



IEEE-USA EBOOKS PRESENTS

# RFID

THE STATE OF RADIO  
FREQUENCY IDENTIFICATION (RFID)  
IMPLEMENTATION AND POLICY IMPLICATIONS

21 NOVEMBER 2005

This eBook was developed from a white paper by the Committee on Communications and Information Policy of The Institute of Electrical and Electronics Engineers-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. A roster of committee members is provided in the Appendix F. Special appreciation goes to CCIP member Emily Sopensky, who prepared the committee draft and served as principal committee editor. Whitepapers are designed to provide balanced information on public policy issues in technology-related areas and/or affecting the interests of technical professionals. This document does not constitute a formal position statement of the IEEE-USA and its contents do not necessarily reflect the views of IEEE-USA, IEEE or other IEEE organizational units. IEEE-USA has issued this whitepaper to enhance knowledge and promote discussion of the issues addressed. IEEE-USA is an organizational unit of the IEEE, created in 1973 to advance the public good and promote the careers and public policy interests of the more than 220,000 technical professionals who are U.S. members of the IEEE.

Published by IEEE-USA.

Edited by Georgia C. Stelluto, IEEE-USA Publishing Manager

Cover Design and Layout by Greg Hill, IEEE-USA Electronic Communications Manager

Copyright © 2005 by the IEEE. All rights reserved for original content. No rights claimed over public domain source material used in this whitepaper. Permission to copy granted for non-commercial, informational purposes with attribution to IEEE-USA. Copying of this material for commercial purposes is not permitted without prior written approval from the IEEE. For copying, reprint or republication information, write to the IEEE Manager of Intellectual Property, IEEE Customer Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331

# TABLE OF CONTENTS

- Introduction** ..... 3
- Background** ..... 3
  - More Companies Are Investing in RFID ..... 4
  - DOD Counts on RFID to Streamline Processes..... 5
  - Costs ..... 6
- How Does RFID Work?** ..... 6
  - Read Range..... 6
  - Source of Tag Power ..... 6
  - Coding..... 7
- Issues** ..... 7
  - Operational ..... 7
  - Testing..... 8
  - Reliability ..... 8
  - Certification..... 8
  - Security ..... 8
  - Privacy..... 9
  - Interoperability..... 9
  - Electromagnetic Compatibility ..... 10
  - Data Sharing, Database Use and Management..... 10
  - Consumer Confusion..... 11
- Conclusions**..... 12
- IEEE Xplore Papers on RFID** ..... 12
- Appendix A - Industry Interest** ..... 15
- Appendix B - RFID in Use** ..... 16
- Appendix C - Standards** ..... 19
  - ISO Standards ..... 19
  - EPCglobal Standards ..... 19
  - Proprietary Standards..... 21
  - Government..... 21
- Appendix D - Typical Tag Types** ..... 24
- Appendix E - RFID Frequencies per Country**..... 25
- Appendix F – 2005 IEEE-USA CCIP Membership Roster** ..... 26

## INTRODUCTION

The purpose of this IEEE-USA eBook is to provide a basic introduction to RFID technology and to survey the current state of its implementation. The book includes a basic introduction to the technology, and an extensive bibliography for the reader's further reference. Please email IEEE-USA (d.rudolph@ieee.org) to obtain the bibliography.

## BACKGROUND

The latest indication that RFID is becoming the enabling technology of the 21st Century is the course that the world's biggest retailer and logistics juggernauts have chosen. Both Wal-Mart and the U.S. Department of Defense (DOD) intend on fully incorporating RFID into their supply chain and logistics. More to the point, Wal-Mart will require its top 100 suppliers to use RFID tagging of each item in addition to each pallet. Trials started in Dallas in January 2005.

As the hype and expectations about RFID escalate, so do concerns. Consumer privacy is at the top of the list. Other concerns include the gap between the vision and the current state of RFID build-out. Functionally, exploiting the efficiencies that RFID can provide means overcoming spectrum allocation policies that vary by continent and sometimes by country. "For most businesses, RFID is too expensive, doesn't work well enough (the accuracy of some readers is well below 90 percent), suffers from a lack of standards, and requires a resource-heavy overhaul of supply chain, logistics and manufacturing processes and systems before a worthwhile payoff can be toted up." (Rothfeder, *PC Magazine*, 1 August 2004)

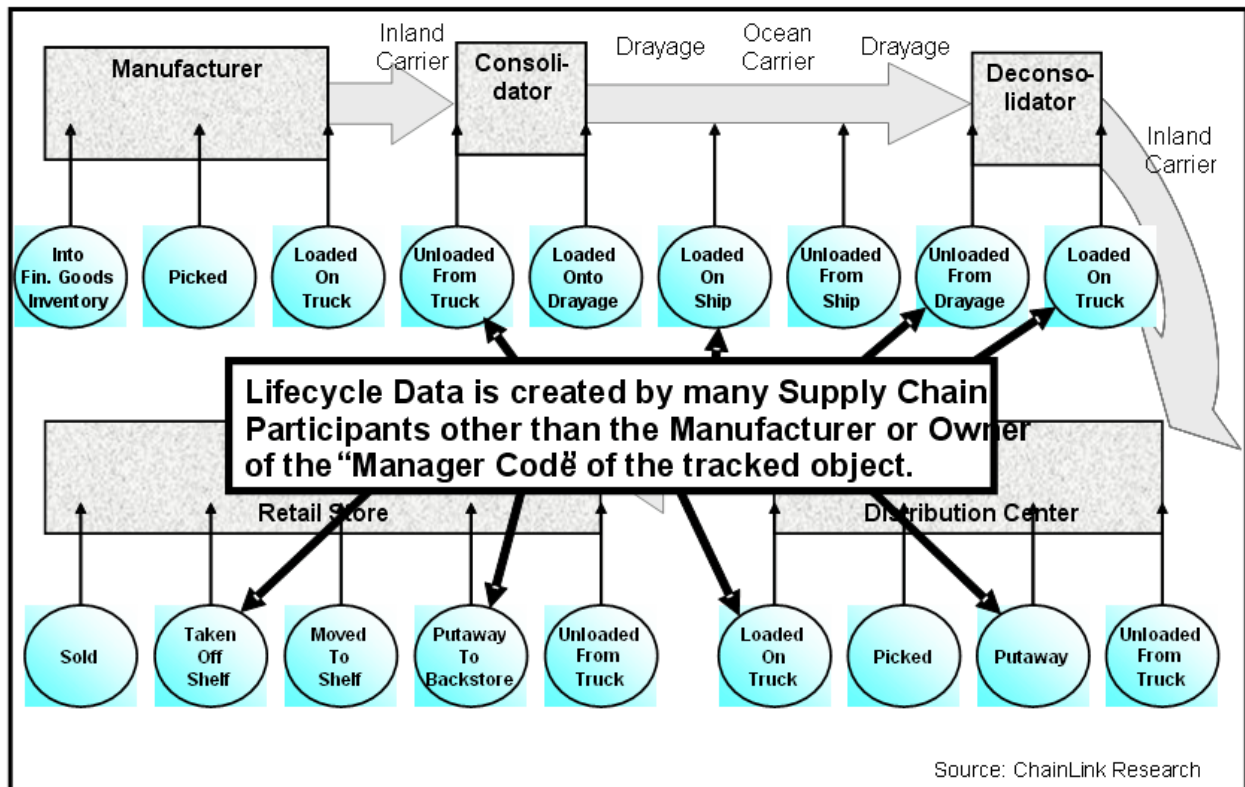
Since it was first introduced in World War II to identify aircraft, RFID technology has benefited a broad variety of uses: identifying livestock and pets; shipping containers; managing vehicle fleets; increasing highway throughput; speeding up transactions at the point of sale; gaining entrance to buildings; and aiding in marathon logistics are just a few practical applications. Because information contained in the tag remains in digital format, manual re-entry is avoided and paperwork can be reduced or eliminated. (See **How Does RFID Work?** for more information.) 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 retailers expect tags to be placed on every item to be sold, much like bar codes are now. In fact, the electronic product code (EPC) identifies RFID tags for retail and supply chain management. With RFID, we have the capacity to provide a unique identifier to every product manufactured. The ability to track a specific item, and not just the case or pallet it was packaged with, introduces a whole new level of control over products globally.

