Center of Cyber Logistics 網際物流研究中心

The Business Integration of RFID Technologies for Hong Kong

Relevant Bibliography

May 1, 2005

1 Introduction

We have searched among trade magazines and academic publications to gain an idea of previous and current works on RFID-related business issues and concerns. We provide some annotation whenever we could. We will continue updating this bibliography each half year as research into RFID-Driven business chains continues.

Bibliography

1. Ahn, H J., "An agent-based dynamic information network for supply chain management," BT Technology Journal (22) 2, Apr 2004
2. AMCOR Australia and Hewlett-Parkard, RFID in the supply chain, a balanced view, business briefing paper, Hewlett-Parkard Development Company L.P. 2004
3. Anderson, A., "The Relationship Between XACML And P3P Privacy Policies," Sun Microsystems, 2004

   In this paper, the following key points were made:
   - P3P is used to express policies that human user can understand. XACML expresses the same policies in terms of computer access control mechanisms.
   - P3P expresses policies at a generalized high level in generic user and data category terms. XACML expresses the policies in terms of specific data resource identities or system-assigned resource descriptors.
   - P3P expresses only privacy policies while XACML expresses policies for any type of access to resources, in addition to just privacy policies. P3P and XACML are complementary to each other and consistent with each other.

4. Anderson, A., "An Introduction To The Web Services Policy Language (WSPL)," 5th IEEE International Workshop on Policies for Distributed Systems and Networks, June 2004 2

   This paper states the characteristics and capabilities of WSPL, for example:
   a. WSPL supports the merging of compatible policies and
   b. WSPL is a strict subset of XACML (didn't study the article in detail)

5. Ashley, P., Powers, C., and Schunter, M., "From Privacy Promises To Privacy Management," Proceedings of the 2002 workshop on New security paradigms, ACM, 2002, 43 - 50

   P3P promises are not backed up by privacy technology that enforces the promises throughout the enterprise. Using the "sticky policy paradigm", the authors proposed an approach to enforce privacy promises enterprise-wide. The structure of the solution is
   - to define an enterprise privacy policy,
   - deploy the policy to the IT systems that contain privacy sensitive information,
   - record consent of end users to advertise privacy policy when they submit privacy sensitive data,
   - enforce the privacy policy and create an audit trail of access to privacy sensitive information,
   - generate both enterprise wide and individualized reports showing accesses to privacy sensitive information and their conformance to the governing privacy policy.

6. ATKearney, "Connect The Dots," A.T. Kearney and Kurt Salmon Associates, Feb 2004

This is a report on how industries see GDS (global data synchronization) and EPC/RFID. Interviews were made with 100 executives from more than 80 organizations, Regarding GDS, many respondents said that

a. GDS is the right path forward,
b. major benefits will only be realized with broad trading partner participation,
c. less than 1% of global sales involve registered and synchronized products.

Regarding EPC, the findings are:

- EPC code should be adopted as the global standard for electronic product identification,
- maximizing the benefits of EPC will require the strong foundation of GDS and in the next three years, pallet and case level applications will widespread

7. Auto-ID Center, "860MHz - 930MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1," 14 Nov 2002

This is Auto-ID Center's specification on Class 1 tags. It states that Class 1 is a reader-talk first system. All tags will not backscatter (respond) until a command from the reader is received. The communication channel is half-duplex.

8. Auto-ID Center, "Draft Protocol Specification For a 900MHz Class 0 Radio Frequency Identification Tag," 23 Feb 2003

This specification describes the reader-to-tag, tag-to-reader communication mechanisms in detail, including the kill command implementation. Class 0 tags are read only tags.

9. Avoine, G., Occhslin, P., "RFID Traceability: A Multilayer Problem," Financial Cryptography -- FC'05, 2005

Two major privacy concerns on RFID are
1. the ability to covertly collect information about people (information leakage),
2. to trace people (traceability).

Current solutions to privacy issues are limited to the application layer. Instead, the authors demonstrated that privacy issues can not be solved without looking into all the three layers of RFID, i.e., the physical layer, the communication layer and the application layer all together. To address the traceability issues, one can forbid the reader to get tag data. Three techniques suggested are

- Kill the tag,
- prevent the tag from hearing,
- prevent the reader from understanding.

The authors suggested that protocols in classical adversarial models do not ensure trace-resistant in an RFID-enable environment. This is because each layer of the RFID tag model can reveal traceable information. To ensure the system is trace-resistant, all layers have to be considered. Here below are some of the points to solve the traceability problem at each layer:

- Application layer: It's about the design of identification protocol. Research works were performed extensively on the application layer already. The general approach is to alter the information from tag to reader at each identification process. Information sent by a tag needs to be indistinguishable from a random number as seen by an adversary and be used for only once. A case study was given.

- Communication layer: It's about the design of singulation protocols. Due to limited computational power on tags, readers have to perform singulation (of tags) without any help from tags. EPC and ISO are two of the open standards. Both deterministic collision avoidance protocol (used in UHF systems) and probabilistic collision protocols (used in HF systems) were discussed. The concept of singulation session during which the singulation identifier does not change was introduced because changing the identifier makes singulation impossible but singulation identifiers have to be dynamic and perfectly random in order to solve the traceability problem.
- Physical layer: physical signal can allow an adversary to recognize a tag even if the information exchanged can not be understood. In a communication channel, parameters follow a given set of standards and use of a different standard makes tags easy to be distinguished. Radio fingerprinting (eg, due to differences in manufacturing technologies) can also be a threat but it's difficult to prevent.

10. Barthel, H., Franciosi, F., "The EAN.UCC Global Approach To RFID For Supply Chain Applications," EAN international, Mar 2001

This article states that EAN.UCC has formed a Global Project Team to access radio frequency technology in May 1997 and released a whitepaper on RFID in Nov 1999. Taking the minimum protocol set (MPS) approach; it says that "no additional protocols, other than MPS, shall be imposed between a GTAG and the reader". (GTAG is the UHF tag defined in EAN.UCC's GTAG program). Furthermore, it mentioned that "GTAG parameters table have been fully developed in full accordance with ISO 18000 parameter table and can be directly submitted to ISO SC31/WG4 for inclusion in their RFID standards". The reasons why taking UHF is because

- It is the most versatile portion of the radio spectrum that meets supply chain applications' business requirements.
- It has the best performance for truly global logistics applications,
- It is a proven technology and,
- It is scaleable down to item level management.

11. Beck, A., "Automatic Product Identification And Shrinkage: Scoping The Potential," Efficient Consumer Response (ECR) Europe, Jul 2002

This report laid out the problem of shrinkage due to internal theft, external theft and supplier fraud. It refers to a study which states that "If all stock loss could be eliminated the profits of a typical European retailer would be 58% higher". The current shrinkage solutions include the following approaches

1. procedures and routines, such as hot product identification, rigorous delivery checking procedures
2. people and processes, such as covert surveillance of customers or employees
3. equipment and technology, such as CCTV, EAS tagging
4. design and layout, such as designing-out blind spots and single direction product flow

The author suggests that the Auto-ID technology can be used to tackle process failures problem which is a "non-malicious unintentional outcome of a breakdown in the management of the movement of products through the supply chain", the supplier fraud when the recipient of goods is unable to perform a physical check of the claimed item delivery, internal theft, collusion and external thefts by using an Intelligent Electronic Article Surveillance system

where even item movements can be monitored. The author states "Auto ID offers the very real prospect of providing shrinkage managers with a window on real stock loss."

12. Beigl, Michael et al. A location model for communicating and processing of context, Personal and Ubiquitous Computing Vol. 6 Issue 5-6, pp. 341-357, ISSN 1617-4909, 2002

13. Borriello, Gaetano, and Want, Roy "Embedded Computation Meets the World Wide Web," CACM 43 (5), May 2000

14. Brock, David L., "The Electronic Product Code (EPC) – A Naming Scheme for Physical Objects," Auto-ID Center, January, 2001

15. Brock, David L., "The Virtual Electronic Product Code," Auto-ID Center, January 2001

16. Buckner, Mark et al. Miclog RFID tag program enables total asset visibility, Proceedings IEEE MILCOM 2002, Anaheim, CA

17. Cachon, G., Fisher, M., "Supply Chain Inventory Management And Value of Shared Information," Management science, (46) 8, INFORMS, 2000, 1032-1048

    Retailer's orders convey a substantial portion of information that a supplier needs to perform ordering and allocation functions. In addition, a retailer's demand information is most valuable when the retailer's inventory level approaches to the point that should trigger the re-ordering process. In other words, when the retailer's information is most valuable (to the supplier), the retailer is already likely to submit an order and thereby, conveying the necessary information without explicit effort on sharing of demand data. Under the settings where demand is known, retailers are identical, there's only a single source of inventory, no capacity constraints, no incentive conflicts and firms choosing a rational order policy, the study concludes that to accelerate and smooth the physical flow of goods is significantly more valuable than using information technology to expand the flow of information.

18. Cavoukian, A., "P3P and Privacy: An Update For The Privacy Community," Center for Democracy and Technology (CDT), March 2000

    P3P cannot protect user privacy in jurisdictions with insufficient data privacy laws. P3P cannot ensure companies to follow their claimed privacy policies. In spite of these, CDT supports the development of P3P because it believes P3P will increase consumer trust and P3P is a component for improved privacy practices (openness of a company's privacy practices) on the Internet.

19. Cavoukian, A., "Tag, You're It: Privacy Implications Of Radio Frequency Identification (RFID) Technology," Information and Privacy Commissioner / Ontario, Feb 2004

    This report covers RFID technologies and pointed out "the fear of ubiquitous tracking of anybody with a proper reader, without knowledge or consent" as a privacy issue. Potential ways (hidden placement of tags, unique identifiers for all objects worldwide, massive data aggregation, hidden readers, individual tracking and profiling) that RFID can be use to

threaten privacy were given. Safeguards (like use of kill switches and blocker tags) were discussed. "Notice and consent, choice, control" were named as the 3 central pillars of privacy. EPIC's opinions on businesses' RFID practices (to protect consumers, not grudgingly deal with privacy merely because of legislation) were stated. a list of companies using RFID was also given

20. Chair of the APEC Electronic Commerce Steering Group, "APEC Privacy Framework (for consideration)," Oct 2004

This document lists the 9 APEC privacy principles. Commentaries for each of the principles were given, together with the guidance for domestic implementation. (cross border guidance are still under development). The 9 principles are

1. Preventing harm, "to prevent misuse of personal information and consequent harm to individuals"
2. Notice, "to ensure individuals are able to know what information is collected about them and for what purpose it is to be used"
3. Collection limitation, "limits collection of information by reference to the purposes for which it is collected"
4. Uses of personal information, "limits the use of personal information to fulfilling the purposes of collection and other compatible or related purposes"
5. Choice, "to ensure that individuals are provided with choice in relation to collection, use, transfer and disclosure of their personal information"
6. Integrity of personal information, "recognizes that a personal information controller is obliged to maintain the accuracy and completeness of records and keep them up to date"
7. Security safeguards, "recognizes that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards"
8. Access and correction, "this principle includes specific conditions for what would be considered reasonable for what would be considered reasonable in the provision of access" and "form in which access would be provided"
9. Accountability, "When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent"

Guidance for domestic implementation fall into the following categories

1. "maximizing benefits of privacy protections and information flows
2. giving effect to the APEC privacy framework
3. educating and publicizing domestic privacy protections
4. cooperation between the public and private sectors
5. providing for appropriate remedies in situations where privacy protections are violated
6. mechanism for reporting domestic implementation of the APEC privacy framework"

21. Chin, L., Wu, C., "The Role Of Electronic Container Seal (e-seal) With RFID Technology In The Container Security Initiatives," 2004 International Conference on MEMS, NANO and Smart Systems (ICMENS), IEEE 2004

Container security initiative (CSI) is created after the Sept 11 terrorist attack to ensure cargo containers coming in to the U.S.A from ocean are well monitored and inspected along the way to ensure they arrive in U.S ports without mass destruction material. E-seals from different

manufacturers employ different communication frequencies, different communication protocols and tamper detection methods. There are e-seals working at 433MHz (Savi, e-logicity), 916.5MHz (Hi-G-Tek) and 2.44GHz (All-Set) Trade-offs in system design include communication protocols, frequency selection, reader infrastructure and seal location and read range limitations.

22. Closs, D., Mollenkopf, D., "A Global Supply Chain Framework," Industrial Marketing management 33, 2004, 37-44

    Michigan State University created a "21st century logistics framework". The framework identifies six competencies and can be grouped into operational (customer integration, internal integration and supplier integration), planning (technology and planning integration, measurement integration) and behavioral processes (relationship integration). To measure a firm's success, 13 logistics and supply chain variables are used to describe 5 key performance areas (customer service, cost management, quality, productivity and asset management). A study was carried out to compare the differences between the US and ANZ companies. It had been found that internal integration may not be important for small companies but high levels of logistics competencies do lead to superior logistics performance.

23. Cole, Peter. A study of factors affecting the design of EPC antennas & readers for supermarket shelves, Auto-ID white paper

24. Consumer Privacy and Civil Liberties Organizations, "RFID Position Statement of Consumer Privacy And Civil Liberties Organizations," Nov 20, 2003

    RFID technology poses threats to privacy and civil liberties. For example:
    - hidden placement of tags,
    - globally unique identifiers for objects,
    - massive data aggregation,
    - hidden readers,
    - individual tracking and profiling

    This article suggests the following RFID practices that should be prohibited:
    - merchants force customers to accept live or dormant RFID tags,
    - prohibition on individuals to detect RFID tags, readers and disabled tags on items possessed,
    - use RFID to track people,
    - used in the way to eliminate or reduce anonymity, eg, embedding into currency.

    Some of the areas that is acceptable for usage are:
    - tracking of pharmaceuticals (permanently removed before being sold to consumers),
    - tracking of manufactured goods(permanently removed before being sold to consumers),
    - detection of items containing toxic substances (when they are delivered to the landfill)

25. Cranor, L., "Designing A Privacy Preference Specification Interface: A Case Study," Workshop on Human-Computer Interaction and Security Systems, 2003

    This paper reviews some of the challenges that the author faced while designing the user interface for the AT&T Privacy Bird, a P3P user agent. Challenges in designing a user interface for setting privacy preferences include:

- privacy policies are complex,
- user preferences are also complex,
- users are inexperienced and unfamiliar with the terminology

To approach these challenges, the author suggested to focus on a subset of the vocabulary (in P3P), bundle similar vocabulary elements together, do not use jargons and use a layered interface design, such as a separate "Advanced" menu, to hide complicated options from users who will never need to access.

