

Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology

*As approved by the IEEE-USA
Board of Directors (17 Feb. 2006)*

RFID systems present a unique technical and policy challenge because they allow data to be collected inconspicuously, remotely, and by unknown, unauthorized, or unintended entities. RFID technology, deployments, and uses continue to be developing and evolving. IEEE-USA therefore believes that legislation and regulations relating to RFID systems and the data derived from these systems must address the following concerns:

1) **Openness and transparency:** RFID systems should be built on the concept of openness and transparency. Companies and governments using or specifying the use of RFID technology should be required to include clear notices regarding what data are collected and how it will be used for its applications and implementations. Accountability should rest with those who claim ownership of the data at each step in the system. Privacy of personal data is of paramount concern. However, given the need for openness in the system, requirements that implement security and privacy must be balanced against the limits of technology.

2) **Layered protection:** Appropriate layered levels of protection and security must be required as standard policy with RFID systems and the data collected from those systems. Security measures must take into account the entire system including the hardware, the software, associated systems and parts as well as the environment and location(s) in which the RFID system and tags might be used.

The security provisions for data acquired using RFID technology must adequately address the fact that data can be collected at a distance, inconspicuously and even unintentionally. Because data in an RFID network has little human intervention and is acquired immediately during a transaction and can even be acquired following a transaction, the data aggregation and use for purposes other than those intended are possibilities that must also be addressed.

This statement was developed by the Committee on Communications and Information Policy of the IEEE-United States of America (IEEE-USA) and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA is an organizational unit of The Institute of Electrical and Electronics Engineers, Inc., created in 1973 to advance the public good and promote the careers and public policy interests of the more than 220,000 electrical, electronics, computer and software engineers who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE or its other organizational units.

BACKGROUND

It is the goal of this IEEE-USA position statement to provide a basis for sound policy-making on the subject of radio frequency identification device (RFID) technology. IEEE-USA has also prepared an extensive supporting bibliography and the informational whitepaper, [The State of Radio Frequency Identification \(RFID\) Implementation and its Policy Implications](#), which provide a basic introduction to RFID technology and survey the current state of its implementation. Both of these documents are available upon request to IEEE-USA's Committee on Communications and Information Policy.

RFID is a generic term for technologies that use radio waves to automatically identify people or objects. Unlike bar codes, no clear line of sight is required to obtain an accurate RFID read. RFID technology has the potential to be disruptive as its use becomes ubiquitous globally.

The world's biggest retailer (Wal-Mart) and the U.S. Department of Defense (DoD) intend to fully incorporate RFID technologies into their supply chains and logistics. These commitments demonstrate the escalating importance of RFID in global commerce.

HOW IT WORKS

The basic RFID system comprises a transponder, a reader and an antenna. Data is stored in a transponder device called a tag. There are currently three forms of tags: passive, semi-passive, and active. Tags can be read-only or read/write.

The transponder holds bits of data, which are either reflected or sent back to the reader, depending on whether the tag is passive or active. With passive and semi-active tags, a radio frequency signal is transmitted from the reader to a transponder that passes within range of the reader's antenna and triggers RF emissions from the tag. Active tags periodically send out their data to be retrieved by any readers within range of the transmission. Transponder data includes information such as the transaction record type, the unique transponder ID number, the transaction status code, and the error detection code. Customer data can be included as well, for example with the new biometric passport required by all countries in the Visa Waiver Program. With the U.S. e-passport, the bearer's digitized photo and other data are replicated in an RFID chip implanted in the back cover. Similar information is expected to be included in the proposed document to cross the Canadian and Mexican borders.

Read Range: The read range, or the physical area within which the reader can recognize the tag, is dependent on the 1) tag-reader frequency, 2) antenna design for both tag and reader, 3) tag energy efficiency, and 4) amount of illumination field strength (transmitter power) generated by the reader. Antenna-to-tag orientation issues are impacted by the antenna polarization method used (circular vs. linear).

Source of Tag Power: Tags can be passive, active or semi-passive. Active tags rather than reflecting the signal back to the reader have a transmitter to send back information and thus have a greater read range. The battery, used to power the transmissions in active tags, adds significantly to the cost of the tag and limits its life to that of the battery. The U.S. military uses active tags to track containers arriving in ports. For real-time tracking available globally, DoD plans to couple the active transponders with the Global Positioning System. Semi-passive tags use the battery to power their circuitry, but not the broadcast signal.

Coding: Data stored in RFID tags depends on the application and existing standards. Although many current RFID applications are based on proprietary systems, industries supporting open RFID systems with open standards, are expected to proliferate soon.