Consulting firm AT&Kearney conducted a study of RFID in retail operations, and concluded that 32 cents on every sales dollar could be saved if the retailer fully utilized RFID in its operations. (Rothfeder, *PC Magazine*, 1 August 2004) The study found that "most of the benefits of EPC/RFID adoption are realized in the areas of improved supply chain integrity, improved deduction and claims accuracy, and greater warehouse and inventory efficiency." (AT&Kearney, 3 November 2004) Most savings are projected from eliminating the cost of human errors made in manually re-keying data and processing paperwork. Nevertheless, a savings of one-third is extraordinary, even in retail operations where 200 percent markups

are normal.

However, the point is that RFID technology has the ability to be disruptive. The ability to convey information digitally throughout the supply and distribution, during the entire life of goods and services, will cause a huge shift in the global supply chain operations. That a product can traverse the entire shipping and distribution network easily and seamlessly does not imply that the means to achieve it will be easy. The supply chain lifecycle chart below illustrates the many points in the supply chain where data must be exchanged among participants who geographically may span the globe. But we are just at the beginning of using the technology globally and ubiquitously.



Lifecycle Data Created by Many Players Across the Chain. Source: Chainlink Research, Inc. [www.chainlinkresearch.com](http://www.chainlinkresearch.com)

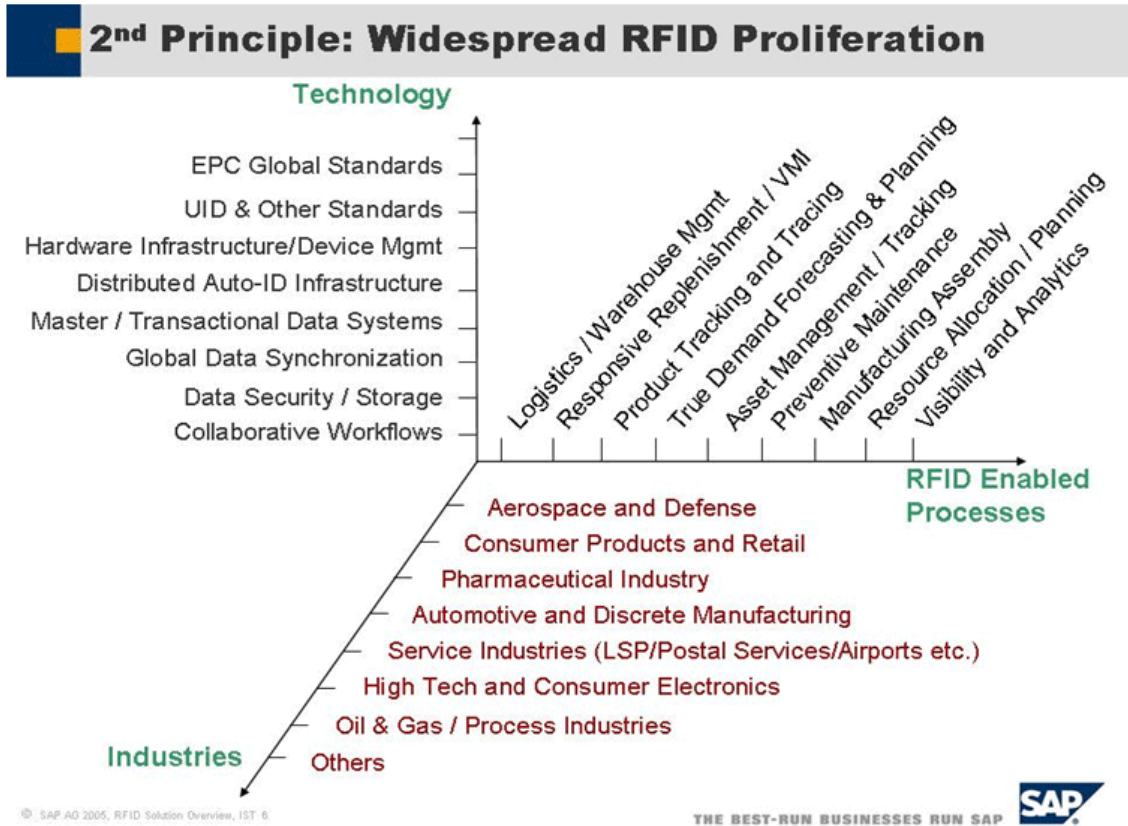
Another major industry, the highly regulated pharmaceuticals, is expected to fully embrace using RFID when all necessary standards are approved. Some manufacturing companies, like Hewlett-Packard, are already using packaging with embedded RFID tags. Tag manufacturers like Texas Instruments have reduced tag sizes and costs to make their uses much more attractive at all levels of the supply chain.

### More Companies Are Investing in RFID

At a 6 April 2005 workshop held at the U.S. Department of Commerce in Washington, D.C., one of the

presenters, Nicholas Tsougas, director of RFID Programs at SRA International (an information technology consulting firm) said: “RFID is an enabler; it cannot fix fundamentally bad processes.” Major U.S. players in tag, reader and systems development are familiar names, such as tag and reader manufacturers Texas Instruments, IBM, Hewlett-Packard and Sun Microsystems. Middleware vendors, such as SAP, Oracle and Microsoft, are investing heavily to provide RFID solutions.

Here, SAP charts the technology, industries and processes involved in RFID:



Source: U.S. Department of Commerce RFID Workshop, 6 April 2005 [www.technology.gov], with the permission of SAP.

**DOD Counts on RFID to Streamline Processes**

RFID has transcended defense logistics and its supply chain. Last year, when DOD Under Secretary for Acquisition, Technology and Logistics Michael Wynne appeared before the U.S. Senate Armed Services Readiness and Management Subcommittee, he spoke of his imperative to implement RFID to optimize the supply chain. “Tags applied to the cases, pallets and freight containers shipped to and within the DOD will enable hands-free processing of material transactions, allowing us to re-apportion critical manpower resources to war-fighting functions...and enable us to better manage and track these critical assets.” See **DOD Tagging Policy** for more information.

Being able to track assets through the distribution process is the initial goal for both DOD and Wal-Mart. Ultimately, tracking and monitoring assets through each stage of the manufacturing process is driving the giants' interest in RFID. Guaranteeing genuine parts manufactured in China, assembled in Japan, shipped through Europe, and distributed in the United States adds value to the finished product, and is a counterbalance to counterfeit and theft throughout the distribution channels.

Monitoring products once in use can also reduce maintenance costs and overhead. Beyond DOD, the Federal Aviation Administration (the agency that oversees civilian aviation) recently approved using RFID in tagging components onboard airplanes. That includes cargo, baggage and equipment, such as aircraft parts and galley carts. (For more information on RFID applications, see **Appendix B: RFID in Use.**)

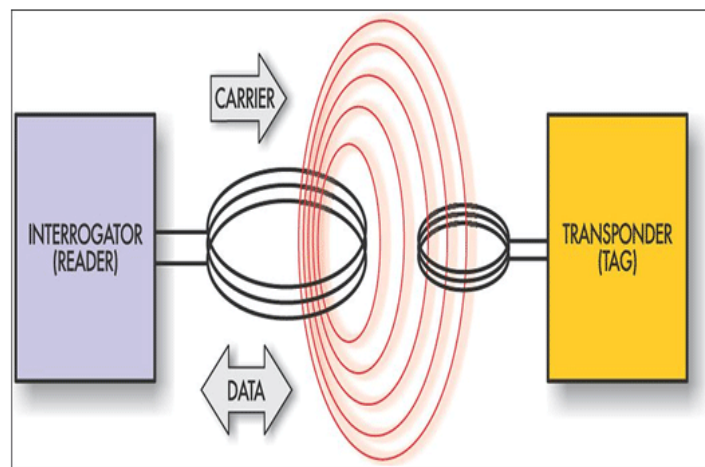
### Costs

While the costs of tags are declining and standards are emerging that will bring overall costs under control, implementing RFID — from chips to system integration — is still an added cost yet to be absorbed into the supply chain. An excellent chart of costs by component is shown in “Solving the RFID Cost-Benefit Equation,” by Shahram Moradpour in *RFID Product News*, published by Lyons Media, Inc., January/February 2005. [Source: [www.rfidproductnews.com/issues/2005.01/feature/cost.php](http://www.rfidproductnews.com/issues/2005.01/feature/cost.php)]

## HOW DOES RFID WORK?

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 read.