26. Cranor, L., "The Role Of Privacy Enhancing Technologies,"
www.cdt.org/privacy/ccp/roleoftechnology1.shtml
last accessed: Jan 31, 2005

    First of all, functions of currently available privacy-related technologies were identified. These functions include
    - prevention of unauthorized access to communications
    - automatic retrieval of data collector's privacy practices file and automatic decision making on the data subject's side based on the claimed practices
    - filtering of unwanted messages
    - prevention of automated data capture
    - preventing communications from being linked to a specific individual
    - facilitating transactions that reveal minimal personal information

    The author states encryption helps to protect privacy and P3P helps indirectly because of the increased transparency in the data collector's privacy protection practices. Spam filter, cookie cutter and anonymizers are discussed. Even though crypto techniques in addition to use of anonymizer could alleviate online privacy concerns, companies hesitate to adopt because it is beneficial to collect customer information. The conclusion drew was that PET is to complement regulatory and self-regulative initiatives and their usefulness is limited.

27. Decker, Christian et al. A peer-to-peer approach for resolving RFIDs, The 5th international comnference on ubiquitous computing, Oct 2003

28. Decker, Christian et al. eSeal - A system for enhanced electronic assertion of authenticity and integrity, Proceedings of Pervasive Computing, Second International Conference, Vienna, Austria, Apr 2004

29. Decker, Christian et al. Revealing the retail black box by interaction sensing, Proceedings of the ICDCS 2003, 2003

30. Dipert, B., "Reading Between The Lines : RFIDs Confront The Venerable Bar Code," EDN, Oct 2004

    Interests in RFID has accelerated dramatically during the last few years and part of the reason for this is due to the advancement if semiconductor technologies. Table 1 in this article lists a comparison of RFID systems in use. LF and HF passive systems have a read range as far as 1.2m while it is 4 meters for UHF passive systems and 15 meters for active microwave systems. Currently, LF has 74% market share, HF 17%, UHF 6% and microwave 3%. Transponder orientation and globally accepted frequency are concerns for both of the UHF and microwave.

The global RFID database could induce privacy issues and it could enable retailers to find out items that their customers bought elsewhere in the world. RFID deployments and applications mentioned in this article include Walmart, DoD, E-ZPass and FasTrak (the highway tolling system), usage in pharmaceutical industry and tagging of clothes in primary school in Japan.

31. Duri, S., Elliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., Tang, J., "Data Protection And Data Sharing In Telematics," Mobile networks and applications (9), Kluwer Academic, 2004

    "Automotive telematics may be defined as the information-intensive applications enabled for vehicles by a combination of telecommunications and computing technology. Telematics by its nature requires the capture, storage, and exchange of sensor data to obtain remote services. Such data likely include personal, sensitive information, which require proper handling to protect the driver's privacy. Data protection challenges in the automotive telematics domain include:

    - data integrity and authenticity,
    - flexibility and heterogeneity,
    - limited user interaction

    The architecture proposed in this paper is to address these problems by giving different stakeholders control over data sharing and use. The architecture allows trustworthy telematics service provider to assume functions of less capable in-car clients and enables data aggregation before data is released to other service providers (thus minimizing privacy issues).

32. EAN International, "Report On The Discussion Regarding The Radio Spectrum Allocation For RFID in UHF in Region 1", RFID and radio spectrum harmonization workshop, Apr 2001

    In regulatory terms, RFID systems fall in the Short Range Devices (SRDs) category. It's understood by EAN and UCC that the UHF band is not exclusive for RFID usage but on a non-interference basis with other users. EAN and UCC had submitted the response to "questionnaire to the industry" issues European Standardization and Telecommunication Institute (ETSI) and a technical proposal detailing how spectrum allocation could look like.

33. EAN.UCC, "White Paper On Radio Frequency Identification," EAN.UCC, Nov 1999

    EAN.UCC started to investigate the potential benefits of RFID in 1996. The work group ISO/IEC JTC1/SC31/WG4 was formed to set standards to allow co-existence of numerous RFID tags and interoperability of RFID systems. At the time of this publication, only the GTAG and JMG submission had been accepted in the ISO18000-6. An RFID application can be divided into 3 layers. The transport layer for the physical interface, frequency; communication layer describes how RFID tags and readers communicate and understand each other and application layer is where data transfers occur for industrial, commercial or other activities. Advantages of RFID were identified for its read-write capability, no line-of-sight scanning, higher data capacity, durability and higher scan rate etc. Constraints identified were cost, conductive material environments, presence of liquids, susceptibility to electromagnetic interference, human exposure to RF emission and read accuracy.

34. EDN Europe, "RFID and the Smart Label; Bye-bye Bar Code?" June 2000

35. Electronic Design, "Smart labels use RFID Technology to Speed Airline Baggage Handling," 4 May 1999

36. Engels, D., "A Comparison Of The Electronic Product Code Identification Scheme And The Internet Protocol Address Identification Scheme," Auto-ID Center, 2002

The EPC numbering system has the following characteristics:
1. EPC is segmented into four hierarchically encapsulated partitions (version, domain manager, object class, serial number) regardless of the total number of bits in the identifier,
2. Regardless to the version number, as long as the domain manager, object class and serial numbers are not changed, the numbers still considered as identical. (so the EPC has 3 levels of hierarchies),
3. Once assigned, the EPC will permanently associate with the object. IP is not assigned permanently,
4. EPC is assigned to physical objects while IP is assigned to network interfaces,
5. EPC is an information pointer but IP is a routing address,
6. EPC has 64 bit, 96 bit and other identifier bit lengths but IP(v6) has a fixed 128 bit

37. Engels, Daniel, "The Use of the Electronic Product Code," Auto-ID Center, February 2003

38. Engels, Daniel, "EPC-256: The 256-bit Electric Product Code™ Representation," Auto-ID Center, February 2003

39. EPCglobal Inc., "Hardware Certification Program," EPCglobal Inc., Aug 2004

This document describes EPCglobal's efforts on developing a uniform hardware certification. This certification program is on Generation 1 standards of the EPCglobal Network hardware components. There are 3 types of tests, conformance test (measure of a device's compliance to a given standard), interoperability test (measure of a device's ability to operate with other devices) and performance test (measure of a device's performance under real world conditions). There are three preliminary determinations (test environment, test equipment and test performer) for each of the tests. In addition, it states that the UHF Generation 2 air interface protocol is to address the end user community's desire for a single foundation protocol. (instead of the two different air interface protocols in Generation 1's Class 0 and Class 1 tags). Details of the tests on Generation 1 and Generation 2 products were given.

40. EPCglobal Inc., "The EPCglobal Network And The Global Data Synchronization Network (GDSN): Understanding The Information & The Information Networks," EPCglobal Inc., Sept 2004

This paper tries to clarify the functions and benefits of the EPCglobal Network and the GDSN. Static information refers to the core data of certain object class and dynamic information refers to the specific data of an individual instance. The role of GDSN is to ensure the quality of static information while EPCglobal Network enables the collection and communication of dynamic information about the movement of individual items. The Global Location Number (GLN) and the Global Trade Item Number (GTIN) are global identification numbers in the

GDSN. They serve to identify locations and trade items respectively in the EAN.UCC system. GDSN provides "a single entry point for trading partners to synchronize static information using interoperable data pools and the GS1 Global Registry." In the EPCglobal Network, Electronic Product Code (EPC) is the standardized item identifier. "Assignment of unique EPC to individual items enables the collection and communication of dynamic information throughout the EPCglobal Network." GTIN has been integrated into the EPC numbering system and thus, "EPC not only provides the global information number for accessing the dynamic information about an individual item in the EPCglobal Network but also the global identification number for EAN.UCC users to access static information about that item's product group in the GSDN." The goal of EPCglobal Network is to provide a method for information collection and sharing about physical movement of individual items. The goal of GSDN is to ensure the quality of static information for collaborative trading.

41. EPCglobal Inc., "The EPCglobal Network Demonstration," EPCglobal Inc. 2004

This paper mentioned 2 cases of EPCglobal Network demonstrated live at EPCglobal US Conference in September 2004. In the first case, it demonstrated "how an EPCglobal Subscriber can positively establish the identity of an EPC tagged product through the EPCglobal Network". Through partner collaboration and communication, how an authentic product arrives at the correct retailer destination. In the second case, it showed that "how trading partners can find out exactly how much product is located in a store's backroom and on the selling floor in a critical product launch scenario." "The information is designed as a high-level guide for organizations wish to understand and take advantage of EPCglobal Network to gain more control of the supply chain and achieve the greatest return on their trading partner relationships."

42. EPCglobal Inc., "The EPCglobal Network: Overview Of Design, Benefits & Security," EPCglobal Inc., Sept 2004

There are five components in the EPCglobal Network: EPC, ID system, EPC middleware, Discovery services and EPC Information Services (EPC IS). The EPC is a unique number, the ID system consists of EPC RFID tags and EPC RFID readers, EPC Middleware manages real-time read events and communicates with the EPC IS, Discovery Services is a suite of service (like Object Naming Service(ONS)) to enable users to find data related to a specific EPC and EPC IS enables users to exchange EPC-related data with trading partners. The EPCglobal Network provides three critical advancements to product identification in supply chain:

1. a unique number of individual objects in motion in supply chain,
2. Use of RFID to remove the line of sight requirement for reading product identification numbers,
3. the network provides real-time object movement information to authorized and authenticated users. On security, EPC provides no information beyond the number itself and all information associated with an EPC is only accessible to authorized users. "Without access to the information, the EPC is meaningless."

43. EPCglobal Inc., "EPC Tag Data Standards Version 1.1 Rev. 1.24", Standard Specification, Apr 2004

"The Electronic Product Code (EPC) is an identification scheme for universally identifying physical objects via RFID tags and other means." A standardized EPC data consists of an EPC (or EPC identifier) and an optional filter value. The EPC identifier is used to uniquely identify an individual object and it consists of a header and a domain identifier. There are three levels of identification (pure identity layer, encoding layer and physical realization layer) and this specification addresses both the pure identity and encoding layers in detail. There are two types of identity in the pure identity layer, the General Type and the EAN.UCC System Identity type. In the General type, "the General Identifier (GID-96) is independent of any known, existing specifications or identity schemes." The GID is composed of three fields – the General Manager Number (assigned by EPCglobal to an entity), Object Class (assigned by the EPC managing entity and unique in each General Manager Number domain to identify a class or type of thing) and Serial Number (a non-repeating serial number for every instance with each object class). "Encodings of the GID include a fourth field, the header, to guarantee uniqueness in the EPC namespace." This specification defines five identity types in the EAN.UCC System type. These are

1. Serialized Global Trade Identification Number (SGTIN)
2. Serial Shipping Container Code (SSCC)
3. Serialized Global Location Number (SGLN)
4. Global Returnable Asset Identifier (GRAI)
5. Global Individual Asset Identifier (GIAI)

The Header "defines the overall length, identity type and structure of the EPC Tag Encoding, including its Filter Value". Its length is variable, "using a tiered approach in which a zero value in each tier indicates that the header is drawn from the next longer tier". The optional Filter Value is not part of the GTIN or EPC identifier. It is "for fast filtering and pre-selection of basic logistics types, such as items, inner packs, cases and pallets". This specification also gives the encoding and decoding procedures for each of the identifier types.

44. Eyefortransport Global Research, "The Next Generation Transportation Management System," March 2004

45. Fano, Andrew, and Gershaman, Anatole "The Future of Business Services in the Age of Ubiquitous Computing," CACM, 45 (12), December 2002

46. Fletcher, R., Omojola, O., Boyden E., Gershenfeld, N., "Reconfigurable Agile Tag Reader Technologies For Combined EAS And RFID Capability," Proceedings of the Second IEEE Workshop on Automatic Identification Advanced Technologies, Summit, New Jersey, 1999

A RFID reader is responsible to transmit energy to tags, to detect tag responses and to translate the responses into meaningful data. In this paper, the authors presented 4 ways to implement a RFID reader (of different specifications and capabilities) as the concept of an open architecture for electromagnetic tagging. These include a $500 parts cost reader that is capable to detect resonant and harmonic signals from DC to 300kHz, a $50 parts cost battery-powered version that operates from 5 to 40MHz and finally, a $5 parts cost micro-controller based solution and finally, making use of FPGA, a soft core solution.

47. Flint, D., "Strategic Marketing In Global Supply Chains: Four Challenges," Industrial Marketing Management 33, 2004, 45-50

Supply chain management provides a cost reduction opportunity for companies and if supply chain management orientations are adopted within a chain, then parties inside the chain will be benefited. Other than cost savings, facilitation of marketing strategies, creation of superior customer value, satisfaction and loyalty can also be obtained. But for global supply chains, the author pointed out 4 significant strategic marketing challenges:

1. The need to learn the immediate down-stream customer's values, goals and relative importance rankings of product and services attributes. For example, survey is an effective means for data collection in the US but not in other parts of the world. To accomplish the task, the first step is to recognize the fact that everyone in the supply chain may value something differently. The second step is to recognize that many methods will be needed to capture those different value perceptions.
2. The need to understand customer value changes in global supply chain. There are two categories of approaches to predict customer values:
    a. trend analysis of aggregate customer/market data,
    b. idiosyncratic customer change analysis.
3. Delivering value. The pace of change in global markets appears accelerating. It is still unclear if this uncertainty would affect strategic supply chain relationships. Market-driven organizations recognize that not only do within-firm functions share a responsibility but linked firms within supply chain share the same responsibility to create and deliver superior customer service. Key firms in strategic alliances as well as 3rd parties, like LSP, have to cooperate to achieve the goals.
4. Customer value process challenge. There must be processes that generate and share market intelligence in a timely manner. In the discussion part, the author laid out a set of question that can help an organization to understand customer values.

48. Floerkemeier, C., Lampe, M., "Issues With RFID Usage In Ubiquitous Computing Applications," Pervasive 2004

This paper presents various sources of error in passive RFID systems.

1. Tag read errors due to tag collision (consequence when more than one tag is in the reader field),
2. Tag detuning (effect when tags are placed too close),
3. Environmental factors (e.g., metals nearby).

Implications of these for a better system design:

1. Use UHF which offers a wider bandwidth and can afford the bandwidth demand for deterministic anti-collision algorithm,
2. Random placement of tags reduces detuning (which occurs when tags are stacked together)

Authors suggested other approaches like, if it's known that certain tags are always moving together, the presence of some implies the presence of those missing (group constraint). Also, RFID technology can be augmented by computer vision systems or weighing scales etc.