Types of Tags: RFID is a broad-based technology with many applications that impact many industries. The type of tag used in an application determines what can and cannot be done with a particular RFID system. The following chart outlines the prevailing RFID tag types and parameters of each:

Type frequency	Frequency range	Read range	Memory	Comments
Microwave	2.4 GHz to 2.4835 GHz	2-meter max	Less than 1 kbit	Silicon technology is in its infancy for this frequency. Not expected to change any time soon.
Ultra High Frequency	300 MHz to 3 GHz (typically 866 to 960 MHz; 915 in the U.S.)	As much as 6-meter or more, depending on regulatory requirements (4 watt EIRP (equivalent isotropically radiated power)) in the US; 2 watt ERP (effective radiated power)) in Europe)	1 kbit for now, larger expected in near future	Sends faster and further than lower frequencies, with good anti-collision capability. Not yet available globally, since spectrum use varies with country. (Europe uses 868 MHz for UHF; the U.S. uses 915 MHz. Japan prohibits the use of UHF spectrum for RFID, but may open the 960 MHz area.)
High Frequency /ISO 16593 (vicinity smart cards)	3 to 30 MHz (usually 13.56 MHz)	1.5-meter at best for high-end readers	256-bit to 8x32-bit blocks, additional data memory up to 4kByte available today	The inductive nature of coupling between tag and reader (near-field coupling) prohibits larger read ranges, even for increased field strengths. Antennas for tags usually consist of printed, flexible coils, making the technology ideal for smart cards.
Low Frequency	30 kHz to 300 kHz	1-meter at best	64 bits to 1360 bits; larger possible but customers prefer 13.56 MHz	Globally available frequency. Low frequency allows tags to be read through watery substances (the only technology that allows this). Low frequency does not allow for fast data speeds though, which is the reason that (as a rule of thumb) no anti-collision handling is offered for tags using this frequency. This is also the

Type frequency	Frequency range	Read range	Memory	Comments
				only technology that allows for small ferrite-based coils as tag antennas, which allows for a small cylindrical form factor for the tag, an advantage in many RFID applications

APPLICATIONS

With a supporting infrastructure in place, a product using RFID technology can traverse the entire shipping and distribution network easily and seamlessly. As RFID becomes implemented, efficiencies and savings will result from eliminating paperwork and from avoiding human errors that occur, for example, in manually re-keying data. To exploit the efficiencies that RFID can provide globally, however, many obstacles must be overcome, including those posed by spectrum allocation policies that vary by continent and sometimes by country.

Since RFID technology was first used in World War II to identify aircraft, a broad variety of uses have been developed. Identifying livestock, shipping containers, and pets; managing vehicle fleets; increasing highway throughput; speeding transactions at the point of sale; gaining entrance to buildings and aiding in marathon race logistics are just a few practical applications. Even new passports issued by countries in the visa waiver program, must contain an RFID chip that contains data that uniquely identifies the bearer of the passport. Because information contained in the tag remains in digital format, manual re-entry is avoided and paperwork can be reduced or eliminated. The supply chain can be collapsed if the same data is moved and integrated digitally from one location and purpose to the next.

The latest surge in RFID deployment is in the retail sector, where tags are expected to be placed on every item to be sold, much like bar codes are today, yet with considerable more capacity. The ability to track a specific item, not just the case or pallet it was packaged with, introduces a whole new level of control over products globally. Simply being able to convey information digitally throughout the supply and distribution of goods and services can make a significant increase in the efficiency of the operations of the global supply chain. For example, the highly regulated pharmaceutical industry is expected to fully embrace the use of RFID when standards are approved.

Improving Processes

Ultimately, commercial and government interests are concerned with tracking and monitoring assets through each stage of the manufacturing and distribution process. Guaranteeing genuine parts manufactured in China, assembled in Japan, shipped through Europe and distributed in the U.S. adds value to the finished product and is a foil to counterfeit and theft throughout the distribution channels.

Monitoring products once in use can also reduce maintenance costs and overhead. In addition to DoD's interests, the Federal Aviation Administration recently approved the use of RFID in tagging components onboard airplanes. That approval includes cargo, baggage and equipment, such as aircraft parts and galley carts.

ISSUES

Issues in RFID implementation concern operations, reliability, testing, certification, security, privacy, interoperability, data sharing and database use, and consumer confusion.

Acceptance of any disruptive technology -- and RFID is one -- takes time. For example, bar code technology, so common and accepted today, had a long gestation period. Invented in the early 1950s, the first bar code reader was installed in 1974, roughly 20 years later. As with any disruptive technology, RFID end users, policymakers, lawmakers and the media require education and experience with RFID before full acceptance.