The basic RFID system comprises a transponder, a reader and an antenna. Data is stored in a transponder device called a tag. Current tags, depending on application, can hold up to 2 kbits of data. Tags can be read-only or read/write.



Source: [www.RFID2VIN.com](http://www.RFID2VIN.com)

A radio frequency signal is transmitted from the reader to a transponder that passes within range of the reader's antenna. The signal triggers RF emissions from the tag. The transponder holds bits of data, which is either reflected or sent back to the reader, depending on whether the tag is passive or active. Transponder data includes information such as the transaction record type, the unique transponder ID number, the reader ID number, the transaction status code, and the error detection code. Customer data can be specified as well.

### Read Range

The read range, or the physical area within which the reader can recognize the tag, is dependent on tag-reader frequency; antenna design for both tag and reader; tag energy efficiency; and 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). Antenna sizes are mostly a function of the operating frequency used.

### Source of Tag Power

Tags can be passive, active or semi-passive. Active tags, which have a longer read range, have a transmitter to send back information, rather than reflecting the signal back to the reader. Used to power the transmissions in active tags, the battery adds significantly to the tag cost, and it limits the tag life to the battery life. 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 the circuitry, but not the broadcast signal.

### Coding

Data stored in RFID tags depends on the application and existing standards. For example, the design of EPCglobal-supported code is divided into four sections (header, manager number, object class and serial number). Although many current RFID applications are based on proprietary systems, industries supporting open RFID systems with open standards may soon proliferate

## ISSUES

That many issues of concern still exist about RFID technology indicates that the technology is still in flux. By recognizing these issues now, we can avoid some of the problems that plague maturing technologies that were once disruptive, for example, the Internet.

**“A key thing to observe here [about the Internet] is that in places where we didn’t plan well in advance, we’re paying the price now with regard to viruses, for instance, and general hacking attacks, denial of service, Trojan horses. We didn’t think in advance about these security problems, and they’ve become extremely problematic and costly now.”**

**(Juels, RSA)**

Operational, testing, reliability, security, privacy, interoperability, data sharing, database use and consumer confusion are the issues selected for this white paper.

### Operational

Some current operational issues are as follows:

- **Mitigating Out of Sequence Tagged Unit Reads** — Ideally, tagged items should be read in their physical sequence (i.e., on a conveyor belt). With RF, you can actually read an item early or late in its “physical order.” With RFID auto-toll tags, this issue can be serious when the wrong person is billed for using the tollway. In logistical processes, such as a conveyor belt holding baggage, decisions are made automatically based on the tags read. If your bag gets read too early or too late, the mechanical switch sends the wrong bag to the wrong tray. Result: Bag is lost.
- **Conveyance Speeds vs. Tag Reads** — Obviously, the faster the tag can be read, the better. But the constraints of the equipment may limit the ability to activate, read and collect the data.
- **Reading Cases on a Pallet** — Reading individual cases within a pallet is not currently a requirement of most RFID systems, but it is a topic of frequent discussion. A logistical system depends on patterns to recognize and “read” a pallet automatically. If the tag is not placed rigorously in the same place on the pallet, the system will not be able to read it. Another issue is orientation of the tag, so that it can be read correctly. Only when pallet-level tagging is regimented will case-level and item-level tagging be seriously considered. Once item-level tagging is incorporated, the question of how to avoid conflicts with pallet-level tags must be dealt with.
- **Determining Required Number of Antennae per Portal Type** — The read zone of each antenna can “bleed” to another read zone, if the layout is not carefully calibrated.
- **Applications** — For example, the global airline industry must sort through RF interference posed by the metal bins that luggage is commonly transported in; must be able to distinguish between RFID tagging on airline parts and luggage; and must be able to agree on global procedures. (Barnaby J. Feder, *New York Times*, 7 March 2005)

## Testing

Test performance specialists observe that a need exists for globally recognized performance test specifications. Based on demand, standards-making bodies in conjunction with manufacturers will most likely develop these specifications.

## Reliability

For global supply chain operations, the RFID network must be always on, reliable and secure, yet accessible for benefits to be achievable. The network must have the ability to automatically react to failures and recover to benefit from a global supply chain. Read rates must be 99.99 percent or higher. Many newly introduced applications do not yet reach those levels of reliability.

## Certification

To validate accepted testing and reliability standards, a vendor-neutral body should be established to educate and certify RFID equipment, systems and technicians.

## Security

The security framework must address authentication, data protection and access control. Ensuring security is a stepped process, meaning that effective authentication, data protection and control techniques cannot

be embodied in one process.

Because data in an RFID network has little human intervention, the first step in establishing trust in the RFID process is determining how two entities trying to communicate with each other are who they say they are. Once the authentication process is complete, data is then moved to another system for authorization.

The RFID network is defined by the size of the antenna, the strength of power in the tag and reader, and the distance between the tag and reader. For a point-of-sale transaction, the tag remains with the product. At this point, the security issue is: Should the tag be deactivated to ensure privacy of the purchaser post-sale? There is no aftermarket value for the tag. But if the tag remains active, restocking is easier in case of returns. Active tags can alert the consumer to date-sensitive products as expiration dates approach. At-will deactivation programs could be similar to current loyalty card programs.

A recent study conducted by John Hopkins University and the security company RSA (JHU-RSA), “Security Analysis of a Cryptographically-Enabled RFID Device” (28 January 2005 Draft) [Source: [www.rfidanalysis.org/DSTbreak.pdf](http://www.rfidanalysis.org/DSTbreak.pdf)] illustrates the problems and hype associated with the security of RFID data and use. As an example, the JHU-RSA team “cracked” the digital transponder encrypted challenge-response protocols of the popular Speedpass network that uses low frequency tags at the gas pump to accelerate the transaction of buying gas. As the researchers themselves acknowledged, the security was successfully challenged at only one level of a full Speedpass transaction. The typical protections that credit card companies use to flush out fraudulent activities were *not* the targets of the study, and no attempt was made to crack these levels of protection.

While the ease with which the researchers accomplished this breach does raise concerns, personal and financial data are secured on separate networks. The unique ID must still traverse several computers for data lookups and authentication before traveling to off-site processing by an enterprise system, where it interacts with financial data that must be verified before the process at the pump can continue.

Regardless, the real-time nature of RFID data creates concerns for privacy and security experts. Eliminating paperwork and removing the human element may speed goods through the supply chain, but it also threatens traditional laws, regulations and procedures established to maintain the flow of goods across borders.

For competitive reasons, the last thing companies want to do is share their information with competitors. Companies sharing data in the RFID network must be confident the network and data are secure. To prevent radio snooping, a combination of authentication, encryption, and authorization is advisable. In addition to current systems for data exchange, authentication within the RFID system — for example, between the reader and tag — should occur before data is transmitted. Other measures to preserve privacy and counterfeiting can include encryption and the ability to deactivate a tag at the point of sale. But that makes the tag unavailable for after-market use. (Hargraves & Shafer, FTC, 2004)

Using a non-public RFID tag on a product for purchase without the consumer’s knowledge is another concern. However, in a profit-oriented economy, the additional cost of such tagging will probably negate the value of placing such a tag, except on high-value items. In addition, the smaller the tag, the closer the reader must be, which, for practical purposes, prevents successful stealth-reads.

## Privacy

Privacy for consumers is like security for companies. To have data in the RFID network, one must be confident that the network and data are secure. In the privacy context, it is important to clearly (and perhaps often) communicate to users the distinctions among active, passive and semi-passive tags, along with their relevant range, cost and capability limitations.

For retailers, disabling product tags at checkout is still under discussion. In addition, the real privacy issue with RFID is not the limited data stored in the tags, but the security of the databases to which the tag data are linked — a problem that exists today with minimal RFID implementation.

One argument against “killing” a tag is that with RFID turned on, refunds and restocking returned items is quicker and more efficient than with current systems. How the tag is deactivated, when, and at whose pleasure are still questions yet to be addressed satisfactorily.