49. Fontanella, J., "Finding The ROI In RFID," Supply Chain Management Review, (8) 1, ABI/INFORMS Global, Jan/Feb 2004, 13

There are four types of RFID implementation mentioned.

1. Discrete process. This is to overcome the shortcomings of the current system. Due to the fact that RIFD is used for a specific purpose, it has the greatest chance for success. (Manufacturing automation, make-to-order/Kanban automation, asset tracking),
2. Intracompany. Extending RFID-enabled business processes across two or more entities within company. (Asset management, raw material to finished goods, plant to warehouse),
3. Intercompany. The synchronization and coordination of RFID-enabled business processes with a limited number of supply chain participants to provide differentiated services. But unless you are the channel master, supply chain partners will expect the deliverable value while causing them minimal disruptions to their operations. It's impossible to control other entities and so, intercompany projects MUST be viewed as a form of process automation. the sponsoring company must retain full control over choice of hardwares etc. (VMI, inventory status and tracking)
4. Synchronization, ubiquitous use of RFID across an entire industry. this is well beyond the current technology. (EPC-enable supply chain, inventory lifecycle tracking). Suggestion: do not move forward to a business case that requires wide-spread adoption of RFID. Instead, focus on smaller projects.

"Based on the interviews did for the report, there are siz common attributes that successful RFID implementation shared to mitigate risk":

- Create company support for RFID adoption,
- Deploy only when all variables are known and under control
- Do not take the face value of the performance claimed
- Minimize application integration requirements
- Use service providers that have hands-on experience
- Protect the investment by structuring RFID contracts so to protect the intellectual property

50. Garrison, C., Clark, D., "Web Site Privacy Policies Must Give Users Notice, Choice, Access, Security," The business journal of Kansas city, March 8, 2004

The FTC has identified "notice, choice, access and security" are the 4 foundations for any online privacy policy. To comply with FTC's suggestion, web sites must offer some level of choice for users. However, a site has complete control over how much choices it wishes to provide. Security refers to the operator's obligation to protect users' information against unauthorized use, access, disclosure, loss or destruction. Failure to adequately implement security measures can lead to FTC prosecution.

51. GCI, IBM, "An Integrated View Of The Global Data Synchronisation Network And The Electronic Product Code Network," Global Commerce Initiative, Sept 2004

This is a 14-page report on the relationship between the Global Data Synchronisation (GDS) Network and the EPCglobal Network. The GDSN consists of

- Interoperable, certified Data Pools,
- A Global Registry,
- A set of EAN.UCC standards

The GDSN holds party data, category specific data, target market specific data and relationship specific data while the EPCglobal Network holds manufacturing information like (lot number, manufacturing data, expiry date) and lifecycle history information. Currently, the GDSN and EPCglobal Network have a shared dependency on core product information (like brand name,

colour, weight etc). This report views both of the networks as "key components in building the foundation for supply chain collaboration".

52. GCI Working Group on Intelligent Tagging, "Intelligent Tagging," White paper, Global Commerce Initiative, Apr 2002

The GCI Intelligent Tagging Model is divided into four supply chain elements - manufacturing, fulfillment (distribution), store and consumer. For each of these elements, four delivery modes (truckload, pallet, box or case, consumer unit) and six components (functionality of the process or application, technical requirements, operating conditions, ergonomic conditions, data required and benefits) were considered. Some of the RFID benefits for supply chain management are improved efficiency, more flexible scheduling, complete visibility of asset movements and total order management. With the availability of the RFID standard developed by EAN.UCC (GTAG) and realizing the need for a standard numbering system, "the GCI Intelligent Tagging working group formed a close and formal liaison" with EAN.UCC and Auto-ID Center "to jointly endorse global and open standards in the field of RFID and Intelligent Tagging".

53. Gilmore, D., "Anatomy Of An RFID Pilot," Supply Chain Digest, Feb 10, 2004

Four application of RFID in supply chain are:
1. for compliance,
2. to improve logistics processes,
3. to improve internal production processes,
4. to track containers of goods across long distances.

The author identifies 4 phases of RFID pilot activity,
1. application definition/business case development,
2. technology immersion,
3. product testing,
4. production pilot.

The objective for phase 1 is to define new RFID process flows and estimate the return of investment. Objective for phase 2 is to gain baseline familiarity with RFID technology and options. Phase 3 is to understand the specific interaction of tag types, placement and reader configuration and in phase 4, to validate technology performance, fine tune process flow assumptions and make a "go or not go" decision.

54. Glidden, R., et. al. “Design of Ultra-Low-Cost UHF RFID Tags for Supply Chain Applications,” IEEE Communications Magazine, August 2004

55. Glidden, R., Bockorick, C., Cooper, S., Diorio, C., Dressier, D., Gutnik, V., Hagen, C., Hara, D., Hass, T., Humes, T., Hyde, J., Oliver, R., Onen, O., Pesavento, A., Sundstrom, K., Thomas, M., "Design Of Ultra-Low-Cost UHF RFID Tags For Supply Chain Applications," IEEE Communications Magazine, Aug 2004

“This article outlines system architecture and circuit design considerations that influence the development of RFID tags”. Table 1 in this article gives details of Auto-ID Class 0, 1, ISO 1800-6a,b forward link and reverse link air interface and data rates. It indicates that ISO 18000-6a uses adaptive collision arbitration while 6b uses probabilistic binary tree search. Both Auto-ID

Class 0 and 1 systems use a deterministic approach. In designing the tag ICs, the challenges are

- power management,
- non-volatile memory,
- ESD damage,
- die area,
- test cost.

56. Global Commerce Initiative, IBM, "Global Commerce Initiative EPC Roadmap," Global Commerce Initiative, Nov 2003

This article gives a summary of EPC technologies. It states that GCI's global data synchronization activity will complement with the emergence of EPC. For customers using the EAN.UCC system, GTIN (global trade item number), SSCC (Serial Shipping Container Code), GRAI (Global Returnable Asset Identifier) can be integrated into the EPC. (For industries that do not use the GTIN, a different header and EPC number format will be used). Tags, readers and frequency bands were also discussed. It mentioned that, under the EPC vision, 2 potential approaches for data exchanges about tagged objects are:
1. Object and event data are held by each trading partner and a means of information access is provided for trading partners as required,
2. Object and event data are published on a public network and access provided as required.
Companies need to consider management policies for

- data ownership,
- data confidentiality and security and
- data retention and archiving.

It foresees that the EPC network will be into three dimensions:
1. internal EPC network,
2. trading partner-to-trading partner EPC network and
3. industry EPC network.

57. Good, N., Han, J., Miles, E., Molnar, D., Mulligan, D., Quilter, L., Urban, J., Wagner, D., “Radio Frequency Identification And Privacy With Information Goods," Workshop on Privacy in the Electronic Society, ACM, Oct 2004

Information goods refer to books, music and video. "with RFID, protecting private inquiry may become much more difficult". "In pre-RFID world, people can pay in cash leaving no records and can hide the fact of purchase to limit third party knowledge" and wholesalers, retailers are have control over their own records before laws demand their disclosure. With RFID, "anyone with an RFID reader can potentially discover individuals' informational preferences without their permission.” Many of the RFID induced privacy risks are due to the technical design of RFID readers and tags. Risks of RFID discussed are:

- broadcasting and lack of access control of tags,
- labeling, (e.g. library's use of numbers can reveal an individual's choice of reading,
- tracking of individuals, (in the EPCglobal network, local readers upload read logs to the centralized EPC database and the EPC discovery service (EPCDS) poses special dangers.) "The same EPC label can be aggregated and displayed by any user of EPCDS". Reduction of information on tag may not help because the globally unique collision identifiers on some tags provide a static way of tracking tags. ISO 15693 13.5MHz tags carries a unique

64-bit MFR tag ID.

- invisibility, when used as an anti theft device, RFID tags are generally hidden and holders of the tags are unlikely to realise a remote read of the tags.
- Joining data, means a RFID reader working in tandem with a camera or when a reader read more than one tag on an individual, inferences can be made.

Solutions suggested:

- technical fixes like killing tags at point of sales but information goods are generally not subject to obsolescence (this opens a new dimension on how different commodities can be classified with respect to RFID) and would encourage the use of the tag after payment.
- instead of killing, write a random number at checkout. but this semi-static identifier still has the threat of point-to-point tracking.

Best practices include:

- kills tags when there's an opportunity,
- write minimal info onto tags,
- do not use standardized labelling formats for information goods (on RFID tag),
- do not subscribe to the EPC discovery service,
- inform customers that RFID is in use

58. Government of Alberta, "Privacy Architecture Glossary," Government of Alberta, 2002

This is a rich collection of privacy terms with definitions, notes and source details presented in table format. There are 96 terms in total and all are sorted in alphabetical order. These terms are used in the Government of Alberta Enterprise Architecture and for each of the terms, the related taxonomy in the Architecture is given.

59. Graeff, T., Harmon, S., "Collecting And Using Personal Data: consumers' Awareness And Concerns," Journal of consumer marketing, (19) 4, 2002, 302-318

This paper presents the results of a survey, together with survey questions, on consumers' awareness of privacy concerns. It finds out very few consumers are aware of how discount cards are used to collect personal level purchase data and concerns about the use of personal information vary by demographic market segments.

60. Gritzalis, D., Moulinos, K., Kostis, K., "A Privacy-enhancing e-business Model Based On Infomediaries," MMM-ACNS 2001, 72-83

e-business is very much about gaining and maintaining the trust between users. As vendors have no time to bargain with every customer and customers do not have the time and endurance to work out the best available deal, an information intermediary comes into the picture. Security requires strong user authentication but privacy needs to use loose authentication in order to provide user anonymity. The authors introduced their informediaries-based, privacy-enhanced business model. The model includes customers, vendors, customer oriented infomediaries (who act on customer's benefit) and super imfomediaries (who are trusted by both vendors and customers). By using a chain of servers (mixes-Chaum) between customers and customer-oriented infomediaries, two levels of end-to-end user anonymity were achieved:

- Customer personal profile anonymity. (Customers only communicate with super infomediaries who strips off personal information from his requests to customer-oriented

infomediaries and set up direct communication between customers and vendors for goods delivery).
- Communication level anonymity

61. Haenel, D., Burgard, W., Fox, D., Fishkin, K., Philipose, M., "Mapping AndLocalization With RFID Technology," Proceedings of the 2004 IEEE International conference on robotics and automation, IEEE, Apr 2004

Detecting RFID data is the common topic for RFID applications. In this paper, the authors presented their research on locating RFID tags and building the accurate positions of RFID tags. Using a robot armed with antennae and a laser range scanner, the robot first build and a geometrical map of the environment. After then, the system assigns points in the vicinity with probabilities of tag detection. Due to the differences in detection zone of the antennae, a likelihood update is performed for each of the points. The authors reported that they were successful to build an accurate location map of RFID tags using the system.

62. Halliday, S., Convener of ISO/IEC JTC1/SC31/WG4/SG3, Letter to EPCglobal Technical Standards Committee on Jun 18, 2004

In this letter, it states that the AFI (application family identifier) is an issue to the tag, not data on the tag. AFI is used to identify which numbering domain is on the tag since not all 18000-6 tags will use the EPCglobal system. Tag ID is also discussed. ISO 18000 requires compliance with ISO 15963 and Tag ID is to identify the IC, not to represent the object to which is attached. Tag ID (Chip ID), is programmed by chip manufacturer and not assigned by any other else, including EPCglobal

63. Hennig, J., Ladkin, P., Sieker, B., "Privacy Enhancing Technology Concepts For RFID Technology Scrutinised," Research Report, RVS-RR-04-02, University of Bielefeld, Germany, Oct 2004

RFID privacy concerns (worldwide unique IDs enable tracking, unnoticed remote reading without line-of-sight, small hidden tags and readers, tracking and profiling through sporadic surveillance) are listed in this paper. It then pointed out database with RFID is a threat to privacy. This argument is backed up by scenario examples like
- In-store tracking and profiling (intelligent shelves to detect how customers are interacting with products)
- Person-related tags (e.g., RFID tag in shoes)
- Tag presence spotting (this is still a problem even if the data contents are not known)
- Combination of tag information ("multiple tags provide for a kind of individual "fingerprint" even if the unique ID cnnot be read")
- Following a unique ID

Referencing to RFID data security guidelines set by concern groups (e.g., CASPIAN, FoeBud), a checklist was developed. Three PET proposals published were then check against the checklist and it concluded that, none of these proposals can fully address all the concerns. The authors also gave a list of misconceptions of privacy issues in RFID
- Only concerned about eavesdropping,
- Data protection associated with the product, not the customer (i.e., cheaper products need not be secured as much as a more expensive product)

- In-store tracking is not seen as a privacy problem

64. Henrici, D., Mueller, P., "Tackling Security And Privacy Issues In Radio Frequency IdentificationDevices," Pervasive Computing, Lecture Notes in Computer Science 3001, Springer-Verlag, Apr 2004, 219-224

    The first section gives an overview of published approaches to enhance RFID privacy and drawbacks of them. Authors then proposed a scheme which changes traceable identifiers securely at each read attempt.

65. Hewlett-Parkard Development Company, "RFID In The Supply Chain A Balanced View," Hewlett-Parkard Development Company LP., Oct 2004

    This is a 27-page report providing "an overview of the business drivers leading companies are accessing to determine if improvements and efficiencies in the supply chain can be achieved using RFID technology". Challenges in supply chain include
    - incorrect shipment,
    - late shipment,
    - required efforts to accurately reconcile physical goods to customers orders and returns,
    - difficulty in locating goods,
    - misplacement of goods and theft,
    - inaccurate demand forecasting.

    Capabilities of current RFID technology include
    - improved rework or repair processes,
    - improved failure-mode analysis,
    - increased visibility in quantity and location for warehouse applications,
    - stock tracking,
    - asset tracking along the supply chain,
    - lot control,
    - tampered goods identification,
    - improved reverse logistics business processes.

    Key challenges and concerns in retail outlets, logistics delivery and distribution partners, warehouse and manufacturing were studied. The report documents a set of sample plans from HP's internal RFID project to illustrate how to develop a planning framework for any RFID based projects.

66. Hjorth, T., "Supporting Privacy In RFID Systems," Master's Thesis, Technical University of Denmark, 2004

    The main problem about using encryption on RFID systems is due to the constraints like size, power consumption and cost. Focus of this thesis is to use encryption on RFID systems. The author discussed several encryption algorithms based on their implementation and concluded at least secret key encryption is possible in RFID systems (and key management issues are left for further studies).

