ICEB 2008 Proceedings

International Conference on Electronic Business (ICEB)

Fall 9-30-2008

A Relationship-Based Acess Control Model for On-demand Privacy and Security Entitlement in RFID-enable Supply Chains

Sung Chi Chu

Waiman Cheung

Timon C. Du

A Relationship-Based Access Control Model for On-demand Privacy and Security Entitlement in RFID-enabled Supply Chains

Sung Chi Chu, The Chinese University of Hong Kong, Hong Kong, scchu@baf.msmail.cuhk.edu.hk
Waiman Cheung, The Chinese University of Hong Kong, Hong Kong, wcheung@cuhk.edu.hk
Timon Du, The Chinese University of Hong Kong, Hong Kong, timon@baf.msmail.cuhk.edu.hk

Abstract

RFID adoption in supply chains is both viable in gaining on-target end-to-end visibility and crucial to sustain competitiveness. RFID-based information flow will cut across partners in business chains that extended beyond borders. Privacy and security preferences (PSP) are manifested when supply chain parties are sharing (EPC-RFID-based) data to gain visibility. The role of each party cannot be singly used to determine the preference of either party to derive the necessary entitlement for the requesting party. The preference-based entitlement must ensure data sharing is privacy-protected and security-enforced.

In this research, a Relationship-Based Access Control (ReBAC) model is proposed for on-demand privacy and security entitlement in RFID-enabled supply chains. The model includes two key concepts: on-demand preference and privacy and security scheme. Preference is governed by the two parties' relationship, and the scheme is driven by the data dimensions (i.e., data sensitivity, data location and data ownership). RBAC is capable of addressing one party's need to gain pre-determined permissions according to role assignment or activation. The relationship-based approach is on-demand, two-party, relationship-based preference to gain entitlement (for visibility services) with scheme-enabled privacy and security activation.

Keywords: RFID, Privacy and Security, Supply Chain

1. Introduction

The adoption of RFID technology will be extensive, both in scope globally and in participation among industries. RFID-based information flow will cut across partners in business chains (e.g., supply chains and logistics service chains) extended beyond borders. The impact of the RFID technology on e-business can be broadly identified in three aspects:

1. Effective Information Sharing. The data offered by a RFID tag with a single unique identity (SUI) enable effective information sharing with consistency and accuracy among collaborative partners, used individually to improve efficiency, and at the same time used collectively in business chains to achieve greater visibility.
2. Global Information Infrastructure. Some form of global information infrastructure must be reached, e.g., the EPCglobal network, to serve as a neutral information platform – to ensure uniformity and interoperability in RFID-based information exchange [1][8].
3. Effective Managed Information Flow. The new security and privacy concerns stemmed from the SUI-guided information flow among partners must be managed and protected without compromising trade secrets, and managed and accessible without exposing sensitive corporate data and information.

The on-demand capability concept of trading partners sharing RFID-based data and information without compromising individual privacy and security is crucial to the success of RFID adoption in business chains. The objective of the project is to enable on-demand data sharing in RFID-enabled supply chains with no inherent privacy and security issues. The objective is ascertained with the the new Relationship-Based Access Control (ReBAC) model with two key components:

1. to develop concept and model of the ReBAC which dissolves both privacy and security concerns for any two supply chain partners sharing RFID-based data,
2. to develop preference determination method based on roles of the data sharing parties and their relationship. The method will be called upon every-time when sharing is initiated, and,
3. to formulate privacy and security scheme which on one hand, helps supply chain partners to carefully place RFID-based data at EPC network and on the other hand, facilitates entitlement determination.

2. Literature Review

RFID and EPC Global

RFID is an automatic identification system that uses radio frequency technology in product tags. The advantages of RFID tags are that, unlike printed barcodes, they do not need a direct "line of sight," and multiple tags can be identified in a short time (from tens to hundreds per second). Moreover, the tags are resistant to dirt, have a large amount of unique identifiers, and can be read (and written) by readers without being visible. However, the disadvantages are that the signals that are transmitted from the tags can be read by other equipment within range, and interference can occur when more than one reader is transmitting or more than one tag is responding. Possible consumer privacy issues are also a concern.