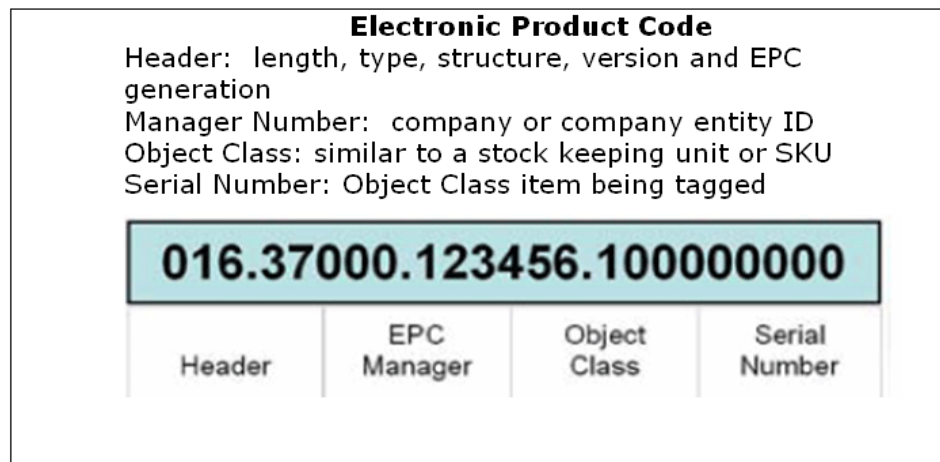
Regardless, deactivating the “always-on” RFID tag must always be an option.

## Interoperability

For the RFID network to provide the benefits that retailers like Wal-Mart determined for their return on investment strategy, RFID systems must be built for interoperability. Generally, this functionality refers to systems built by competing vendors. Just as important, many trade groups as well as vendors favor systems built on open standards, which aids in building interoperable systems. Many UHF RFID tags are being built to meet standards developed both by ISO and EPCglobal. See **Appendix C - Standards**.

Labeling standards are less developed. For privacy advocates, acceptable practices, let alone laws and regulations to enforce such practices, are yet to be determined for letting the general public know about the presence of an RFID tag in the box that was purchased.

The unique identifier is the basis of the electronic product code (EPC) system and is a constant in all EPC specifications. Wal-Mart and DOD are proposing that eventually every item inventoried will be tagged by an RF identifier. Wal-Mart is requiring its 100 largest suppliers to comply or discontinue as a Wal-



Source: U.S. Department of Commerce and Electronic Product Code: [[www.EPCglobalus.org/Network/Electronic%20Product%20Code.html](http://www.EPCglobalus.org/Network/Electronic%20Product%20Code.html)]

Mart vendor. As the world's largest retailer, this dictum has significant global impact. Digital numeric identification — manufacturers' IDs as well as electronic product object codes — composes part of the data contained in an EPCglobal tag.

Another issue of interoperability is that the advantages of RFID assume global acceptance. RFID is spectrum-dependent, but countries vary in their use of spectrum. (See **Appendix E: RFID Frequencies per Country**.) Some RFID applications, for example, must manufacture systems using different frequencies, depending on the country where the system will be installed.

### **Electromagnetic Compatibility**

Emissions from RFID readers may potentially interfere with medical devices.

### **Data Sharing, Database Use and Management**

The new threats from RFID arise from the proliferation of data, the sharing of the data, and from the possibility of snooping via radio. One suggestion is that developing and disseminating a policy framework for different RFID applications based on best practices and standards would help address legitimate concerns and enable deployment. (CSIS RFID Working Group draft paper, Jan 2005)

“We can swim in the data, but knowing it may not be sufficient in the long run,” says Morris Cohen, co-director of the Fishman-Davidson Center for Service and Operations Management. “Figuring out what to do with [the data] should be worth even more.” (Cachon, K@W (*Knowledge at Wharton*) newsletter, 9-22 March 2005.)

For example, the EPC does not describe the item or its owner, but provides a unique lookup identifier to databases that hold the information. Each datum itself in its integral parts is not a threat. It is when associations are built with accessed databases that sensitive relationships are revealed or discovered, resulting in damage — actual or potential.

To be able to decipher codes that protect and prevent access to RFID databases is daunting, but the difficulties posed are insufficient to feel confident that security is good. With codes being standardized, it's only a matter of time before the program code to decipher tag-data easily is available on the Internet.

RFID can create mountains of information. Where will it be stored? How will it be managed? What are archival procedures, if any? Data structures are usually optimized for the industry generating and using them. How will security and access be applied to the databases? With business leaning towards an easily programmable RFID network, how can new behaviors be introduced in a secure and controlled manner without compromising security? How will this network scale globally and across the supply chain?

If using tags is going to be as common as bar codes, policies notifying consumers may also require giving the consumers options to permanently disable or discard the tags without incurring cost or penalty. On the other hand, consumers may be enticed to leave the tags enabled if the tags are integrated into their own personal network. For example, the “smart” refrigerator will be stocked with items that have their expiration date that can be “read” by the refrigerator or a handheld reader.

### **Consumer Confusion**

Currently, each industry that uses RFID has mounted its own educational campaign to inform its customers

about the technology. But RFID is a generic technology with many applications. Each application has its own benefits and limitations. One issue is how much is too much information for consumers. For example, the average consumer could care less about the technology behind the automobile industry's use of read-only transponders that provide encrypted remote keyless entry. But they do care that the remote entry works all the time and is secure.

Acceptance of any disruptive technology — and RFID is one — takes time. Bar code technology, so common and accepted today, also had a long gestation period. Invented in the early 1950s, the first reader was installed in 1974 (Kahn, *Wall Street Journal*, 8 July 2005), roughly 20 years later. Today, bar coding allows many of us to scan and bag our own groceries to avoid long lines at the supermarket. Few small independent retail operators can survive without point-of-sale scanning equipment.

The real downside to consumer confusion is that it extends easily to policy-makers and law-makers, and is echoed in the press — confounding any inherent misunderstandings about the technology.

Examples:

- “U.S. Department of Homeland Security officials have hotly denied reports by some other publications that the agency’s upcoming ID cards will use radio-frequency identification. Instead, the DHS will deploy another type of RF technology known as ISO/IEC 14443, which is soon to be required for all federal employee ID cards — and which carries a far shorter coverage range.” (Emigh, *eWeek*, March 17 2005) [Source: [www.thegadgetfiles.com/archives/20050307/165/homeland-security-gets-rfid-cards](http://www.thegadgetfiles.com/archives/20050307/165/homeland-security-gets-rfid-cards)]
- “The distinction is part of an effort by the Department of Homeland Security and one of its RFID suppliers, Philips Semiconductors, to brand RFID tags in identification documents as “proximity chips,” “contact-less chips” or “contact-less integrated circuits” — anything but “RFID.” (Beard, *Wired*, 29 March 2005)
- “Bar Codes Would Mark the Spot, Fido or Fluffy,” *The Washington Post*, Monday, 28 February 2005; Page B5. “Early next month, the Montgomery County Council will consider a law requiring any animal that lands in the county shelter to receive the implant...”

## CONCLUSIONS

**Evolving technology.** Despite the relative age of RFID technology, any policies or technical developments must recognize that both RFID technology and its industry are currently evolving. Standards, too, are emerging, but none exist globally.

**Openness and transparency.** General agreement exists that the RFID network should be built on openness and transparency. Because RFID allows data to be collected inconspicuously, consumer organizations advocate clear notice of purpose, limiting data collection, and acceptance of accountability by business and consumers alike. Personal data privacy is of paramount concern. Security and privacy must be balanced against the limits of technology, given the need for openness in the system.

**Layered protection.** Concurrent, layered protection, such as multi-layered authentication, must be required as standard policy with digitized data, regardless of source. Internet security measures conjoin hardware and software solutions used concurrently. We suggest the same strategy be employed with RFID applications. As mentioned earlier, RFID security should involve a stepped process, instead of it being embodied in one, comprehensive process.

For example, the passive, low-frequency RFID tag used for Exxon-Mobil Speedpass transactions uses a challenge response digital signature that is encrypted. When bolstered with authentication, authorization and identification handshaking protocols in other linked systems and databases, the layers of security add up to much better protection.

Hash-based encryption can be coupled with technology techniques such as basic access control (BAC) for protocol handshakes, the RFID network being defined by the size of the antenna, the strength of power in the tag and reader, and the distance between the tag and reader.

For point-of-sale transaction, deactivating tags should be the standard procedure, unless clear explanations, incentives and waivers are provided to the informed customer.