67. Hochheiser, H. "The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context," ACM Transactions on Internet Technology 2 (4), November 2002, 276-306

68. Hodges, Steve. Chapter 4, RFID: The Concept and the Impact, The Security Economy, OECD 2004

69. Holcomb, M., Fugate, B., Ross, T., Quinn, F., "The Right Connections: Survey of Connectivity And Visibility," Supply Chain Management Review, Oct 2004

This is a study based on responses from 374 supply chain and logistics professionals. Every position is the supply chain is represented in the study. Questions asked include:

- "how order status is communicated (29% by phone, 27% by email with customers; 40% by email and 16% by EDI with suppliers)",
- "How companies communicate (via email: 30% for giants, 38% for non-giants)",
- "How companies rate their internal visibility (out of 8 key supply chain areas, finished goods inventory at field DC level received the highest visibility score while inbound shipment status receives the lowest score.),

On primary tools for distribution and transportation management, 47% use commercial packages for distribution management; 30% use commercial packages and 29% use 3rd party provider for transportation management. Over 40% of the respondents implemented WMS, MRP, ERP, order fulfillment and inventory management systems. CRM gets the highest % (38%) in the top 5 technology investment areas. Budget (35%) is named as the biggest obstacle to technology spending.

70. Huhns, M.N., and Stephens, L.M. "Automating Supply Chains," IEEE Internet Computing, August 2001

71. Hult, G.., "Global Supply Chain Management: An Integration Of Scholarly Thoughts," Industrial Marketing Management 33, 2004, 3-5

The author introduced the globalEDGE portal created by MSU-CIBER (Michigan State University's Center for international business education and research). globalEDGE "connects international business professionals worldwide to a wealth of information, insights and learning resources on global business activities." The heart of the centre is the "integration of consumer needs with the process of new product and service development, strategic management of global operations, product and service assortment management and geographical dispersion". The author also mentioned the six areas of supply chain management are: marketing (including competitor orientation, customer orientation and supply chain coordination), logistics, supply management, operational management.

72. Hultkrantz, O., Lumsden, K., "E-commerce And Consequences For The Logistics Industry," The Impact of E-commerce on Transport, Joint OECD/ECMT Seminar, Paris, 5-6 June 2001

For e-business to grow, the logistics infrastructure must be in place, customers and businesses must have Internet access, sites must have multi-language support, e-commerce must be safe in terms of privacy and monetary transactions, the speed of technology must be satisfactory and international standards must develop. The customer order point will move upwards in a supply chain and demand for faster and more accurate deliveries will increase. One problem

in e-business is that shippers and forwarders do not understand each other's perspective. Shippers concern about how precise and valid a cargo (e-commerce) is while forwarders care about how actually the transportation is carried out (e-fulfillment).

73. Hwang, S.O., Yoon, K.S., "Privacy Protection In Ubiquitous Computing Based On Privacy Label And Information Flow," Computational Science and Its Applications - ICCSA 2004: International Conference, May 2004

The authors investigated informational privacy issues in the ubiquitous computing environment. Informational privacy means "the right of people to determine for themselves when, how, and to what extent personal data about them is communicated to others." By considering the implications of ubiquitous computing environment (control heterogeneity, task dynamism, device heterogeneity, application mobility, context-aware and various types of authentications), the authors proposed a "privacy-protecting framework base on information flow control from individuals to other communication parties." The concept of privacy label that consists of level and domain is used. An individual's private data is transformed into an information set with appropriate privacy label attached. Information flow is controlled according to the privacy labels.

74. IBM Global Services, "Privacy Architecture (PA) Overview," Government of Alberta, May 2003

The Government of Alberta Enterprise Architecture (GAEA) has 6 component architectures dealing with business, data, applications, technology, security and privacy. The Privacy Architecture (PA) is one of the components. Under the PA, there are 10 guidance elements (the glossary, the taxonomy, identity key scheme, design guidance, transformation, active privacy architecture, data placement and private access) and 12 requirements (terminology, identity keys, data classification, data sharing/placement, user interface, data transformation, data subject access, acquisition criteria, consent with choices, access control, PETs and privacy monitoring). Two tables are given in this article to map eight privacy principles and requirements to these elements.

75. Inaba, T., "An Analysis Of Physical Object Information Flow Within Auto-ID Infrastructure," Master's thesis, Engineering Systems Division, MIT, May 2004

From studies, data types (in a supply chain) were found to be 1. historical data, 2. property data. Property data can further be divided into "product-level" and "instance-level". One fundamental assumption of the EPC IS (EPC Information Server) is that it is different in different industries. In this thesis, the author proposed an information flow architecture by defining the requirements of an EPC-IS making use of generic business processes (1. query of product-level data, 2. query of instance-level data, 3. query of location data, 4. query of path data) executed in the Auto-ID infrastructure. By using three simple message schemas with vocabulary sets that are separately defined in dictionaries, a robust and scalable interface was achieved.

76. Information Today, “3M Announces Major New Library Technology System,” January 2000

77. Intermec, "The Write Stuff: Understanding The Value Of Read/Write RFID Functionality," White paper, Intermec, 2003

This white paper describes the capabilities of read/write RFID technology, explains how the read/write technology overcomes the limitations of read-only systems and explains the benefits the rewritable capability in specific supply chain applications. It states that the price difference between read-only and read/write tags is very little while read/write tags can be erased, reused and hold more information locally (thus enables faster processing, reduce data latency). The database dependence problem of read-only tags (created by a scenario where manufacturers, raw material suppliers, logistic providers and retailers need to access the same tag database for their supply chain interactions and created "questions and possible disputes over who "owns" the database.") was discussed. It concludes that read/write technology will be able to meet sophisticated applications needs and provide flexibility to accommodate future changes.

78. Ishikawa, Toshiharu et al. Applying Auto-ID to the Japanese Publication Business, whitepaper, Auto-ID center 2004

79. Isrealsohn, J., "RF Unlocked," EDN, Mar 2003

RF transmission bands for short-haul vary by locale. Because of the ISM bands are shared, use of spread-spectrum technique allows autonomous networks to coexist as noise sources for one another.

80. ISTPA, "The ISTPA Privacy Framework, version 1.1," International Security, Trust and Privacy Alliance (ISTPA), 2002

The set of principles and fair information practices (notice and awareness, choice and consent, access, information quality and integrity, update and correction, enforcement) are only high level guidelines and not operational specific. The ISTPA proposed the framework that enables businesses to deploy automated mechanisms that supports the aim "the proper handling and use of personal information throughout its life cycle, consistent with data protection principles and the preferences of the subject". There are 7 services (audit, certification, control, enforcement, interaction, negotiation and validation) and 3 capabilities (access, agent and usage) under the ISTPA framework. The alliance group agrees that, security is necessary for privacy but the proper handling and use of personal information requires an even broader set of privacy management functions.

81. ITAA, "Radio Frequency Identification, RFID... Coming Of Age, " Information technology association of America (ITAA), Jun 2004

Efficiency gains by using RFID: reduce in labour, errors, handling costs. This report quoted a survey by Cap Gemini and Ernst & Young which finds that, 23% of consumers had heard of RFID, 48% of respondents had no opinion about it, 42% indicated a favourable perception and 10% had an unfavourable perception. Issues related to RFID-induced privacy: hidden placement of tags, globally unique identifiers, massive data aggregation, hidden readers, individual tracking and profiling. According to an analysis performed by VDC (Venture

Development Corporation), the top three fastest growing RFIC sectors, in descending order, are retail services, commercial services and healthcare services. Challenges in using RFID include:

- It requires standardization and stabilization with regard to actual technology and functionality,
- Automated gathering of information stirred up privacy issues,
- The volume of signals generated is large and vendors need to develop a rich two dimensional infrastructure.

82. Jacobson, Joseph, "The Desktop Fab," CACM 44 (3)

83. James, M., "Where Are You Now? Location Detection Systems And Personal Privacy," Research note, Information and Research Services Group, Commonwealth of Australia, Jun 2004

    In this article, it states that "the possible linking of RFID tags on purchased items to personal credit card details and transaction trails raises privacy concerns." The author suggested the following rules for use of RFID tags on consumer product:
    - consumer notification of RFID tags, on purchase,
    - tags can be removed easily by consumers,
    - tags able to be disabled by default,
    - tags are placed only within the packaging, not the product

84. Juels, A., "Minimalist Cryptography For Low-Cost RFID Tags," The Fourth International Conference on Security in Communication Networks -- SCN 2004, Sept 2004

    Low cost RFID tags are computational weak devices and unable to perform basic symmetric-key cryptographic operations. In this paper, the RFID tag under consideration is of weak computational power but with a small amount of rewritable memory. Using the concept of pseudonym throttling, an RFID tag stores a list (refreshable) of random identifiers. Each time the tag is queried, it emits the next pseudonym in the list, cycling to the beginning when the list is exhausted. Such a scheme explores the characteristics of physical limits of adversaries (asymmetric reader/tag signal powers). The scheme is not perfect but offers some degree of security protection. (details and mathematical models omitted)

85. Juels, A., "Strengthening EPC Tags Against Cloning," RSA Laboratories, Oct 2004

    EPC tags are simple and are themselves weak authenticators. Without modifying standard EPC tags, the author proposed a technique to strengthen the resistance of EPC tags to cloning. A skimming attack is a simple reader scan to retrieve a valid EPC which can then be cloned. The author proposed to use the PINs for EPC write kill functions and leverage reader-to-tag authentication to achieve tag-to-reader authentication. (details omitted)

86. Kambil, Ajit, "RFID: Retail's 800 pound gorilla," Logistics Today, October

87. Karjoth, G., Schunter, M., Herreweghen, E., Waidner, M., "Amending P3P For Clearer

Privacy Promises," Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003

A major contribution of P3P to privacy protection is enhanced transparency. Even though it merely reflects and advertises the promises of a particular website and not necessarily to enhance or decrease the privacy of consumers, P3P forces enterprises to describe precisely their privacy practices to website users. This raises privacy-awareness but could also lead to a false sense of privacy. In this paper, the authors criticized the ambiguities in the specifications of P3P (e.g., statement elements RECIPIENT, RETENTION and PURPOSE are not clearly separated) and missing guidelines for user agents (as the user agent interpretation is completely undefined). They suggested an extended but simplified syntax and a revised consent model where opt-in/opt-out choices are grouped into one 'consent block'.

88. Karjoth, G., Schunter, M., Waidner, M., "Privacy-enabled Services For Enterprises," Proceedings of the 13th International Workshop on Database and Expert Systems Applications 2002

This paper is about IBM's Enterprise Privacy Architecture (EPA). This is a methodology and consists of 4 building blocks: privacy regulation analysis, management reference model, privacy agreement framework and technical reference architecture (E-P3P is a refinement of EPA's technical reference architecture). All these building blocks were discussed. It identifies that privacy management services and privacy-enabled security services are the core technologies for enterprises to protect customer's privacy.

89. Karjoth, G., Schunter, M., Waidner, M., "Platform For Enterprise Privacy Practices: Privacy-enabled Management Of Customer Data," 2nd Workshop on Privacy Enhancing Technologies (PET 2002) San Francisco, CA, USA. Apr 2002

There are a number of privacy problems for enterprises that collect data from customers:

- enterprises may not know what type of data they have collected and where the information is stored,
- enterprises may not know the consent a customer has given nor the legal regulations that apply to a specific customer record,
- when customer data are exchanged between enterprises, it's unable to enforce privacy consistently on behalf of the collecting enterprise

This article describes the Platform for Enterprise Privacy Practices (E-P3P) and proposed that E-P3P can be used in:

- Formalizing privacy practices,
- Formalizing policy options,
- customer consent management,
- policy enforcement and
- compliance audit

P3P provides no mechanism for enforcement and audit and the current control access systems only check whether a user is allowed to perform an action on an object. E-P3P is a scheme for

privacy-enabled management of customer data and there are at least four players in the system: data subjects, data users, privacy officer and security officer. E-P3P enables the management of the data subject's consent on a per-person and per-record basis. The stick policy paradigm ensures the user consent and preferences are guaranteed even if the data is passed to another enterprise. The E-P3P works within an enterprise with trusted systems and administrators against misuse or unauthorized disclosure. It cannot protect data if the systems or administrators are not trusted.

90. Karkkainen, Mikko, "Increasing Efficiency in the Supply Chain for Short Shelf Life Goods Using RFID Tagging," International Journal of Retail & Distribution Management, 31 (10), 529

91. Karkkainen, M., Ala-Risku, T., "Automatic Identification - Applications And Technologies," Logistics Research Network (LRN) 8th annual conference, London, UK, September 2003

This paper discussed four categories of automatic identification applications (authentication, tracking, process effectiveness and information management) and how different identification technologies (like bar code, RFID, OCR, biometrics, smart cards, magnetic stripe, Bluetooth, GPS and GSM cell location) are used for each of them. It concludes by comparing the bar code system and the RFID technology under each of the application categories. It states that, RFID is "far more suitable for authentication type applications (due to the relative ease of copying and forging bar codes") and is a viable option for tracking, especially when environmental factors like dirt, damp are considered. For information management applications, the authors suggest if read/write is required, RFID is preferred.

92. Kerer, Clemens. Presence-aware infrastructure using web services and RFID technologies, Technical report, TUV-1841-2004-11, University of Vienna

93. Keskilammi, M., Sydaenheimo, L., Kivikoski, M., "Radio Frequency Technology For Automated Manufacturing And Logistics Control. Part 1: Passive RFID Systems And The Effects Of Antenna Parameters On Operational Distance," International Journal of Advanced Manufacturing Technology (21), Springer-Verlag 2003, 769-774

Antenna parameters like the frequency used for identification, the gain, the orientation, the polarization, the placement of the tag on an object all have an impact on the RFID system's read range.

- Gain: The read range of an RFID system is highly dependent on the reader antenna gain. Using multiple antennae connected to a reader or adding a few additional elements in a antenna array will significantly increase the gain.
- Frequency: the size of an antenna is proportional to the wavelength used in a system. Generally, the antenna size is a limiting factor for RFID transponders.
- Polarization: polarization mismatch is the polarization inequality between the receiving antenna and the transmitting antenna. The amount of power extracted by an antenna from the incoming signal can be varied by polarization. If the angle of polarization-mismatch increases, power loss starts to increase significantly. A circular polarized field consists of two linear fields having a 90-degrees phase shift and a linearly polarized

transponder antenna can detect the matched part. In application, if position known, one can use linearly polarized antenna to maximize the read range. If position and angle not known, use circularly polarized antenna on the reader. If transponder antenna is linear and reader is circular, the max read range is always less than the case for polarization-matched, linearly polarized antennae.