The encoding scheme for RFID tags refers to the Electronic Product Code (EPC), which is an identification scheme for the universal identification of physical objects. The EPCglobal Network [10], which was developed by the Auto-ID Center (now called Auto-ID Labs) to manage the EPC, includes a physical layer that captures the location of a tag and other information, and an information layer that provides the name service, such as the object name service (ONS) and the EPC Discovery Service (EPCDS) [27]. The ONS was introduced by the Software Action Group of EPCglobal (using technology that was transferred from the Auto-ID Center; www.epcglobalinc.org) and the Auto-ID Center to map RFID codes to the network addresses of the services that contain the actual data. The ONS is similar to the domain name service on the Internet, and has a hierarchical structure. An inquiry is sent to the Root ONS to locate the data owners, and the query is then re-directed to the Local ONS of the data owner, and data can be retrieved from the local EPCIS[1] (ECP Information Service). In January 2004, VeriSign (www.verisign.com) was selected by EPCglobal to operate the Root ONS.

Privacy Protection, RFID Tags and RBAC

Privacy can be viewed as a state or condition of limited access to individuals [29]. From an information perspective, privacy deals with the proper use of what information, while security ensures the access to information is as intended. Traditionally, these issues have been studied for users of offline nature [20][32]. Online information privacy concerns have also been studied [21][30]. As RFID-tagged products reach the consumption point, privacy concerns of consumers will be of different nature. Minimal encryption techniques can be applied, or the tag can be 'killed' or selectively 'blocked'. Consumer privacy issues are also a concern [22]. Before the product reaches the market, the business processes involved from raw materials to finished products in a business chains interact across corporation boundaries. Privacy issues across corporate boundaries differ to those of consumers, and those within a corporation: consumers' concern is of case by case in an individual basis, while corporation is of a business unit's decision among departments with a well-defined goal, versus, ad hoc or partnership decision to share with a party outside of the corporate boundary in a business chain.

To observe the right to privacy, countries or regions define their own guidelines according to their cultures. A comprehensive guideline that comprises eight privacy protection principles that has been endorsed by 30 countries can be found in [23]. Privacy protection guidelines were issued by the Organization for Economic Co-operation and Development (OECD) as early as 1980 to protect privacy and the trans-border flow of personal data.

We have looked at seven privacy protection guidelines for personal data from around the world (US, Canada, Hong Kong , Australia, Singapore, Japan, and OECD), and found these guidelines are based principally on all the eight principles. They are, 1) Collection limitation, 2) Data quality, 3) Purpose specification, 4) Use limitation, 5) Security safeguards, 6) Openness, 7) Individual participation, and 8) Accountability. These principles are useful in terms of identifying differences when considering privacy related to RFID-based data sharing.

RSA Laboratories has considered privacy issues in the air protocol [16], and the RFID systems [17]. "RFID

Privacy" was also addressed as threats as information is being shared with other enterprises, and technical solutions were proposed with respect to the control of data already on the tag, rather than what information should be stored on tag [13].

3. The Relationship-Based Access Control (ReBAC)

RFID adoption in supply chains is both in gaining on-target end-to-end visibility and crucial to sustain competitiveness. Pilot studies project the many benefits of using RFID technology in supply chain processes of a trading party with implication to foreseeable gains of both upstream and/or downstream partners. The adoption of this unique identification technology provides a pivotal (e.g., using EPC) mark to aggregate (sticky-glue) data of an item, a carton, to a shipment. Supply chain visibility at different levels can now be offered with clarity and minimal information latency. This and the possible synchronization of information, physical and financial flows in a supply chain are crucial to sustain status quo of supply chain practices, competitiveness among supply chains, and move towards supply chain supremacy in adaptability, alignment, and agility.