**Certification.** A vendor-neutral, policy-free means of certifying RFID equipment, systems and specialists should be encouraged — especially because RFID technology is remotely readable, invisible and captures data in real time. Trust that the data is being captured and transmitted safely and securely is a valuable commodity. Certifying that the RFID product is what it says it is, and the specialist is trained to work with RFID in acceptable ways, will be important to RFID technology proliferating.

## IEEE XPLORE PAPERS ON RFID

- Alfonsi, B.J., “Privacy debate centers on radio frequency identification,” *IEEE Security & Privacy Magazine*, Volume 2, Issue 2 (Mar-Apr 2004) p. 12

*Abstract:* The emergence of radio frequency identification (RFID) has brought with it a plethora of privacy concerns and experts are questioning whether the hoopla surrounding RFID is justified. Using RFID should trigger the same privacy concerns as other commonly used technologies such as credit cards, cell phones, and the Internet. RFID’s potential to revolutionize the retail industry by maximizing suppliers’ ability to control inventory and reduce theft is widely recognized. In fact, some technology forecasters predict that RFID tags will eventually replace bar codes on almost all product packaging. The privacy debate centers around RFID tags themselves, which function like tiny radios, wirelessly transmitting information to network receivers. If RFID tags were to remain active even after consumers complete their purchases and exit stores, their wireless technology would let the stores track consumers’ movement and behavior; or so goes the argument.

- Juels, Ari; “Yoking-Proofs for RFID Tags;” Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (Orlando, Florida) March 14 - 17 2004, p. 138-

*Abstract:* We propose the concept of a yoking-proof, namely a proof that a pair of RFID tags has

been scanned simultaneously. Our particular aim is to permit tags to generate a proof that is verifiable off-line by a trusted entity, even when readers are potentially mistrusted. We suggest that such proofs are a useful tool for maintaining integrity in supply chains, particularly as RFID data will commonly flow across multiple, loosely affiliated organizations.

- Michael, K.; McCathie, L.; “The Pros and Cons of RFID in Supply Chain Management,” *Mobile Business, 2005. ICMB 2005. International Conference Proceedings* (11-13 July 2005) pp. 623 – 629

*Abstract:* This paper presents the pros and cons of using Radio-Frequency Identification (RFID) in Supply Chain Management (SCM). While RFID has a greater number of benefits than its predecessor, the bar code, it currently comes at a price that many businesses still consider prohibitive. On the one hand, RFID is advantageous because it does not require line-of-sight scanning, it acts to reduce labor levels, enhances visibility, and improves inventory management. On the other hand, RFID is presently a costly solution lacking standardization. It has a small number of suppliers developing end-to-end solutions, suffers from some adverse deployment issues, and is clouded by privacy concerns. Irrespective of these factors, the ultimate aim of RFID in SCM is to see the establishment of item-level tracking, which should act to revolutionize SCM practices, introducing another level of efficiencies never before seen.

- Philipose, Matthai; Smith, Joshua R.; Jiang, Bing; Mamishev, Alexander; Roy, Sumit; Sundara-Rajan, Kishore; “Battery-free Wireless Identification and Sensing ,” *IEEE Pervasive Computing*, Jan 2005; pp37-45.

*Abstract:* Dense, long-term, wide-area deployments of tiny wireless sensors can potentially enable many novel and useful monitoring-based applications. A fundamental challenge in realizing this potential is to supply each sensor with enough power for its sensing and communication needs.

- Want, R.; “Enabling ubiquitous sensing with RFID,” *IEEE Computer*, Volume 37, Issue 4 (April 2004). pp. 84 – 86

*Abstract:* Radio frequency identification has attracted considerable press attention in recent years, and for good reasons: RFID not only replaces traditional barcode technology, it also provides additional features and removes boundaries that limited the use of previous alternatives. Printed bar codes are typically read by a laser-based optical scanner that requires a direct line-of-sight to detect and extract information. With RFID, however, a scanner can read the encoded information even when the tag is concealed for either aesthetic or security reasons. In the future, RFID tags will likely be used as environmental sensors on an unprecedented scale.

- Weinstein, R; “RFID: a technical overview and its application to the enterprise,” *IT Professional, IEEE*, Vol. 7, Issue 3 (May-June 2005), pp. 27-33

*Abstract:* Radio frequency identification (RFID) offers tantalizing benefits for supply chain management, inventory control and many other applications. Only recently, however, has the convergence of lower cost and increased capabilities made businesses take a hard look at what RFID can do for

them. This article offers an RFID tutorial that answers the following questions: What is RFID, and how does it work?; What are some applications of RFID?; What are some challenges and problems in RFID technology and implementation?; and How have some organizations implemented RFID?

- Xingxin Gao; Zhe Xiang; Hao Wang; Jun Shen; Jian Huang; Song Song; “An approach to security and privacy of RFID system for supply chain,” *IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, 2004. pp. 164-169.

*Abstract:* Radio frequency identification (RFID) is expected to become pervasive and ubiquitous, as it can be embedded into everyday items as smart labels. A typical scenario of exploiting RFID is supply chain. The RFID based supply chain management yields convenience, efficiency and productivity gains. However, RFID systems create new risks to security and privacy. We briefly present the current solutions to RFID security and privacy. A new approach is then proposed, which exploits randomized read access control, and thus prevents hostile tracking and man-in-the-middle attack. In addition, compared with current schemes that achieve the similar security level, the proposed approach dramatically decreases the computation load. Another benefit is that it is suitable for RFID systems with a large number of tags.

- Yang, Geng; Jarvenpaa, Sirkka L.; “Trust and Radio Frequency Identification (RFID) Adoption within an Alliance,” *Proceedings of the 38th Hawaii International Conference on System Sciences – 2005*; March 2005.

*Abstract:* Dense, long-term, wide-area deployments of tiny wireless sensors can potentially enable many novel and useful monitoring-based applications. A fundamental challenge in realizing this potential is to supply each sensor with enough power for its sensing and communication needs.

## APPENDIX A — INDUSTRY INTEREST

Comparing the attendance of the annual RFID World Conference in 2004 and 2005 reflects the rising importance of RFID in the financial, legal, food and textile industries. Corporate management is increasing its interest, too. The 2005 conference, held in Dallas, Texas, attracted more than 3,000 attendees and 130 exhibitors. RFID World is one of the two or three major conferences on RFID in the United States. The long-time venue for *RFID Journal Live!* — another major annual U.S. conference — is Chicago.

Attendance has increased significantly from those providing professional services (legal, finance, accounting) to larger companies and the technically curious. This trend indicates that RFID-tagged products are moving out of the lab to those wanting to implement RFID in a large-scale environment. More corporate management is also attending.

### RFID World 2004 and 2005

Attendance by Industry & Corporate Role at a major RFID Conference

Industries represented at RFID World	2004 (%)	2005 (%)
Automotive & Transportation Equipment	4	1
Banking/Finance, Legal, Accounting	9	26
Chemical, Petroleum, Rubber Products	2	3
Communications, Postal Services	2	2
Computer & Office Equipment	13	n/a
Educational	N/A	3
Electrical & Electronic Machinery	6	2
Engineering, Architectural, R&D	5	3
Food & Food Products	N/A	23
Government (SERVICES)	4	1
Healthcare	3	3
Management Consulting Services	N/A	1
Misc mfg	2	n/a
Pharmaceuticals	3	n/a
Retail Consumer Goods	13	n/a
Textile Mill Products	N/A	12
Transportation, Freight	N/A	2
Utility	N/A	4
Warehousing & Distribution	13	4
All other	19	n/a
Source: <i>RFID World 2005</i> . [ <a href="http://www.Shorecliffcommunications.com">http://www.Shorecliffcommunications.com</a> ]		

Role within Organization	2004	2005
Engineering & Technical	3	13
Corporate Management	27	46
IT/IS Management	22	20
Operations Management	18	17
Other	n/a	4
<b>Source: <i>RFID World 2005</i>. [<a href="http://www.Shorecliffcommunications.com">http://www.Shorecliffcommunications.com</a>]</b>		

Size of Company	2004	2005
Less than 49	77	31
50 to 249	6	16
250 to 499	10	8
500 to 999	3	9
Above 1000	33	37
<b>Source: <i>RFID World 2005</i>. [<a href="http://www.Shorecliffcommunications.com">http://www.Shorecliffcommunications.com</a>]</b>		

## APPENDIX B — RFID IN USE

As a technology with boundless uses, here are some applications that currently garner management's interest:

### **Retail**

The cost savings and benefits of RFID in retail are associated with streamlining business processes, shipping faster, managing inventory better, and reducing labor costs. Wal-Mart's expressed dedication to embracing the best that RFID can provide may shake up the doldrums for this retail giant. U.K.'s Tesco Corp. is tagging cases of nonfood items at its distribution centers for use in its stores. Target Corp. is requiring some suppliers to apply RFID tags to pallets and cases. By 2007, the Food and Drug Administration expects all pharmaceutical producers, wholesalers and retailers will thwart counterfeiting by placing RFID tags on pallets, cases and unit items.