94. Kim, A., Hoffman, L., Martin, C., "Building Privacy Into The Semantic Web: An Ontology," Position Paper, International Workshop on the Semantic Web, May 2002

The Semantic Web could bring profound effects on how personal information is collected and used. The authors suggested trust, security and a standard method of exchanging privacy policies are required to achieve privacy.

95. Kimball, Dan. RFID Technology Primer, DoD 2004 RFID summit for Industry

96. Knospe, H., Pohl, H., "RFID Security," Information Security Technical Report (9) 4, Elsevier 2004, 39-50

"This article describes the technical fundamentals of RFID systems (components and the communication model consists of the Application layer, the Data Link layer and the Physical layer) and the associated standards (ISO 18000 series for item management; EPC HF, UHF 0, 1 for Electronic Product Code; ISO 14443 and 15963 for contact-less chipcards and ISO 14223, 11784, 11785 for animal identification.) Security and privacy aspects (confidentiality, integrity, availability, authenticity and anonymity) were covered in the article. A survey on current proposals for RFID security enhancement was presented. The proposals include approaches like access control and authentication, tag authentication, encryption and message authentication.

97. Kumar, R., "Interaction Of RFID Technology And Public Policy," paper presentation at RFID privacy workshop @MIT, Massachusetts, Nov 2003

In this paper, ways (like "kill tag", "faraday cage", "active jamming", "smart tag") to preserve privacy in an RFID-enabled environment were discussed. To kill a tag, one has to issue the "kill" command from the reader but this command may not be functional all the times. The faraday cage approach is to shield the tag with metallic foil but this is also a way to do shop lifting. Active jamming is to broadcast a radio signal so to interrupt readers but this may be illegal. The smart tag approach involves cryptographic methods and selective blocking of unauthorized readers and discloses information selectively decided by the customer but complexity involved may be a "logistical nightmare". To protect privacy by a regulation approach, the author discussed self regulation and states that, instead of using a pure market approach where a company's privacy practice is driven by customers' demand, government-legislation, enforcement and adjudication have to be in place. The author states also there is a lack of fair information practices followed by database owners. Internet also makes it possible for organizations to disseminate information without the immediate knowledge of consumers. Quoting Simson Garfinkel's self regulatory framework, the "RFID bill of rights" is as follows: "

- The right to know whether products contain RFID tags,
- The right to have RFID tags removed or deactivated when they purchase products,
- The right to use RFID-enabled services without RFID tags,

- The right to access an RFID tag's stored data,
- The right to know when, where and why the tags are being read"

Examples for good practices include:

- respect confidentiality (strip off all personal and identifying information),
- don't flame (data collected must not be altered),
- don't be anonymous (data collector should tell when where how and for what purpose the data was collected),
- don't allow third party to access other's data (without valid and authentic reasons),
- don't misrepresent or lie,
- follow government's general guidelines (repository owners or managers should check if data solicitor has RFID privacy policy),
- consider presentation of message (repository owners must evaluate the content of data to be disseminated and aware of cultural differences and other issues that may result.)

The three aspects have to be considered are:

- quality of the data being collected,
- quality of the data being stored,
- quality of the data being disseminated.

To conclude, the author suggested the following approaches as solutions to privacy threats:

- technical solution (kill, faraday's cage, smart tag),
- regulatory approach(a. "business shall not combine or link an individual's non-public information with RFID, b. consumer must be informed about RFID collection system and what would be done in future to data collected"),
- self regulation (each commercial organization should define a policy framework and follows that),
- protocol setup (a proper protocol has to be set up to achieve a good level of security at data repositories and exchanges)
- data integrity (business should not disclose an individual's non-public information in association with RFID tag information to an unaffiliated third party)
- non identification (business shall not, directly or through an affiliate or non-affiliated third party, use RFID tag info to identify an individual),
- limited access to the personal data (data exchange systems should be password protected)
- branding RFID and educating the public (educate shoppers the benefits of RFID they will gain and assuring them their privacy will not be intruded)"

When framing a RFID policy, questions like how will the policy affect other parties, what are the legal baselines to follow, what operational features of RFID and data collection, storage, dissemination systems should affect any policy on access, use and disclosure, what analogies can be made to help to formulate the policies, what criteria should be used to evaluate the policy and has the policy been disclosed in advance to all concerns, are needed to be asked. (These factors should also be taken into consideration: who from the commercial organization, privacy advocates and government agencies should participate in the development of the policy; what corporate resources are involved in formulation, what information to gather in advance and what kind of research methods to be used)

98. Landt, J., "Shrouds Of Time," AIM Inc., 2001

Author is the founder of Amtech Technology, a spin off of the Los Alamos Scientific Lab (LASL) in 1977, and is the chief scientist in Transcore, leading technical development of RFID systems. This paper gives an overview of RFID development from 1940 to 2000.

99. Laurant, C., Farrall, K., "Comments Of The Electronic Privacy Information Center To The Federal Trade Commission," Electronic Privacy Information Center (EPIC), Jul 2004

In this article, it suggests that, the "Collection limitation principle", the "Openness principle" and the "Accountability principle" under the OECD privacy principles should further be extended for the RFID regime. On Collection, it suggests that 1. RFID tags should easily be removable by consumers, 2. associating RFID tags to PII should be avoided, 3. if tag PII association is the case, it should be voluntary, with consumer written consent, 3. no covert capture is permitted. For "Openness", tag labeling should be displayed clearly and no secret tag-reading. For "Accountability", an accountability mechanism MUST be established

100. Leaver, S., Mendelsohn, T., Overby, C., Yuen, E., "Evaluating RFID Middleware, Picking The Right Solution For Integrating RFID Data Into Business Applications," Tech Choices, Forrester Research Inc., Aug 2004

"To stand the test of time, RFID middleware must include a balanced combination of core infrastructure and packaged application features, including device management, integration, data management and packaged business logic." Based on these criteria, the paper compared currently available products from Savi Technology, TIBCO Software, ConnecTerra, RF Code, Microsoft, OATSystems, Sun Microsystems, IBM, Oracle, Manhattan Associates and SAP. It found that packages from Manhattan Associates and OATSystems are "best suited for meeting the needs of time-strapped early adopters" and forecasted that platforms from Oracle and IBM will dominate when the firms build out broader RFID architectures.

101. Leong, Kin Seong. Prospects for Ubiquitous item identification, Proceedings of the Auto-ID Labs Workshop Zurich, 2004

102. Li, Y., Zhu, S., Wang, L., Jajodia, S., "A Privacy-enhanced Microaggregation Method," Proceedings of the Second International Symposium on Foundations of Information and Knowledge Systems, 2002, 148-159

Microdata sets are groups of records containing information about individual respondents and each individual respondent is recorded in microdata with two types of variables, the identification variables (e.g. name) and sensitive variables (e.g. salary). These variables need to be protected due to the "right of the individual to privacy". Somehow, "right of society to information" requires adequate statistical information to be supplied and released to the public. Microaggregation is a family of disclosure control methods for protecting numerical variables in microdata and the basic idea is to cluster individual records in microdata into a number of mutually exclusive groups prior to publication. The average over each group will be published instead of individual records. (Details ignored but just to capture the idea of microaggregation)

103. Lind, M., "RF Tags - Introductory Basics," Pacific Northwest National Laboratory, Jul 2001

An RF tagging system requires at least two components, a tag and an interrogator. The author classifies RF tags into three categories, passive, semi-passive and active. Tags can be read only, read/write or sensor based. "Passive tags use backscatter modulation to reflect incoming RF energy from the interrogator to communicate via a code sequence". "Semi-passive tags also use backscatter modulation and they have an energy storage device on board which powers the electronics. The interrogator wakes up the tag to begin communication." Active tags have an active RF transmitter as well as a power source on board. Tags are subject to RF constraints, cannot be seen in a metallic enclosure, generally orientation sensitive and may not be compatible between different vendors (due to differences in communication protocols, frequencies and designs)

104. Lind, M., Carrender, C., "A Primer On RF Communications And RF Tags," Pacific Northwest National Laboratory, Nov 1999

"A basic RFID system consists of three components: an antenna coil, a transceiver (with decoder) and a transponder that is electronically programmed with unique information." A generalized read range of a RFID system is as follows:
125kHz systems: 30 cm passive and semi-passive, no active counterpart
13.56MHz systems: 70cm passive and semi-passive, no active counterpart
433MHz systems: 15 meters passive, 30 meters semi-passive, 200 meters active
915MHz systems: 10 meters passive, 20 meters semi-passive, 150 meters active
2.45GHz systems: 1 meter passive, 10 meters semi-passive and 50 meters active
5.8GHz systems, no passive counterpart, 10 meters semi-passive, 50 meters active
Wireless standards (IEEE 802.11, IrDA, GSM, etc) as well as technologies for Electronic Article Surveillance (acousto-magnetic, electromagnetics, swept-RF and microwave) were also mentioned and explained.

105. LogicaCMG, "Making Waves: RFID Adoption In Returnable Packaging," RFID benchmark study, LogicaCMG Nederland B.V., 2004

This is a 76-page report focused on RFID's use on returnable transport items (RTI) such as pallets, crates and roll containers. The study was through an interview with 50 organizations in six European countries with added cost/benefit analyses and a review of literatures.

106. Luckett, D., "The Supply Chain," BT Technology Journal, 22(3), Jul 2004

The author names operational improvements, audit trails, inventory efficiency and security are some of the reasons for RFID deployment. Consumer privacy was discussed. The author points out a mobile phone is already a device that enables tracking and surveillance and RFID privacy concerns may due to the fact that consumers do not see too many advantages of using RFID, even though the manufacturers or retails said that the cost savings will be passed down to them.

107. Madsen, P., Adams, C., "Privacy And XML," XML.com, Apr 2004

The XML-based techniques relevant to privacy are:
P3P (developed by W3C),
XACML (proposed by OASIS, provides fine grain control of authorized activities),

XML Encryption (W3C proposal, an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it),
XML Signature (W3C, XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere),
WS-Security (a proposal from Microsoft, used to add security metadata to SOAP messages),
SAML(OASIS, provides a standard way to define user authentication, authorization and attribute information in XML documents)

108. McGinity, Meg "RFID: Is This Game of Tag Fair Play?" CACM 47 (1), January 2004

109. Meloan, S., "Toward A Global "Internet Of Things"," Sun Microsystems Inc., Nov 2003

RFID will have fundamental impacts on retail, industries of manufacturing, transportation, health care, life sciences, pharmaceutical and governments. It offers the opportunity of a real-time view of assets and inventories throughout the supply chain. Brief description of EPC network components is given.

110. Merrells, J., "Introduction To XACML," presentation, Parthenon Computing Ltd.

XACML is the extensible access control mark-up language published by OASIS. The article describes the Access control language, the processing environment and the request/response protocol. The access control language consists of types, equality operators, arithmetic operators, string functions, numeric conversion, logical operators, arithmetic comparators, string comparison functions, bag functions, set functions and higher-order bag functions (any-of, all-of). In the XACML processing environment, data flows between Policy Access Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP) and Policy Information Point (PIP). It states that the XACML request/response protocol is used between PEP and POP.

111. Miller, Steven P. What is RFID? AIDC, Western Carolina University

112. Ministry of Economic Development. An Engineering Discussion paper on spectrum allocations for short range devices, Ministry of Economic Development, New Zealand, Aug 2004

113. Molnar, D., Wagner, D., "Privacy And Security In Library RFID Issues, Practices And Architectures," CCS'04, Oct 2004

Owning to the need for item tracking, authors investigate the use of RFIDs in library as a candidate to foresee privacy issues that would happen when item-level tagging becomes more popular. Authors mentioned the tracking and hotlisting are privacy concerns. This shows that the conventional wisdom believing there is no privacy issue as long as the adversary has no access to the database is not necessary true. They stated that "good security practice dictates that each tag has a distinct secret key" and to solve the problem "how can two parties that share a secret key authenticate each other without revealing their identities to an adversary?" They proposed a private authentication protocol.

114. Motorola, "RFID: Everything You Need To Know," Motorola Inc., 1997

In this article, how RFID works is explained. Aspects like communication methods (eg, using cyclic redundancy check to avoid noise-induced misread), tag orientation, collision, radio frequency selection were discussed. It states also "there is a little difference between an RFID tag and a contactless smartcard". RFID can be use for a wide range of applications which include access control, animal identification, asset management, athletic event management, automotive anti-theft, container tracking, electronic article surveillance, fare collection, fueling management, fugitive emission inspection systems, gas cylinder tracking, hazardous material tracking, industrial laundries, luggage tag, meatpacking plants, process manufacturing, product identification, raw material inventory, restaurant service, scale interface, ski industry, time and attendance, tools, toll roads, vehicle identification, warehouse management, waste management, yard management. A sample of cost justification analysis is given comparing the cost of a bar code system and a RFID system.

115. Murry, S. et. al. "Tracking Semiconductor Part Changes Through the Part Supply Chain," IEEE Transactions on Components and Packaging Technologies, 25 (2), Hune 2002

116. Naedele, M., "Standards For XML And Web Services Security," IEEE Computer, Apr 2003

This article gives a brief description of different XML security specifications, especially on SAML and XACML

117. Narasimhan, R., Mahapatra, S., "Decision Models In Global Supply Chain Management," Industrial Marketing Management 33, Elsevier Inc., 2004 21-27

This paper presents a list of decision models in supply chain management categorized into different problem areas, for example, strategic decision making, tactical aspects and operational aspects. Five models (related to

- investment implications of innovation-based competition between buyer and supplier,
- bidding by a prospective supplier of a product,
- bid evaluation and supplier selection by a buyer dealing in multiple products,
- integrated operations in a supply chain and
- market integrated distribution)

were examined and used to "illustrate the diversity of analytical approaches and their usefulness in managing global supply chain issues".

118. Nasution, B., Kendall, E., Khan, A., "Algorithm Exchange Of A Security Control System For Web Services Applications," Proceedings of the 38th Hawaii International Conference on System Sciences, 2005

The authors propose that algorithm exchange will be more appropriate than key exchange for Web services. Algorithm exchange is the core part of the TTSN (Trusted Transient Simple Network) which is still under development. The authors believe that the current XML-based

transaction are likely to be intercepted since encryption methods used are from a "standard set" of technologies (eg, DES, Blowfish etc.) and use of PKI is not feasible because dynamic update of secret key is not possible. They claim this paper to be the first one on algorithm exchange implementation and comparisons to IPSec and Opportunistic encryption were given

119. Oasis, "eXtensible Access Contol Markup Language (XACML) Version 2.0, Committee Draft," Organization for the Advancement of Structured Information Standards, Dec 2004

    Other than describing the elements of XACML, important concepts like the PAP (policy administration point), PDP (policy decision point), PEP (policy enforcement point) and PIP (policy information point) were introduced. This helps the reader to build a better picture of data-flow path in a supply chain, from a security point of view.