However, the growth in the use of RFID which enables the unique identification of objects and invisible tracking, has given rise to increased concern about the invasion of privacy. To end consumers, notable privacy threats such as leaking information pertaining to personal property and tracking the consumer's spending history and patterns and physical whereabouts have been raised. In a supply chain, privacy and security issues of partners are of a different nature with multi-dimensional characteristics. The issues are of two-party, relationship-based, and on-demand with data characteristics of locations, sensitivity and ownership.

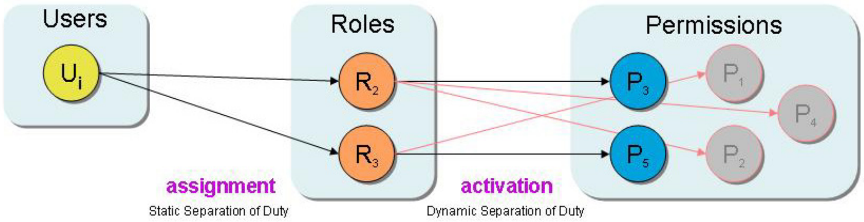

Figure 1. Role-Based Access Control (RBAC) Structure

Role-Based Access Control (RBAC) [12] as proposed in the literature alone is not sufficient to address the on-demand preference and privacy and security scheme issues. Role-based access control (RBAC) applies policy based solely on the role of a user at the time of accessing a data source. Roles are pre-determined. Role-permission can be activated to avoid conflicts (See Figure 1). For RFID-based data and information sharing between supply chain participants access policy is applied base on their relationship of which the role of the requesting side is only one of many attributes. The access policy is further determined by other relationship attributes such as long-term vs. one-time, dominant vs. causal as well as the parties' dual willingness to share. The relationship needs to be determined at the time of sharing as it changes over time even when data requestor's role remains unchanged. Hence, the one-party, pre-determined, role-based access control is not applicable to two-party, derived on demand, "relationship-based" access control requirement for sharing RFID-based data.

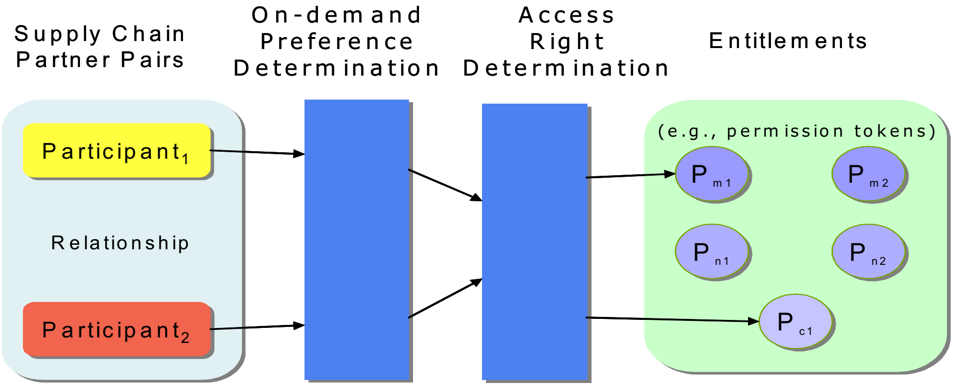
Supply Chain Partner Pairs
On-demand Preference Determination
Access Right Determination
Entitlements
Participant1
Relationship
Participant2
(e.g., permission tokens)
Pm1
Pm2
Pn1
Pn2
Pc1

Figure 2 Relationship-Based Access Control (ReBAC)

The proposed Relationship-Based Access Control model (See Figure 2) addresses two fundamental issues: 1) the on-demand preferences are manifested when two parties are sharing data to gain visibility. The role instances of these parties, other than as that inhered in supply chain participation (e.g., buyers, sellers, manufacturers and logistics service provider), are defined by the relationship (e.g., partnership, alliances, third-party agent) of the parties with respect to the request of data sharing., and 2) the privacy and security scheme that leads to the definition of access rights to the visibility services, or more specifically, the data and information needed. The scheme allows the consideration of the data characteristics with respect to its location, sensitivity and ownership. Via the scheme, an entitlement can be reached that is both privacy-protected and security-ensured

As data can be obtained from different sources, some aggregation of the data is necessary (that is why the use of services to encapsulate both the data and the visibility rules). Thus, on-demand privacy and security entitlement is crucial in facilitating data and information sharing of trading partners in RFID-enabled supply chains. Achieving real-time visibility for partners as such information and physical flows are timely synchronized, even to the unique item level.