### **Pharmaceutical / Healthcare**

By 2007, the Food and Drug Administration expects pharmaceutical producers, wholesalers and retailers will thwart counterfeiting by placing RFID tags on pallets, cases and unit items. A report issued in February 2004, *Combating Counterfeit Drugs*, states that FDA anticipates reliable RFID to "make the copying of medications either extremely difficult or unprofitable." See *Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs: Guidance for FDA Staff and Industry* [Source: [www.fda.gov/oc/initiatives/counterfeit/rfid\\_cpg.html](http://www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html)]

Reducing hospital errors and healthcare costs may drive industry to use RFID tagging for patient and asset tracking.

### **Airline baggage**

Strapped with high oil prices and a glut of independent airlines, the airline industry is looking at any way possible to decrease operational costs. The cost of misdirected or lost baggage can cost as much as \$200 per bag on average, some industry analysts' estimate. Yet the cost-effectiveness of RFID is still marginal at best. Eventually, domestic airlines may be forced to adopt RFID luggage tracking for security reasons. Quickly finding a bag, even after it has been loaded on a plane, is an advantage that RFID tagging offers over the current bar code systems, and one of the reasons that the Transportation Security Administration, is investing more than \$50 million in a new baggage management system.

### **Airplane parts**

Both Boeing and Airbus are planning to use passive RFID tags to track and maintain airplane parts on airplanes currently in use. The U.S. Federal Aviation Administration recently decided to authorize using passive RFID in this fashion, as long as the tags are not interrogated while the plane is in use. See "FAA to Publish Passive RFID Policy," (Roberti, *RFID Journal*, 30 June 2005) [Source: [www.rfidjournal.com/article/articleview/1695/1/1/](http://www.rfidjournal.com/article/articleview/1695/1/1/)] for a list of other restrictions.

### **Animal tagging**

According to *The Washington Post*, (Trejos, *The Washington Post*, 28 Feb 2005), a veterinarian “inserts a microchip-sized ID into the neck of a pet dog named Basia,” a practice that other veterinarians are beginning to use. Livestock, now pets, were the first animals to receive implantable tags that will identify the breed, owner and feeding regimen of the animals. Implants in humans have been suggested. In fact, one manufacturer offers an implantable, low frequency tag. But concerns about privacy will inhibit widespread use of these in humans for at least the near future.

### **Passports**

The federal government chose RFID technology to embed digital biometric data in passports. The capacity of the RFID chip for larger image files was one reason this technology was chosen over 2-D bar code already in use. The first generation chips contain all data, including the passport holder’s picture, readable on the passport data page. Data on the chip verifies the data page information, nullifying any illicit attempts to tamper with the passport. The U.S. State Department expects that future generations of the passport chip will contain fingerprint and iris images as well.

“Early interoperability tests have indicated reliability and privacy problems with regard to reading the chips.”(Zetter, *Wired*, 4 May 2005). While none of the information on the chip is currently encrypted to avoid the risk of sharing decryption methodology (Singel, *Wired*, 21 Oct. 2004), The State Department is considering adding encryption in response to security and privacy concerns.

The International Civil Aeronautics Organization (ICAO), the *U.S. Patriot Act*, and the technology itself set forth the boundaries and requirements of the biometric passport. For example, ICAO requires the chip to contain a country-specific digital signature, so that when within range of the reader, this signature verifies that the government created the chip.

### **Auto tires**

The U.S. Department of Transportation now requires tracking tires from tire to automobile manufacturers. Information about the plant, tire size and any unique attributes are spelled out in ANSI MH108.4 material handling specifications. More than 67 million new tires were shipped in 2000. In 2003, Michelin North America Inc. implanted RFID tags on some tires to keep track of their performance and wear. Dealers and service centers can better track inventory and determine tire performance.

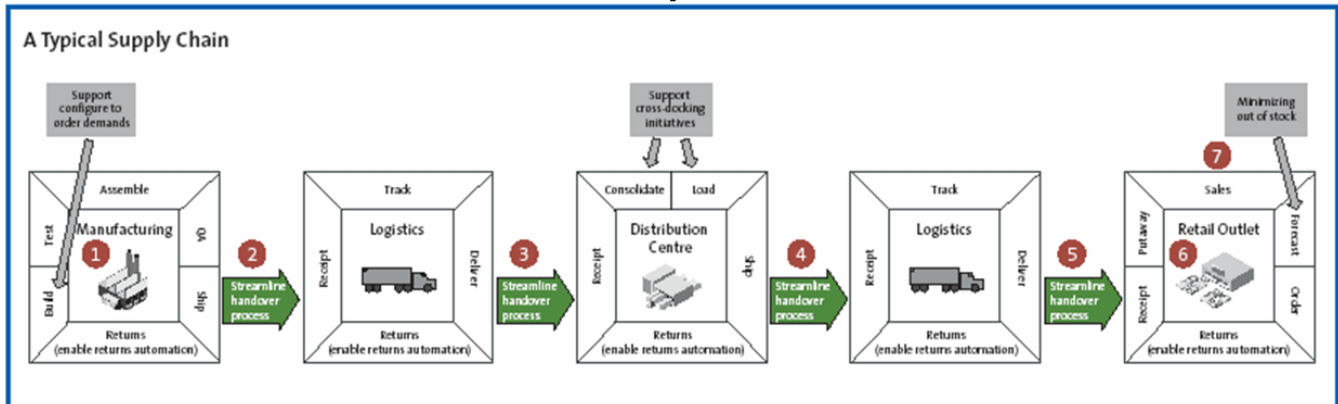
### **Libraries**

The thought of being able to check out books without a librarian’s help, of the library completing a comprehensive inventory in record time, and easing the burdens of repetitive tasks of checking in a book have made RFID applications in the library very attractive, and a fast-growing RFID application. To maintain user privacy for this item-level application, such organizations as the Electronic Frontier Foundation advocate practices like private authentication. See Libraries under Standards in this paper.

### **Supply chain**

Theft, counterfeiting, terrorism, transportation and product diversion are all major concerns in delivering

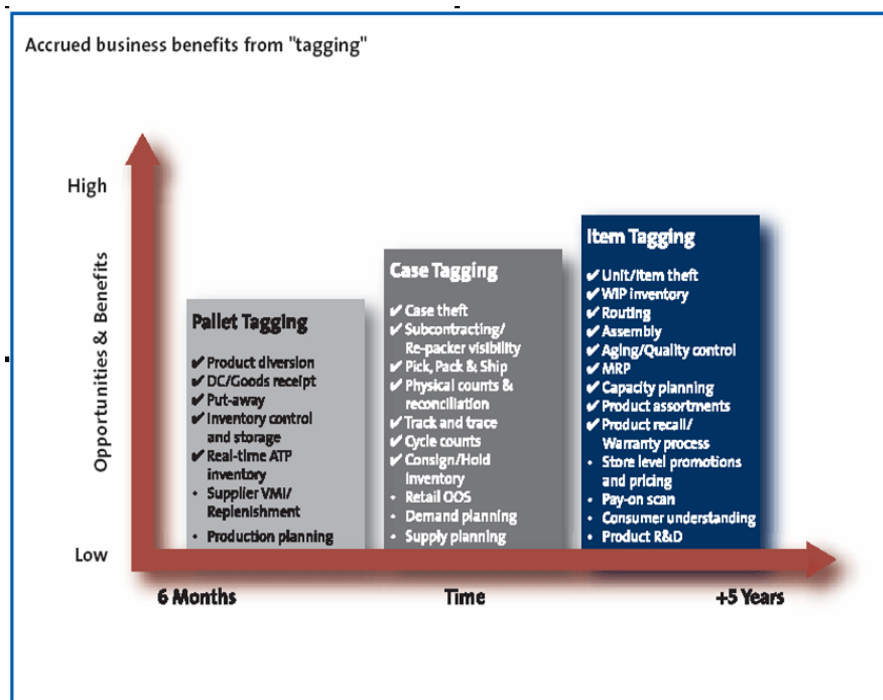
goods. The costs associated with them inevitably add to the cost of goods sold.