120. OECD, "OECD Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data," Feb 2002

    Recognising the common interest in protecting privacy and individual liberties, the automatic processing and transborder flows of personal data contribute to economic and social development, the council of OECD determined to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among member countries and put into effect of the implementation guidelines on Protection of Privacy and transborder flows of personal data on 23rd September 1980. This document states the privacy protection principles and guidelines with detailed comments. Up to date, OECD (Organization for Economic Co-operation and Development) has 30 country members.

121. OFTA, "Adoption Of Performance Specification For Radio Frequency Identification Equipment Operating In 865-868MHz And/Or 920-925 MHz Bands," OFTA, Nov 2004

    This memo proposes the adoption of HKTA 1049 specification which states that, “the radio equipment shall operate in the 865 - 868 MHz and/or 920-925 MHz bands with the peak transmitter power not exceeding 4W EIRP”. Other technical specifications for 865-868MHz band shall follow ETSI EN 302 208-2 and for 920-925MHz band, follow FCC part 15.247

122. OFTA, "Frequency Allocation For Radio Frequency Identification Equipment," OFTA, Jul 2004

    RFID reader transmitting in the 902 -928 MHz band will cause harmful interference to GSM900 base-station receivers using the 890-915MHz band. RFID tags comply with ISO18000-6 respond to frequencies anywhere from 860-960MHz. In HK, there is a vacant frequency block from 920-925MHz. The 864.1 - 868.1MHz band has been allocated to CT2 services (cordless phones), which is declining rapidly worldwide. There is a directive in Europe to withdraw the CT2 service before the end of 2005. So, OFTA proposes the 865-868 MHz and 920-925MHz bands for RFID applications.

123. Ohkubo, M., Suzuki, K., Kinoshita, S., "Cryptographic Approach To "Privacy-

Friendly" Tags," RFID Privacy Workshop, MIT, 2003

RFID privacy problem has two components, 1. data leakage from RFID-tagged belongings and 2. behavioral tracking and personal identification by tracing tag IDs. One of the important technical points when constructing an RFID scheme is to ensure forward security, ie., "data transmitted today will still be secure even if secret tag information is revealed by tampering in the future". This paper suggests how the author's previously proposed low-cost hash chain mechanism for user privacy protection.

124. Overby, C., "RFID: The Smart Product (R)evolution," The TechStrategy Report, Forrester Research Inc., Aug 2002

This 20-page report covers the basics of RFID, its uses, the benefits of RFID in a supply chain (providing information on what is the product, where the product has been, what is the demand for the product, how the product was consumed and disposed), conditions were RFID deployment should be considered (labour-intensive and error-prone, vulnerable to supply chain loss, high-dollar assets and demand limited collaboration) and suggests health, beauty and tobacco products are prime RFID candidates. A forecast on the number of CPG tagged items rises from 5 billion in 2005 to 45 billion in 2009 is given.

125. Philips, Tagsys, Texas Instrument, "Item-level Visibility In The Pharmaceutical Supply Chain: A Comparison Of HF And UHF RFID Technologies", White paper, Jul 2004

RFID advantages mentioned in this article include visibility, efficiency in supply chain, accountability, brand protection, anti-counterfeiting, expiration management, reduced shrinkage, and advantages over bar codes. Differences between HF and UHF were given, like read range, coupling methods and the effects of water and metal. Due to a better defined field, HF offers a better performance to locate tagged items packed within a small area. HF has been tested for years in garment to withstand liquid, pressure and temp changes. For UHF, bending the antenna will cause substantial tag performance. HF is well developed, the 13.5Mhz is available worldwide and power limits are uniform. UHF is very different, available frequency band, allowable transmission power and bandwidth restriction vary between regions and countries. A few cases on how HF systems are used in the pharmaceutical field (such as, surgical garment management, locating tissue samples, tracking pathology samples and blood matching) were reported.

126. Polizzi, T., "RFID Class Warefare," Wireless Communications, Computing and Networking (WCCN) Letter, June 2004

This article presents two scenarios on the what-ifs when EPCglobal takes Gen2 to be ISO 18000 based or not. It expects, if EPCgloabl doesn't take the ISO route, then infrastructure suppliers may support both ISO and EPCglobal standards but chip suppliers may not. The author expects that people will pick the ISO standard because of ROI. Tag standardization is also another problem.

127. Pottie, Gregory J. “Privacy in the Global E-Village,” CACM 47 (2), February 2004

128. Pounder, C. and Kosten, F., "Managing Data Protection," Chapter 4, Second Edition, Butterworth Heinemann

This is a review of the 8 data protection principles from Council of Europe Convention 1981 with interpretations and comments. A list of procedural review questions and a checklist of audit issues were also given.

129. Price, J., Jones, E., Kapustein, H., Pappu, R., Pinson, D., Swan, R., Traub, K., "Auto-ID Reader Protocol 1.0," Auto-ID Center, Sept 2003

The reader protocol has 3 layers, the reader layer (specifies the content and formatting of messages between the reader and the host), the messaging layer (specifies how messages defined in the reader layer are framed, transformed and carried on a specific network transport and how an underlying network connection is established, initialization messages required etc) and the transport layer (corresponds to the networking facilities provided by the operating system or equivalent). For the messaging layer, there are multiple alternative implementations, eg, TCP/IP based or bluetooth-based. The interface between the reader layer and the messaging layer is defined in terms of message channels. Two message channels are defined, the control channel and notification channel. A reader has 2 subsystems as well. The read subsystem consists of the source stage, the data acquisition stage and read filtering stage. The event subsystem consists of the smoothing and event generation stage, the event filter stage and report buffer stage. Details for each of these were given.

130. Q.E.D. Systems, "Active And Passive RFID: Two Distinct But Complementary Technologies For Real-time Supply Chain Visibility," Q.E.D. Systems, 2004

RFID can be used for different functions in a supply chain. For area monitoring, high-speed multi-tag portal capabilities, electronic manifest, use of active tags is recommended. For cargo security, both active and passive can be used for e-seal but passive cannot be powered while cargo in transit. Active tags can continuously monitor and report seal location and with built-in sophisticated anti-spoofing functions. Passive tags are with limited read range, unable to detect at high speed, may require substantial process re-design and worker training. On the other hand, passive tags are cheap, right choice for applications that have rigid business process, with constrained asset movement, require very simple security and limited data storage. To conclude, active and passive are fundamentally different and neither of them provides complete solutions for the supply chain applications.

131. Quinn, J., "Retailers Face The Question: Is The Future In RFID?," Supply chain management review, (8) 1, ABI/INFORM Global Jan/Feb 2004

Benefits of RFID: faster scanning, easier location of goods and total visibility. Problems faced by manufacturers include added cost of placing tags and the value of the technology will diminished if there's a disconnection along the chain. The author believes the migration to EPC/RFID will be driven by retailers because the technology helps the retailers to eliminate the "lost" items in warehouses which in turn, for most of the time, results sales loss.

132. R. Moroz Ltd., “Understanding Radio Frequency Identification (RFID) – Passive

RFID", July 2004

133. Ranasinghe, D., Engels, D., Cole, P., "Low-cost RFID Systems: Confronting Security And Privacy," Auto-ID Labs research workshop, Sept 2004

In terms of RFID, security refers to one or a combination of the following:

- message content security,
- Integrity of message content,
- Authentication of sender and recipient,
- Non-repudiation by the sender and recipient and availability

RFID system's privacy implies providing 1. anonymity (location privacy) and 2. unlinkability. "tags and readers are constantly in an un-trusted environment that lacks confidentiality and the integrity of the message is doubtful and there are no means for establishing non-repudiation by readers or the RFID labels". Labels are exposed to physical attacks. Spoofing is a serious threat e.g., replacing a tag with a cheaper item's tag. Denial of service (DoS) attack can be carried out by placing a large number of fake labels to the reader. Most of the privacy concerns are generated by 1. the unique identification label, 2 collection of information, 3. dissemination of information 4. mass utilization of the RFID technology. The authors point out that the current bar code system has many the same risks but they do not have the potential for these operations to be performed wirelessly and unconstructively on an immense scale. Challenges in providing security and privacy for low-cost RFID systems include: cost, regulation, power consumption, performance and power disruption. The primary difficulty is due to the scarcity of resources on the RFID IC. Cryptographic hardware consumes considerable power and will severely shorten the read range and overall system performance. UHF regulation on power limits the maximum power available to the tags, regulation for frequency hopping (changing of frequency after certain period of time) limits the maximum transaction time (400 msec in US). Authors stated that "security and privacy issues concerning RFID are solvable using a set of security mechanisms. A security mechanism is a collective term used to refer to a combination of cryptographic primitives and protocols used to provide security". Security primitives include "primitives without using keys", "symmetric key primitives" and "asymmetric key primitives". References were given for more details on wireless attacks, physical attacks. For the low cost RFID tags, they generally will have 400 gates and it's not feasible to implement the available security primitives on them. (e.g. AES needs 20k to 30k gates) however, it states that it may be possible to create new hash functions by using existing or new private key cryptosystems. Randomized access control, use of cellular hash and use of non-linear feed back shift registers were mentioned. The authors conclude that perfect secrecy is only a mathematical concept, areas like cost effective and efficient hardware implementations of cryptosystems, development of hardware efficient hash functions, develop protocols with the flexibility to incorporate different cryptographic primitives, optimization of coupling between readers and labels will benefit the improvement of RFID security and privacy.

134. Ranasinghe, D., Engels, D., Cole, P., "Security And Privacy: Modest Proposals For Low-cost RFID Systems," Auto-ID Labs Research Workshop, Sept 2004

With the assumptions on constraints for UHF RFID tags (200-4000 logic gates, 5-10 msec response time, 100kbps data transmission rate, lower than 150 microwatt power consumption),

the authors proposed the following concepts to countermeasure the weakness in low-cost RFID security and privacy.

- to use a challenge response pair created by Physically Unclonable Functions (PUF),
- to store an encrypted version of the EPC concatenated with a random number at the POS (secret key is known solely to the retailers) before purchase and using a customer's public key,
- a shared secret scheme (not studied in detail)
- a many shared secrets scheme

135. Rao, K V S., "An Overview Of Back Scattered Radio Frequency Identification System (RFID)," Proceedings of IEEE Asia pacific microwave conference, Singapore, Dec, 1999, 746-749

    RFID system based on modulated backscatter signal detection was discussed. Description of back scatter signal detection principle and typical RFID chip specification were given. "A back-scattered RFID system has a RF base station module, computer controller, an RF transponder and a detecting and processing unit attached to the transponder in the form of a chip." "The base station has a micro-controller module, DSP module, radio module and a circularly polarized base station antenna pair. Frequency hopping is used in US.

136. Raza, N., Bradshaw, V., Hague, M. "Applications of RFID Technology," IEE Colloquium on RFID Technology, 1999, Other articles in the same colloquium: "RFID Solutions for the Express Parcel and Airline Baggage Industry", "A Simple Radio-Frequency System for Asset Tracking Within Buildings"

137. Resources and Networks Branch, "An Engineering Discussion Paper On Spectrum Allocations For Short Range Devices," Ministry of Economic Development, New Zealand, Aug 2004

    The band differences in Europe and US appear to be inevitable. NZ sees the need to accommodate RFID from both of the regions and in order to minimize the impact to growth of RFID, NZ will freeze issuing licences in the 868 to 870 , 915 to 921MHz bands

138. Robertson, I.D., Jalaly, I., "RF ID Tagging Explained," IEEE Communications Engineer, Feb 2003

    In this paper, there includes a table of ISM bands in different countries, description of different tag types. Long range systems use electromagnetic waves to power tag chips and tags communicate with readers by backscatter modulation.

139. Reagle, J. and Cranor, L. "The Platform for Privacy Preferences," Communications of ACM 42 (2), February, 48-55.

140. Rogerson, S., "Tag Ethics," Originally published as ETHIcol in the IMIS Journal (14) 5, Oct 2004

    Animal identification, vehicle anti-theft systems, library book tracking, pallet tracking and

building access control are some of the current applications of RFID. The six elements for an integrated approach to public policy relating to RFID are: 1. technical, 2. industry self-regulation, 3. ethical approach, 4. legislation, 5. RFID branding, 6. consumer education. Of the ethical approach, it would be based upon: 1. respect confidentiality, 2. don't "flame", 3. don't be anonymous, 4. "don't allow 3rd party to access other's data", 5. "don't misrepresent or lie, 6. follow government's general guidelines, 7. consider presentation of message.

141. Rugman, A. Girod, S., "Retail Multinationals And Globalization: The Evidence Is Regional," European management journal (21) 1, Feb 2003

Defining global retail multinational enterprises (MNE) are those with sales balanced across the EU-North America-Japan triad with at least 20% in two other parts of the triad and 50% or more in total sales are foreign, a empirical study was performed on 49 largest retail MNEs in the world. It's been found that only one company (LVMH) is truly global and Wal-Mart is only a regional MNE. Wal-Mart has a five-format-retail pattern: convenience store, Supercenters, Sam's club (membership based), neighborhood stores and online retail

142. Rutner, S., Waller, M., Mentzer, J., "A Practical Look At RFID," Manufacturing Net, http://www.manufacturing.net/SCM/article/CA380959.html, accessed 9/24/2004

In manufacturing, RFID can be used to support quality control. In distribution centers, RFID can speed up the record of truck appointment time and input of exact counts of goods to warehouse management system automatically. This results an improved product flow through the distribution center. RFID can also be used to identify compatibility problems of hazardous materials, help management to set benchmarks and evaluate employees and to improve accuracy of the shipping process. In retail industry, shopping behavior highly impacts the amount of safety stock needed. If a product type has more than one holding location in a store, then RFID helps to allocate inventory more accurately, reduced inventory-holding costs, optimize sales and reduced costs. RFID also facilitates product-rotation practices. The negative aspect is the consumer privacy concerns.
Possible supply chain impacts include:

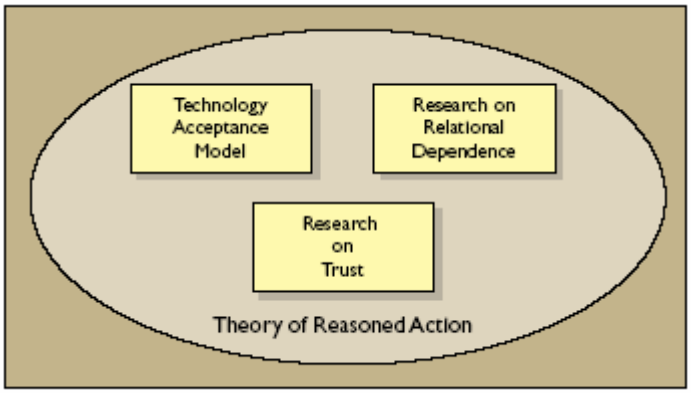
- RFID may increase the power of retailers in the supply chain relative to suppliers,
- RFID may reduce retailers' reliance on suppliers for category management,
- RFID may increase the economic power of larger retailers in the supply chain as compared to smaller ones.