4. Developing the On-demand Preference Model

A Role-based Access Control (RBAC) model (as shown in Figure 1) is to allow a coordinated view of how access control can be activated and maintained with respect to the role of the requestor at the time of request, rather the actual person as he or she could assume different roles (research director and professors) in different environment (research center and department) of the same organization (a research university). In a supply chain context, the implication is a bit more complex and of a different perspective. For example, we must consider: 1) the requestor's role which is determined with respect to his organization's role (distribution center) in the supply chain, 2) the organization or the partner in the supply chain that is the information granter (not provider), 3) the visibility service requested (such as outbound logistics schedule of EPC 2091), and 4) the (supply chain) relationship between the grantor and the requestor. There are other factors and it is our attempt in this research to conceptualize these aspects and proposed a framework to view the data sharing privacy and security issues in a RFID-enabled supply chain.

A Relationship-Based Access Control (ReBAC) model will be proposed (See

Figure 3). The model articulates the need to derive on-demand preference when the relationship of the two parties is manifested for data sharing. The scheme guides the determination of entitlement based on the role instances and data characteristics for the visibility session.

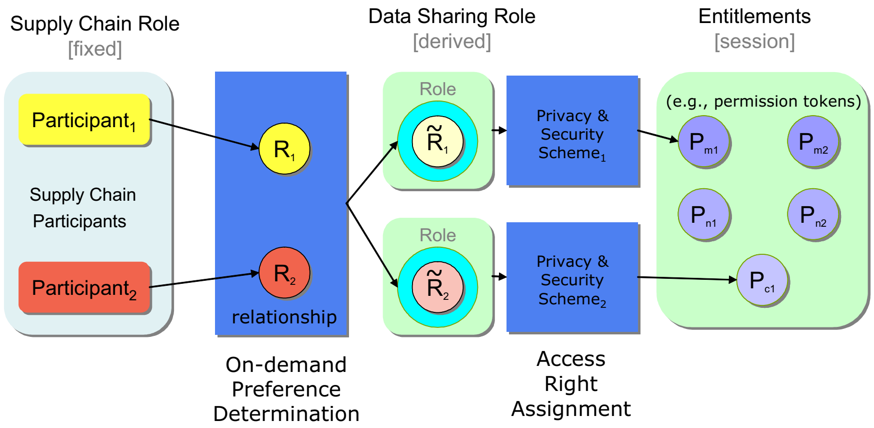

Figure 3. Relationship-Based Access Control (ReBAC) Struture

We need a mechanism for a partner to specify the privacy preference of data sharing such that appropriate access control or authentication can be effected. The Platform for Privacy Preferences (P3P) provides an insight for, in this case, how to 'specify' preferences for website to collect personal information of any user [27]. The dominancy is the website where a website defines what data will be collected during online usage, and the user can, based on the information, opt out on certain data collection [12]. E-P3P is an enterprise privacy preference proposed by IBM to enforce privacy protection, enabling audit trailing to allow accountability from a management perspective [1]. Data sharing among partners can be ad hoc and not restricted in the browser environment (the user of a website can choose options with an enabled browser). We have a preliminary view of what is needed in the supply chain participant's privacy preference as follows:

