retail chains can "kill" the tag as it leaves the store. The standard also supports data lock so that the tag cannot be spoofed or changed without a password. EPC Global (www.epcglobalinc.org) is a good source for standards information.
- The operational environment of the RFID and the reader needs to be considered. Issues such as distance between the tag to the reader, environmental weather proofing, possible obstructions between the tag and the reader, are among the many considerations.
- While costs for RFID are dropping, in order to realize low RFID implementation costs, it is important to properly match the RFID solution with the application.
- Transferring the data from the reader to the computer device is only the beginning of using RFID technology. The volume and frequency of data being transferred into integrated applications also needs to be considered.

LINKS TO MORE RFID INFORMATION

Information

- EPC Global:
www.epcglobalinc.org/home (UPC and RFID standards)
- RFID Journal:
www.rfidjournal.com

Analyst firms

- Current Analysis
www.currentanalysis.com (provides good coverage on this technology and vendors in this space)
- Gartner:
www.gartner.com

Security

- NIST Special Publication 800-98
Guidelines for Securing Radio
Frequency Identification (RFID)
Systems April 2007,
<http://csrc.nist.gov/publications/PubsByLR.html>

Vendors

- Alanco Technologies:
www.alanco.com
- Filetrail:
www.filetrail.com
- Infolinx:
www.infolinx.com
- Intermec :
www.intermec.com
- Symbol/Motorola:
www.symbol.com