Managerial implications include:
1. To exam if the enhanced information and visibility can provide the biggest and fastest returns and to consider the organization's position in the supply chain (a retailer with poor product rotation practice may get hurt by the increased information visibility)
2. Decide the implementation or adoption time,
3. Judge the capability of current information system.

143. Salam, A.F., Iyer, L. Palvia, P., and Singh R. "Trust in e-Commerce," Communications of the ACM 48 (2), February 2005, 73-77.

The authors "explore the comprehensive framework they developed for understanding trust in the context of Internet-enabled exchange relationships between consumers and Web-based vendors in any industry." They claim the framework draws on findings from four main

research streams: TAM, theories on trust, theories on relational dependence, and fused together via the theory of reasoned action (TRA) – shown in Figure 1 copied as follows:



The interest at this point is to find out 'research on relational dependence which "examines issues related to different types of relationships and their characteristics." (Fiske, A. Relativity within moose culture: Four incommensurable models of social relationships. *Ethos* (1990), 180-20

144. Sama, S., Engels, D., "RFID Systems, Security & Privacy Implications," white paper, Auto-ID Center, 2003

Discussions on tag anti-collision and reader anti-collision were given. EPC is retrieved as part of the anti-collision process. Some approaches to RFID protection were discussed as well. [contents similar to #109]

145. Sarma, S., "Integrating RFID," ACM Queue (2) 7, ACM, Oct 2004

After a brief history of how Auto-ID Center was founded, the author stated the two-pronged strategy they took in designing the EPC tag. Their first part was to lower the tag cost by minimizing the complexity of the state machine and memory required on the RFID chip. The second part was to put much of the tag associated data on a network. Challenges in tag reading are unreliable reads and the generated high volume of data. Device management is complicated by the differing standards around the world.

146. Sarma, S., Brock, D., Engels, D., "Radio Frequency Identification And The Electronic Product Code," IEEE Micro Nov-Dec 2001

Near field RFID systems run at 13.56MHz, with distance up to a few feet. Far field systems run at 915MHz, extending to over 10 feet. Applications of RFID include warehouse management, transportation and quality control in the supply chain's back-end, on-shelf stock monitoring, theft control, automatic retail checkout. Bar code scanning is 5 billion daily and RFID offers a single platform on which several applications can be implemented simultaneously. The possibility of delivering 5-cent tags requires a system-level approach, encompassing IC design and manufacturing, RF protocol, reader design, back-end networking, antennae manufacturing. EPC was designed with these objectives:

- To reduce memory burden on tag,
- To reduce IC area and power requirements,
- To save RF bandwidth,

- To make the system more robust

Alien Technologies developed a fluidic assembly technique for assembling ICs into the package. Depending on anti-collision algorithms, a tag may need a random number generator; more counters and buffers on-chip. For frequency bands, none of them has all the benefits for all applications. Authors also suggested using the same API regardless of the system frequency.

147. Sarma, S., Weis, S., Engels, D., "RFID Systems And Security And Privacy Implications," Cryptographic Hardware and Embedded Systems -- CHES 2002, Aug 2002

On the RFID basics, a RFID system consists of 3 components, transponder, transceiver (reader), data processing subsystem. Passive tags obtain their operating power by harvesting energy from the electromagnetic field of the reader's communication signal, either by inductive coupling or far-field. For inductive coupling, the communication signal induces a current in the coupling element (eg a coiled antenna). This current charge up a on-tag capacitor. The whole system behaves like a loosely coupled transformer This coupling method works to a maximum of 1/2(pi)f meters from the signal source. Far field starts where near field ends. In the far field, "a reader communicates with and powers a passive tag using the same signal. Using the same signal for both power transmission and data communication has 2 trade-offs. 1. Any modulation of the signal causes a reduction in power to the tag", 2. modulating information onto the spectrally pure sinusoid spreads the signal in the frequency domain. (side band) This spread, together with the maximum power level at any frequency, is regulated by local government. This restriction limits the rate at which data can be sent from reader to tag. Side band limits and emitted power levels are especially stringent for ISM bands. Passive tags do NOT actively transmit a signal. In the near field, tag to reader communication is achieved by load modulation. (modulating the impedance of the tag). In the far field, tag to reader communication is done by backscatter. (modulating the radar cross-section of the tag antenna). In the US 915MHz band, it is required to change channel frequency every 400msec. This also limits length of transaction between tags and readers. In the data coding section, it states that level codes (like non-return-to-zero NRZ) and transition codes (eg pulse pause modulation PPM) are two main categories used in RFID. To select a coding scheme, one has to consider:

- the code must maintain power to the tag as much as possible
- the code must not consume too much bandwidth
- the code must permit the detection of collision.

Most RFID systems use PPM (pulse position modulation) or PWM (pulse width modulation) for reader to tag communication and Manchester or NRZ (Non-Return-to-Zero) for tag to reader. For modulation methods, Amplitude Shift Keying (ASK) is generally used for HF load modulations while Phase shift keying is commonly used for backscatter modulation. Two tag anti-collision methods are discussed, probabilistic (tags respond at randomly generated times, based on Aloha, common for HF) and deterministic (base on their unique identification number, e.g. binary tree walking, common for UHF). Performance metrics of an RFID system include: speed at which tags can be read, outgoing bandwidth of the reader signal, bandwidth of the return signal, the amount of states can be stored on tag, tolerance to noises, cost of tags, cost of readers, ability to tolerate tags which enter and leave the field, the count accuracy, the read range. Anti-collision algorithms have to be leverage in order to increase efficiency. On reader collision, (Frequency hopping is a technique used to keep two

or more readers from interfering with each other while reading RFID tags in the same area. For example, UHF RFID readers in the United States are said to operate at 915 MHz. They actually operate between 902 and 928 MHz, jumping randomly (or in a predetermined sequence) to frequencies in between 902 and 928 MHz. !david, no frequency hopping in Europe, unknown for asia/region 3)
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=43) It's similar to frequency assignment in wireless systems. The solution is to allocate frequencies over time to a set of readers either centrally or in a distributed manner. (There are around 50 channels, each of 250kHz bandwidth for frequency hopping in US) EPC system has 4 key components, the EPC, the ONS, the Savant and RFID transponder. The EPC identifier is used in anti-collision algorithm and there is a self destruct command (kill) for EPC tags. RFID new privacy threats are due to the higher difficulty for tag owners to physically impede unauthorized communication with tags. Security goals include reader/tag authentication, channel security, no association between tags and holders, no information leak to unauthorized readers. The basic design of factory-programmed, read-only tags violates these two privacy goals: tag-reader authentication and tracking. The solution to tracking could be to erase the unique serial number at the point of sales. As for tag-reader authentication, a public key cryptography solution could be used but this is not feasible for low cost tags. The author mentioned using symmetric message authentication as well (but compromising one tag will compromise the whole batch). Authors then suggested a one-way hash function approach (assuming a portion of the memory is reserved for a meta-ID and rewritable and tags only reply queries with a correct meta-ID.)

148. Sarma, S., Weis, S., Engels, D., "Radio Frequency Identification: Security Risks And Challenges," Cryptobytes (6) 1, RSA Laboratories, 2003, 2-9

RFID creates new security issues. Consumer privacy is compromised by unauthorized extraction of tag information, being physically detected by tag to identity association. On the corporate side, inventory with un-protected tags can be monitored by competitors and yielding valuable sales and marketing data. Strong cryptographic solution is not feasible on low cost tags. Tag contents are used as a look-up key into the back-end database and independent databases may be built by anyone, allowing unrelated users in the supply chain to develop their own applications. Entire history and whereabouts of a particular item can be monitored and associated with shipping and purchasing data. It assumed that low cost tags have insecure memories that contents can be extracted by physical attacks like laser, water etching, x-ray or ion-probing. Location privacy is violated even if the tag contents are secure. This is because as long as the tag response is predictable, association of tags to individuals can be made. Corporate spies might be able to derive valuable logistics information without knowing the actual contents of the packages. Low-tech attacks like putting tagged items into a metal lined bag can be prevented by traditional methods like cameras. DoS, spoofing were also mentioned. The main differences between these attacks on RFID and bar-codes are:

- they can be carried out wirelessly,
- can be on massive scale (automatic).

Challenges faced are:

- asymmetric signal strength should be taken into consideration when designing protocol,
- low cost tags may need to be resistant to protocol attacks for 10 minutes,
- to protect location privacy, tags cannot respond in a predictable manner.

- tag key management,
- an efficient means to transfer tag ownership.

The authors believe the line between RFID tags, smartcards and general purpose computers will blur in the future.

149. Satoh, Ichiro. Linking physical worlds to logical worlds with mobile agents, IEEE International Conference on Mobile Data Management (MDM'04), 2004

150. Scharfeld, T., "An Analysis Of The Fundamental Constraints On Low Cost Passive Radio Frequency Identification System Design," Master's thesis, Department of Mechanical Engineering, MIT 2001

    Constraints in electromagnetic, communications, command protocols, regulations and physical implementation were discussed. Constraints for range are field strength, orientation, antenna geometry, environment, power delivered, power consumed and power reflected. Data rate is affected by the choice of operating frequency and identification rate is related to the performance of the anti-collision protocol.

151. Senior Review 15 (1) , "RFID Enhances Materials Handling," 36-39, 1995

152. Simchi-Levi, D., Zhao, Y., "The Value Of Information Sharing In A Two-stage Supply Chain With Production Capacity Constraints: The Infinite Horizon Case," Manufacturing & Service Operations Management 4(1), Winter 2002

    Under the assumption that the retailer faces independent demand and the manufacturer has finite production capacity, the study was carried out to characterize the impact of information sharing in a two-stage supply chain with a single manufacturer and a single retailer in infinite time horizon. The conclusion says that, "for any finite cyclic order-up-to policy, the associated inventory positions and shortfalls give rise to Markov chains with a single irreducible, positive recurrent class and a finite steady-state average cost." The authors observed that "the percentage cost savings due to information sharing increases as production capacity increases" and "non stationary demand may have a substantial impact on both the benefits from information sharing and the optimal timing of information sharing."

153. Singh, Nitin, "Emerging Technologies to Support Supply Chain Management," CACM 46 (9)

154. Smaros, J., Angerer, A., Fernie, J., Toktay, B., Zotteri, G.., "Retailer Views On Forecasting Collaboration," Logistics Research Network Annual Conference, Dublin, Ireland, September, 2004

    Collaborative planning, forecasting and replenishment (CPFR) supposed to be a very good idea to increase efficiency and improve customer service but in reality, the adoption rate is very slow. To find out the reason(s), the authors put out three hypotheses

    - The technology investments required for large-scale collaboration slow down adoption but do not present a critical obstacle to forecasting collaboration,
    - retailers' limited forecasting resources and lack of forecasting processes present a critical

obstacle to CPFR-style forecasting collaboration, but not to more streamlined collaboration practices,

- Due to different replenishment lead-times and aggregation levels, retailers and suppliers have different forecasting and collaborative needs

and examined them by using the data collected through in-depth interviews with 12 European grocery retailers. It was found that the lack of forecasting capabilities is a more important obstacle than investments in IT. Evidence on different forecasting needs was also observed.

155. Sorrells, P., "Optimizing Read Range In RFID Systems," EDN Dec 7, 2000

This article is on LF and HF tags. It has identified that the maximum reader power output, coupling and tag power consumption are important design factors for an RFID system. A tag design example was also given.

156. Spiegel, R., "RFID Report," Supply Chain Management Review, (8) 4, ABI/INFORM Global, May/Jun 2004

This article reports some of IT suppliers' RFID projects which include Microsoft set up the RFID Council industrial group and its membership with EPCglobal, Oracle's sensor-based services and the RFID pilot kit, Siemens' release of flexible RFID applicator, Apriso's EPC/RFID integration into its FlexNet.

157. Spiekermann, S., "Stated Privacy Preferences Versus Actual Behaviour In EC Environments: A Reality Check," Proceedings of Wirtschaftsinformatik 2001, Augsburg, Sept 2001

From the results of a survey, it finds that the actual behaviour of online shoppers differs from their said privacy preferences. It suggests that the assuming privacy conscious people will also act accordingly may be wrong. It appears that people appreciate the EU regulations but forget privacy concerns once they are on the Web.

158. Spiekermann, S., "The Desire For Privacy: Insights Into The Views And Nature Of The Early Adopters Of Privacy Services," International Journal of technology and Human Interaction, 1(1), Jan - Mar 2005, 74-83

There are different types of mentality that drives people want to be kept anonymous. In table 5 of this article, there gives a categorization. They are

1. The general conscious
2. freedomers
3. Orwellians
4. the curious
5. people with secrets
6. the political conscious
7. filter counterers
8. sniff avoiders
9. free netters

10. hacker avoiders

159. Spiekermann, S., Berthold, O., "Maintaining Privacy In RFID Enabled Environments, Proposal For A Disable-model," Privacy, Security and Trust within the Context of Pervasive Computing, The Kluwer International Series in Engineering and Computer Science, Springer Verlag, 2005

The authors proposed 2 types of privacy enhancement models for RFID tags since they expect (sooner or later) RFID tags should have the write-many capability and this is good for consumers as well, if that's used properly.
Type 1: replace kill command with enable/disable. At POS, RFID product tags are disabled after payment and newly generated random password is written to the tag. The new passwords are printed on the receipts. If the tags are to be used later, they can be re-enabled by the passwords. In addition, with correct password, disabled tags will not reply to any reader request.
Type 2: use a challenge response method to verify a password, based on a typical cryptographic one-way function. This is to defeat sniffing practices on high value goods. Both of these two enhancements may drive the cost higher. Authors believe that one common password makes life easier for consumers. Password printouts don't increase transaction cost.