P3P	SAML/XACML	To Be Proposed Privacy Preference Templates
Expresses privacy policies that human users can understand	Expresses (the same) privacy policies that computer systems can enforce them (in terms of computer access control mechanisms)	Express privacy policies that computer systems can enforce them in *different locations* and *among different relationships manifested by partnerships*
Policies at a generalized high level, in generic user and data category terms	Policies in terms of specific data resource identities or system-assigned resource descriptors. Policies are fine-grained and in applicable form inside computer systems	Different hierarchies of data resources will be defined similarly for supply chains and logistics; policies must be addressable in different levels of granularity
Expresses only privacy policies	Expresses, in addition to privacy policies, policies for any type of access to resources (e.g., deny or permit)	Privacy policies must be expressed to allow access control to be generated and can be enforceable accordingly for that partnership, that time frame, and that location of the data

5. On-Demand Preference Determination

The on-demand preference determination is mainly based on three key parameters, namely data location, data sensitivity and data ownership.

Data Location. An RFID tag is a good medium to carry and collect data that needs to be shared among supply chain participants. A typical tag contains an EPC which has four segments, and in many cases, additional memory. To create an RFID-enabled supply chain, we adopt the EPCglobal Network to the supply chain operating environment leading to an IT architecture. According to the EPCglobal Network, there are three locations where RFID-related data are stored, namely, global and local EPC-IS [9] repositories and RFID tag. In a typical supply chain, data shared among partners are facilitated by an information infrastructure consists of an extranet and/or an intranet. We propose five data locations: RFID tags, the Internet EPC-IS (global EPC-IS), the Extranet EPC-IS (local EPC-IS), the Intranet EPC-IS (local EPC-IS), and corporate databases.

Data carried in RFID tags is vulnerable in nature, even though encryption can be applied to protect the data [18][3]. Data that are stored on the Internet EPC-IS are designed to be accessible to the public, but the data that are associated with RFID and are shared by supply chain partners on the Extranet EPC-IS and Intranet EPC-IS are for internal use only. Corporate databases are likely re-designed to house RFID-related data; while non-RFID-related data are shared using conventional approach by supply chain partners – this is not a focus of this study.

Extranet is central to data sharing of partners in a supply chain, and it is not intended for external access such as the consumers. Consumers access EPC related information via the Internet EPC-IS such as the EPCglobal Network. The EPCglobal Network, as it is now designed, is a two-tier design with global EPC-IS and local EPC-IS. When this EPCglobal Network is imposed/applied to an RFID-enabled supply chain, local EPC-IS is necessary in the Extranet (i.e., Extranet EPC-IS, or 'EPC Extranet') and in the Intranet (i.e., Intranet EPC-IS). Further research is needed to this new approach. For example, the issue of a three-tier (Internet, Extranet, and Intranet EPC-IS) design of the EPCglobal Network is necessary and the scalability should also be considered accordingly.

Consumers access data stored in Intranet EPC-IS via the Internet EPC-IS with an EPC obtained from an RFID tag. The Internet EPC-IS using the discovery services locates the local EPC-IS in the intranet (Intranet EPC-IS) where consumers' owned data are stored. Highly sensitive data are not for sharing but must be accessible to the owner according to the privacy ordinance. The discovery services as prescribed in the EPCglobal Network are modeled with respect to web services. Extranet is designed for supply chain facilitation and not for parties outside of the supply chain such as the consumers.

Data Sensitivity. Data sensitivity is determined by the potential use of data (open-restricted), their association with the data subject (public-private), and the properties of data (general-specific). Data that are specific and created for internal use are highly sensitive, and therefore belong at the top of the sensitivity pyramid. A checklist can be usefully employed to carry out an analysis of data sensitivity. For example, if the data are related to personal information, then they are very sensitive; if the data can be used to identify the associated subject, then they are sensitive; and if the data are aggregated, then they can be shared without revealing individual information and are therefore less sensitive. Furthermore, the more specific and detailed the data, the more sensitive they are, especially from a product design perspective.