Source: Hewlett-Packard, 2004

Any organization within the supply chain encounters:

- 1) Incorrect goods shipped
- 2) Late delivery of goods
- 3) Difficulty locating goods
- 4) Difficulty reconciling physical goods to customer orders/returns
- 5) Misplaced/stolen goods
- 6) Inaccurate forecast of goods



Source: Hewlett-Packard, 2004

## APPENDIX C — STANDARDS

Especially for the intended uses in the supply chain and logistics, RFID must be based on global, non-proprietary, royalty-free standards. Suppliers are working on interoperable protocols now dependent on radio frequency, distance, power and reading speed. Standards required fall into four categories:

- Air interface protocol (communication between tag and reader)
- Data content (organization and data format)
- Conformance (testing)
- Applications
- Packaging

### ISO Standards

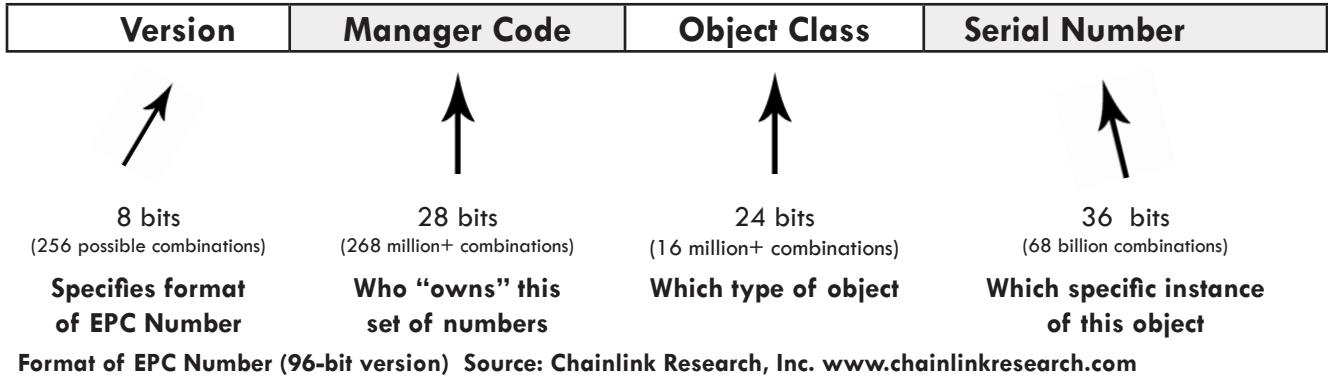
ISO Standards for RFID Tagging	
11784	Data structure for use in animal identification
11785	Air interface protocol
10536	Proximity cards
14443	Contact-less smart cards
15693	Vicinity cards
18000	Series for UHF
18000-1	Generic parameters for air interfaces for globally accepted frequencies
18000-2	Air interface for 135 KHz
18000-3	Air interface for 13.56 MHz
18000-4	Air interface for 2.45 GHz
18000-5	Air interface for 5.8 GHz
18000-6	Air interface for 860 MHz to 930 MHz
18000-7	Air interface at 433.92 MHz
18047	Conformance of RFID tags and readers
18046	Performance of RFID tags and readers

Currently, RFID tagging uses the International Organization for Standardization (ISO) standards.

### EPCglobal Standards

Standards developed for the electronic product code (EPC) evolved from those proposed by the Auto-ID Center. To track products through the supply chain, the Auto-ID Center was established in 1999. Initially rejecting ISO standards as too complex, the Center established electronic product codes to be used much like the bar code is now. Because the EPC had to be readable in an environment requiring a longer

read range, the standards were developed for ultra-high frequency, along with network architecture to support web-based tracking. The Uniform Code Council (UCC), which oversees bar coding standards, licensed the EPC technology and formed EPCglobal, a joint venture with EAN International, formerly



AutoID, Inc. EPC codes are similar in structure to those standardized under EAN. Class 0 and Class 1 standards are now in use.

Generally, spectrum for lower frequency tags is available globally. However, UHF spectrum is not universally available. Although EPCglobal Generation 2 standards may offer forward compatibility, ISO and EPC standards currently are incompatible. Systems based on Gen 2 standards are due out later this year from many manufacturers. Many of them also worked on the ISO UHF standard, in the ISO 18000 series. Gen 2 tagging is faster, more secure, and feature rich. Gen 2 has a longer range than Gen 1, Class 0, and 1, and it avoids interference.

Class	Target	Tag Type P=Passive A=Active
0	Read-only, factory programmed	P
1	Read-only, field programmable	P
2	Read-write, 65 KB	P
3	Read-write 65 KB with battery for longer read range	S-P
4		A
5		A + GPS tracking

**Auto-ID Center RFID Tag Standards (Original)**

**International Civil Aeronautics Organization**

Draft standards for biometric passports were released December 2004, relying on ISO 14443. See: [www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1\\_1.pdf](http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf)

ISO/IEC, ECMA International, ETSI, and several national standardization bodies are working for the adoption of global standards for RFID.

**Data Structure**

For RFID to be as pervasive as the business community projects, a global standard for handling data must be accepted and used universally. Users and businesses should have clear intentions about who controls what data in the supply chain. For example, consumers should be able to control the use of data and identity information. No one business should have all the data used throughout the supply chain. Control over data and personal privacy govern RFID’s acceptance. Information practices differ, depending on region and culture, but the elements of importance are as follows:

- Notice. Open and transparent information collection.
- Declaring intent. Collection of personal data relevant to the purposes for which it is collected.
- Limited use. Use is only for the intended purpose.
- Accurate. Collected data is accurate, complete and timely.
- Protected. Personal data is protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification, or disclosure.
- Access. Individuals can view all information collected about them.
- Accountability. Compliance to these elements is implementable.

**IEEE**

- 802.11
- 802.15.4. Not yet ratified, the standard for wireless personal networking is the basis for the Zigbee, high-level protocols for low-power, digital radios. Membership in the Zigbee Alliance is required for commercial use. Meter reading is one such application.

**Proprietary Standards**

- Zigbee [Source: [www.mywiseowl.com/articles/ZigBee](http://www.mywiseowl.com/articles/ZigBee)]

**Libraries**

RFID Tagging Standards for Libraries		
Tag Type	Example Library	Example Vendors
Checkpoint WORM	Santa Clara City	Checkpoint
Checkpoint writeable	None	Checkpoint
TAGSYS C220-FOLIO	U. Delaware	VTLS, TechLogic
ISO 15693/18000-3 MODE 1	National U. Singapore	3M, Bibliotheca, Libramation

<b>RFID Tagging Standards for Libraries</b>		
<b>Tag Type</b>	<b>Example Library</b>	<b>Example Vendors</b>
ISO 18000-3 MODE 2	Not yet available	Not yet available
EPC Class 1 13.56MHz	Not for library	WalMart
EPC Class 0 915MHz	Not for library	WalMart
EPC Class 1 915MHz	Not for library	WalMart
<b>Source: ETF</b>		

### **Government**

U.S. Government RFID applications are summarized in the following table compiled by the U.S. Department of Commerce.

<b>U.S. Government RFID Applications?</b>	
<b>Agency</b>	<b>Application</b>
Department of Defense	Logistics support and material tracking
Department of Health and Human Services	Drug authentication, chip implants
General Services Administration	Asset management and transportation
Department of Transportation	Freight and mass transport
Department of Homeland Security	Immigration, border control and customs (US-VISIT), search and rescue, and disaster response
Department of Veterans Administration	Patient and supply chain tracking
Department of the Treasury	Records management
U.S. Postal Service	Mail security and tracking
National Aeronautics and Space Administration	Hazardous materials management
Department of State	E-Passports
Department of the Interior	Access cards
Department of Agriculture	Animal tracking for disease control
<b>Source: Radio Frequency Identification: Opportunities and Challenges in Implementation, U.S. Dept of Commerce, April 2005 [<a href="http://www.technology.gov/reports/2005/RFID_April.pdf">www.technology.gov/reports/2005/RFID_April.pdf</a>]</b>	

**Department of Defense (DOD) RFID Tagging Policy**

The following is a high level view of DOD’s tagging policy. By January 2007, EPCglobal tag data construct will comply with the Department of Defense’s Commercial and Government Entity (CAGE) code, and the DOD’s Activity Address Code (DODAAC) — used by suppliers to identify shipments.