160. Spiekermann, Sarah, E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior, Proceedings of ACM conference on electronic commerce, oct 2001

161. Spiekermann, Sarah. Stated Privacy Preferences versus actual behaviour in EC environments: A Reality Check, Proceedings of the 5th International Conference Wirtschaftsinformatik (Business Informatics) - Finanzdienstleistungen (Information Systems in Finance) WI-IF 2001

162. Stapleton-Gray, R., "Scanning The Horizon: A Skeptical View Of RFIDs On The Shelves," Stapleton-Gray & Associates, Inc., Nov 2003

The author suggested that the envisioned benefits of using RFID in retail commerce may be less than anticipated. Some of the arguments are:
- Tag reads are less than 100% reliable and performance of readers and tags in real-world environment "perhaps more an art than a science",
- RFID-checkout makes sense when all products sold are tagged and, all tags function successfully and, customers can't easily defeat the tags,
- Significant consumer resistance to post-purchase RFID tags will hurt retailers,
- Problems like shrinkage reduction that RFID might solve can also be solved by other solutions (eg, enhance the current video surveillance),
- Various parties across the supply chain have varying interests

"Examples of RFID across supply chain assume a willingness and disregards a much more complex economy for information."

163. Stapleton-Gray, Ross. Scanning the horizon: a skeptical view of RFIDs on the shelves,

RFID Applications, Security and Privacy, Addison Wesley, March 2005.

164. Stewart, B., "The Economics Of Data Privacy: Should We Place A Dollar Value On Personal Autonomy And Dignity?," The 26th International Conference of Privacy and Data Protection Commissioners, Wroclaw, Poland

To strike a balance between free flow of information and protecting privacy is difficult because economic costs can always associate with a monetary value while privacy is not. Data protection and privacy commissioners should strive for cost effective regulations while not making privacy undervalued. The OECD guidelines explicitly recognize uncoordinated domestic legislation can hinder trans-border data flow. Interests in privacy are not absolute and must be weighed, with complementary and associated interests, against competing public and private issues. The author talked about the Cost benefit Analysis (CBA) in data privacy regulation and suggested that it's certainly able to put monetary figures upon some of the costs of complying with data privacy law but it's difficult to quantify the benefits in monetary terms. CBA is used as part of the evaluation of proposed data matching programmes in New Zealand. To conclude, the author states:

- the international instruments on data privacy were premised upon reconciling the need for human right(privacy) and the need to avoid unwarranted barriers to transborder data flows,
- the international approach is implemented in national data privacy laws. This costs money but strike for a balance between privacy and competing public interest,
- commissioners should seek for ways to implement data privacy laws in a cost effective way.

165. Stockman, Harry. Communication by means of reflected power, Proceedings of the I.R.E. Oct, 1948

166. Stufflebeam, W., Antón, A., He, Q., Jain, N., "Specifying Privacy Policies With P3P And EPAL: Lessons Learned," 3rd ACM Workshop on Privacy in the Electronic Society, October 2004

P3P is a semi-structured privacy policy specification language that allows an organization to specify its website privacy practices in a machine-readable format. EPAL is an IBM project that's developed mainly as a business-to business technology to help streamline information flows during business interactions. Like P3P, EPAL policies also contain meta-information that does not specifically address information access and usage. The authors reported that

- In contrast to EPAL, P3P does allow one to specify whether or not there is a recipient. Because information recipients are relevant to information systems and transactions, P3P helps to ensure that relevant recipient data was expressed on the statement,
- Both P3P and EPAL are insufficient for specifying high-level company obligations,
- P3P has limited scope as a public privacy policy specification language,
- P3P cannot express "effective On" dates

167. SUN Microsystems, "Sun's XACML Implementation," SUN Microsystems, Jul 2004

XACML is an OASIS standard access control policy language. SUN's implementation of XACML is a set of Java classes. This guide introduces the XACML standard and how to build XACML support into applications.

168. Swaminathan, Jayashankar M. Modeling the dynamics of supply chains, Proceedings of the AAAI-94 Workshop on Reasoning About the Shop Floor, August 1994

169. The Under Secretary of Defense, "Radio Frequency Identification (RFID) Policy," DoD, Jul 2004

    Business rules for passive RFID: 860-960MHz range, accepts both EPC tag data constructs and DoD tag data construct. Case, pallet and item packaging for Unique Identification items will be tagged at the point of origin except for bulk commodities (sand, gravel, bulk liquid, ready-mix concrete, coal and agricultural products). If the unit pack for UID items is also the case, only one RFID tag will be attached to the container. Minimum read range is 3m (didn't say anything on environment), DoD accepts EPC class 0 (64-bit read only, 96-bit read only) and Class 1 (64-bit read-write, 96-bit read-write). Commence date was on 1st of Jan, 2005.

170. ThinkMagic, "Elements Of An RFID System," ThinkMagic

    In this presentation file, there includes a brief RFID history, tag anatomy, frequency ranges, reader block diagram. Picture of the circuit board of a reader, communication model of passive systems and a calculation shows that 19.4m is the theoretical maximum read range for UHF systems.

171. Tippins, M., Su, W., "The Implications Of Mismatching Organizational Decision-making And Communication Structures Within US Retail Firms: The Role Of Scanner Data," International review of retail, distribution and consumer research, 14(2), Apr 2004, 241-253

    In large retail organizations, corporate buyers and store managers are considered to be interdependent. Somehow, there are potential conflicts as well. Three specific ones are goal incompatibility (store managers concentrate on customer's buying habits while corporate buyers concentrate on aggregated performance of multiple stores, getting the best quantity discount), domain dissensus (store managers believe they should have a greater merchandising decisions) and perceptual difference of reality (store managers and corporate buyers have different interpretations regards poor store performance). By investigating both the decision flow and the information flow, the paper suggests that a decentralized decision making structure with a decentralized communication structure minimizes intra-firm conflicts.

172. Usami, M., "An Ultra-small RFID Chip: μ-chip," 2004 IEEE Asia-Pacific Conference on Advanced System Integrated Circuits(AP-ASIC2004), Aug 2004

    The μ-chip is 0.4mm x 0.4mm, with RF antenna (made of gold) built-in RFID chip made by Hitachi. Max communication distance is 1.2mm. It has 128-bit memory and works at 2.45GHz

173. van Eeden, Hendrik. Reader talks first vs tag talk first RFID protocol, whitepaper,

iPico Identification, 2002

174. Vogt, H., "Efficient Object Identification With Passive RFID Tags," In International Conference on Pervasive Computing, Zurich, 2002

This paper investigates the stochastic approach for tag anti-collision (used in HF systems). In the presence of multiple tags, multiple read cycles have to be performed in order to achieve a high recognition rate. Somehow, if the number of reads is too many, this will induce a high delay and cause poor user experience (as in supermarket checkouts). If the number of reads is too few, some tags may be missed. The author found that, the optimal value for number of read cycles varies with the reader- changeable Framed-Aloha's frame size N and the actual number of tags n. Author demonstrated a way to compute the optimal frame size N for a given number of tags n under a desired assurance level. In real life implementation, the assurance was not able to achieve the desired value and author suggested that it may be related to environmental influences.

175. Want, Roy "Enabling Ubiquitous Sensing with RFID," IEEE Computer, April 2004

176. Want, R., "The Magic Of RFID," ACM Queue (2) 7, Oct 2004

Passive tags are usually powered by magnetic induction up to 100MHz. Load modulation is the changing of current in the tag's coil, in a defined manner, over time. Near field is the region within which the tag's coil intersects with the magnetic field lines of the reader coil. Beyond this is the region called far field where energy breaks away from the antenna as propagating waves (radio signal). The boundary of near field and far field is governed by the system frequency, eg, 3.6m for 13.56MHz and 6cm for 915MHz. This is theoretical and magnetic field strength falls off fairly rapidly. Energy declines at 1/d3 for near field and 1/d2 for far field. When it drops to below certain level, the tag will not be able to derive enough energy to power on. One way to increase the reception is to use a larger coil. In practice, most 13.56MHz systems operate between 1 to 30cm, considerably shorter than the near field limit. To overcome the range problem in UHF systems, the tag does not use load modulation anymore. Instead, it uses radio frequency backscatter. By varying the antenna impedance in a meaningful manner, some of the RF energy from the reader will be reflected. The reader receives this reflection and decodes the ID from the reflection pattern. Author suggested one way to accommodate the multiple standards is to build multi-protocol readers. With the power requirement drop in the tag's semiconductor and higher sensitivity receiver designs, it is expected that the read range will increase. The next major hurdle is the software systems needed to manage RFID-based inventory control.

177. Weinberg, Jonathan. RFID and privacy, Oct 2004, http://ssrn.com/abstract=611625

178. Weis, S., Sarma, S., Rivest, R., Engels, D., "Security And Privacy Aspects Of Low-cost Radio Frequency Identification Systems," Security in pervasive computing 2003, Lecture Notes in Computer Science 2802, Springer-Verlag 2004, 201-212

Three security proposals (hash-based access control, randomized access control, silent tree walking and backward channel key negotiation) were discussed.

Hash based access control works in the way that there is a portion of memory of the tag is used to store a temporary metaID. Upon receiving the metaID value, the tag enters its locked state. The tag owner stores both the random key and metaID in a backend database. To unlock a tag, owner queries the metaID from the tag and looks up the appropriate key and transmit the key to the tag. The tag hashes the key and compares it to the stored metaID. If the values match, it unlocks itself and opens full functionality to any reader nearby. Tags may still function as object identifiers while in locked state. Tracking of individual is possible. In randomized access control, tags do not respond predictably to queries by unauthorized readers. Tags have to equip a random number generator. In replying a reader's query, tag sends back with a pair (r, h(ID||r)) where r is chosen randomly. A legitimate reader performs a brute force search of its know IDs, hash each of them with r until it finds a match. This method is feasible for relative small number of tags.
Silent tree walking and backward channel key negotiation: the asymmetric signal strength makes eavesdropping possible from a long distance. It's possible to derive tag contents by monitoring the reader signals if the binary tree walking algorithm is used for tag singulation. Assuming a group of tags sharing the same prefix ID, the authors proposed a silent tree walking on two bits scheme (using XOR on 2 consecutive bits).
Other measures to strengthen RFID system are:

- deploying read detectors to find out unauthorized reads or attacks,
- use a reserved frequency for tags to "scream" when killed,
- enable users to access full tag functionalities after purchase,
- readers should reject tag replies with anomalous response times or signal power levels,
- employ frequency hopping to avoid session hijacking (because passive tags can be designed to follow reader frequencies)

179. Wheeler, David. TEA, a tiny encryption algorithm, Computer Laboratory technical report, Cambridge University, Nov 1994
180. Wienberg, J., "RFID And Privacy," (10/18/2004 draft), Versions of this paper are forthcoming as chapters in Securing Privacy in the Internet Age, from Stanford Univ. Press, and RFID: Applications, Security, & Privacy, from Addison-Wesley

    The author identifies profiling, surveillance and "action threat" are possible privacy issues related to RFID. It's easy to imagine RFID tags with sophisticated access controls but current inexpensive RFID tags don't incorporate such a feature. The author suggests the simplest yet most effective way is to require tags to be clearly labeled and can be removed easily.

181. Williams, J., "Can A "social" Protocol Help Protect Web Privacy?," Georgetwon University Law Center, Nov 1998

    P3P is a social protocol because it's created for people to express preferences rather than for network performance. P3P negotiation is single round only. The aim is to lessen the burden of users to read confusing and vague privacy statements of a web site. P3P is not a silver bullet and it does not provide any enforcement mechanism.

182. WJ Communications Inc., "Programming Tags With The MPR Series RFID PC Cards," RFID application note, WJ Communications Inc., Dec 2004

This is a concise description of EPC tag states (unprogrammed, programmed, locked, killed) and commands (Write, verify, erase, lock). In the unprogrammed state, the contents are set to zeros after executing the Erase command. When data with valid CRC has written to the tag, the tag enters its programmed state. In programmed state, the tag can responds all commands, including the Class 1 Verify command which reports the CRC and passcode sections of the tag contents in addition to the EPC. Tags become Locked when 0xA5 is written to the last byte of its memory. Once locked, tags will not respond to any programming commands. With matching CRC, a tag can be killed by the Class 1 Kill command. "A killed Class 1 tag will not reply to any commands and cannot be revived."

183. Yang, G., Jarvenpaa, S., "Trust And Radio Frequency Identification (RFID) Adoption Within An Alliance," IEE proceedings of the 38th Hawaii International Conference on Systems Sciences, 2005

RFID is a newly emerged interorganizational system (IOS). Previous studies on IOS were concentrated on relationships with unbalanced power and influence and this paper investigates the case where partner relationships are balanced. The focus was on the contractual alliance type where group members work together to accomplish a collective task without any share of ownership or administrative structure among them. There are two forms of trust, experience-based and category-based (where the existence of salient social categories within a group has an important influence for group members' beliefs, attitudes and perceptions about each other. (reading not finished yet)

184. Zebra Technologies, "Managing The EPC Generation Gap," Application white paper, Zebra Technologies, 2004

This paper describes the differences of tags in reality and the EPCglobal specification. For example, EPC Class 1 tags are supposed to be write once read many but in reality, vendors create "Class 1-compliant" which is read write many. A table summarizing the differences between Gen 1 and Gen 2 tags is given. It states that Gen 2 has a upper frequency of 960MHz (it's 930MHz in Gen 1), memory capacity of Gen 2 ranges from 96 to 256 bits (it is 64 to 96 bits in Gen 1).

185. Zebra Technologies, "Zebra's RFID Readiness Guide: Complying With RFID Tagging Mandates," Application white paper, Zebra Technologies, 2004

This document states that shipping errors cost between $60 tp$250 to resolve and RFID can help to increase shipment accuracy. In addition to a new way for data collection, RFID opens opportunities to explore benefits of having ID data and ID-event related data (time, location). For RFID implementations, testing may not reveal every hurdle but can be overcome by thorough planning. A clear understanding of requirements and options is pre-requisite

186. Zhou, F., Jin, D., Huang, C., Hao, M., "Optimize The Power Consumption Of Passive Electronic Tags For Anti-collision Schemes," Proceedings of the 5th International ASIC conference, Oct 2003

The authors proposed a new anti-collision scheme by considering at both the protocol and circuit levels together. Binary-tree, query-tree and the proposed improved-query-tree anti-collision schemes were explained and compared. From cost functions, it concluded that their improved-query-tree is better than the other two.