<b>DOD RFID Tagging Policy</b>		
Level	Target	Tag Type P=Passive A=Active
0	Item	P
1	Packaging	P
2	Transport Unit (carton, box)	P
3	Unit Load (pallet)	P
4	Container (freight)	A
5	Movement Vehicle (truck, train, airplane, ship)	A + GPS tracking

**Federal Communications Commission**

In the United States, regulating RFID falls largely to the FCC, since it regulates allowable frequencies, power output, emissions and other performance characteristics (FCC Title 47, Part 15). For example, the 2.4 GHz and 902-928 MHz frequency range is identified for industrial-scientific-medical and short-range devices. Because the FCC oversees the combination of frequency and allowable power levels, the functional range, such as the power output of a reader, is also under FCC’s purview.

“RFID is regulated under Part 15 of the FCC’s rules for low-power devices. Since Part 15 equipment has a relatively low probability of causing harmful interference to other wireless operations, a user may operate it without a license. Although RFID devices are unlicensed, the FCC’s rules require that (with limited exceptions), they must be authorized by the FCC as meeting its radio frequency (RF) emissions limitations, power restrictions and other requirements before they may be operated or marketed.” (Quirk, *RFID Journal*, 11 April 2005)

**Federal Trade Commission**

The FTC has a vested interest since the technology and its devices facilitate many of the activities that involve consumers. In its June 2004 Radio Frequency Identification Workshop, the FTC was the first government agency to begin public dialog about RFID. [See: [www.ftc.gov/bcp/workshops/rfid/index.htm](http://www.ftc.gov/bcp/workshops/rfid/index.htm)]

**Department of Health and Human Services/Federal Drug Administration (DHHS/FDA)**

The DHHS/FDA regulates the pharmaceutical industry, which is seen to benefit from RFID, especially as a defense against counterfeit drugs. FDA released guidance in its November 2004, *Division of Compliance Policy*. Injectable devices — for both animals and humans — are also under study, as well as adhesive tags for humans.

To date, the FDA has issued no more than a few reports and guidelines. However, it is relying on stakeholders, such as pharmaceutical companies, to use RFID technology to help eliminate counterfeiting. This government agency will have to be a principle player in determining how and what labeling will apply to incorporate RFID tagging. To date, only unenforceable guidelines have been issued.

As with wireless devices, issues about electromagnetic compatibility of RFID tags remain to be identified and resolved. For example, the stability of susceptible drugs exposed to electromagnetic radiation associated with RFID and interference with other devices. Devices possibly susceptible to picking up signal harmonics include neuro-stimulators and pacemakers.

### **Department of Commerce/National Institute of Standards and Technology**

In addition to the general role that the DOC has in overseeing U.S. commercial interests globally, it's the home for NIST. The agency's mission is to "develop and promote measurement, and technology to enhance productivity, facilitate trade, and improve the quality of life." DOC recently hosted an RFID workshop on RFID that coincided with its publication of a six-month study on RFID.

### **U.S. State Department**

The State Department plans partial issue of passports with RFID tags beginning in late 2005 as part of its goal to prevent passport fraud, with full implementation by October 2006. To date, privacy and security advocates have assailed the use of RFID in passports. Framed by requirements of the ICAO and the *U.S. Patriot Act*, and in conjunction with the Department of Homeland Security, the State Department is required to complete roll out of biometric passports by FY 2008. In the meantime, it is addressing all issues raised by citizens, interest groups and regulatory bodies.

## APPENDIX D — TYPICAL TAG TYPES

Type frequency	Frequency range	Read range	Memory	Comments
Microwave	2.45 GHz	2 meters 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 meters or more, depending on regulatory requirements (4 watt EIRP in the US; 2 watt ERP 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 960MHz area.)
High Frequency /ISO 16593 (vicinity smart cards)	3 to 30 MHz (usually 13.56 MHz)	1.5 meters at best for high-end readers	256 bit to 8x32 bit blocks, 4kByte additional data memory available today	Inductive nature of coupling between tag and reader (near-field coupling) prohibits larger read ranges, even for increased field strengths. Antennas for tags usually consists of printed, flexible coils that makes 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 instead	Globally available frequency. Low frequency allows tags to be read through watery substances, the only technology that allows for this capability. Low frequency does not allow for fast dataspeeds though, which is the reason that (as a rule of thumb) no anti-collision handling is offered for tags using this frequency. This technology is also the only one that allows for small ferrite-based coils as tag antennas, which allow for a small cylindrical form factor for the tag — an advantage in many RFID applications.

## APPENDIX E — RFID FREQUENCIES PER COUNTRY

<b>Table 4: RFID Operational Frequencies in Countries</b>	
<b>Frequency</b>	<b>Regions/Countries</b>
125-134 kHz	United States, Canada, Japan and Europe
13.56 MHz	United States, Canada, Japan and Europe
433.05-434.79 MHz	In most of Europe, United States (active tags at certain locations must be registered with the FCC), and under consideration in Japan
865-868 MHz	Europe
866-869 and 923-925 MHz	South Korea
902-928 MHz	United States
952-954 MHz	Japan (for passive tags starting in 2005)
2400-2500 and 5.725-5.875 GHz	United States, Canada, Japan and Europe
<b>Source: Radio Frequency Identification: Opportunities and Challenges in Implementation, US Dept of Commerce, April, 2005. [www.technology.gov/reports/2005/RFID_April.pdf]</b>	

## APPENDIX F — 2005 IEEE-USA CCIP MEMBERSHIP ROSTER

### Officers:

Robert S. Powers, Chair  
Larry A. Blosser, Vice Chair

### Delegate/IEEE Society Representatives to CCIP:

Robert L. Baldwin, *Region 6*  
H. Stephen Berger, *Electromagnetic Compatibility Society*  
Richard P. Biby, *Broadcast Technology Society*  
Jean Camp, *Social Implications of Technology Society*  
Michael Cardinale, *Aerospace & Electronic Systems Society*  
Jim Carlo, *Standards Association*  
Jack Cole, *Computer Society*  
Sajjad H. Durrani, *Aerospace & Electronic Systems Society*  
Weibo Gong, *Control Systems Society*  
Thomas H. Grim, *Engineering Management Society*  
Lawrence Hamerman, *Region 6*  
John Healy, *Reliability Society*  
Ferdo Ivanek, *Microwave Theory & Techniques Society*  
Clark E. Johnson, Jr., *Magnetics Society*  
Ralph Justus, *Consumer Electronics Society*  
Stanley A. Klein, *Intellectual Property Committee*  
David B. Kunkee, *Geoscience & Remote Sensing Society*  
Derong Liu, *Computational Intelligence Society*  
Luke R. Maki, *Professional Communications Society*  
Jack A. Marin, *Systems, Man & Cybernetics Society*  
Ann Miller, *Reliability Society*  
Seong K. Mun, *Engineering in Medicine & Biology Society*  
Raouf Naguib, *Engineering in Medicine & Biology Society*  
John E. Newbury, *Power Engineering Society*  
Howard Pace, Jr., *Region 6*  
Stephen D. Patek, *Systems, Man & Cybernetics Society*  
Thomas P. Pearsall, *Electron Devices Society*  
Eric J. Schimmel, *Vehicular Technology Society*  
Emily Sopensky, *Intelligent Transportation Systems Society*  
Steven Weiss, *Antennas & Propagation Society*  
Andrew Yang, *Laser & Electro Optics Society*  
Amir Zaghloul, *Antennas & Propagation Society*

### At-Large Members:

William Horne  
George Mattathil  
Alan K. McAdams  
John M. Richardson  
Paul L. Rinaldo  
Carl R. Stevenson

### IEEE-USA Staff:

Deborah Rudolph





1828 L Street, NW, Suite 1202  
Washington, D.C. 20036  
+1 202 785 0017  
<http://www.ieeeusa.org>

P.O.C.: Deborah Rudolph  
E-mail: [d.rudolph@ieee.org](mailto:d.rudolph@ieee.org)