Through such an analysis, data can be categorized into different degrees of sensitivity, such as Highly Sensitive (HS), Sensitive (S), and Less Sensitive (LS). HS-type data are related to personal or corporate trade secrets and are not shared with outsiders; S-type data are sensitive data but can be shared with selected partners or interested parties; and LS-type data are data with low sensitivity or none that are open to outsiders by design. Thus, the determination of where data should be stored depends on the sensitivity of data, the vulnerability of the media, the nature of the data, and the efficiency of a supply chain. Intuitively, both RFID tags and Internet EPC-IS should carry only S- and LS-type data, whereas corporate databases can carry any of the data types. This is because the tags, Internet, and corporate databases are exposed to different security risks and thus have different levels of vulnerability.

Data Ownership. The owner of a RFID tag is generally the data collector who possesses the tag. However, the tag owner does not necessarily own the data written on the tag. As RFID tags are moved across the supply chain, any partner (end users) can write data on the tags, and as a result, becomes the owner of that particular piece of data. Multiple data ownerships can be found on a RFID tag. Data on tags are readable but not necessary understandable without the proper decoding privilege. It is important then to distinguish tag ownership from data ownership. The tag owner, or the data collector, has the obligation to protect the privacy of the data owners. The data owner on the other hands is responsible for the correctness of the piece of data they write. As a tag is vulnerable for damage, all owners should take proper precaution to ensure tag's data integrity. In addition, there is another type of end users who are pure data users. Consumers are likely of that type, using data on the tag and/or obtain more information from Internet EPC-IS with the EPC on the tag.

The level of sensitivity of RFID-based (object related) data is determined by the data owner/data administrator. We agree that sensitivity is a challenging issue as we identify initially three dimensions to be considered. It is difficult to know how and when data should be shared in a supply chain and each requires a separate research effort. We conduct a preliminary research on the factors of willingness to share. We devise a procedural checklist for data administrator to determine data sensitivity and the locations; and accordingly varying schemes for access control can be designed. In this study, schemes are proposed as a guideline for a partner to determine/develop preferences of data sharing based on sensitivity, location, partners and partnership. Each partner can have individual and likely different preferences with respect to the same data due to their perception of data sensitivity and willingness to share.

6. Proof of Concept

Use cases will be used to gain an in-depth understanding of the applicability of a proposed model. Specifically, we want to assess the functionality of the two key components of the proposed model. Two use cases, based on current supply chain practices in the garment industry, will be developed in this research. The candidates for the use cases are a trim and accessories manufacturer, and a local garment enterprise (60 years in business) with OEM manufacturers in China and other Southeast Asian countries. We have worked with these parties in current RFID-based research projects (a complete RFID-enabled supply chain in the garment industry, from trims to retail stores, and RFID adoption practice in the garment industry using SCOR as the modeling tool respectively). Briefly, the use cases are described here:

1. RFID adoption in distribution from the perspective of a manufacturer: RFID tags will be used in the carton-level, and multiple cartons are common for each order; data and information sharing will be among brand name owners, the OEM manufacturers of some brand name owners, local logistics service providers (in Hong Kong and in Dongguan), and customer service offices.
2. RFID adoption in manufacturer-to-forwarder from the perspective of an enterprise serving brand owners, corporate owners and catalog owners, e.g., Brooke Brothers, JCPenny, and Lands' End. Manufacturing plants can be found in Taiwan, China and Vietnam. The enterprise has their own fleet of trucks to make deliver from plants in China to Hong Kong forwarders' warehouses for FOB shipment to their clients. RFID tagging will be at the carton- and pallet-level;

We will borrow from other practitioners in other supply chains and logistics services providers to enrich the data sharing scenarios.

References

[1] Backes, Michael et al. Efficient comparison of enterprise privacy policies, Proceedings of the 2004 ACM symposium on Applied computing, 2004

[2] Bacon, J., Moody, K., and Yao, W. "A Model of OASIS Role-Based Access Control and Its Support for Active Security," ACM Transactions on Information and System Security, 5 (4), November, 2002, pp 492-540

[3] Bailey, D.V., and Juels, A. "Shoehorning Security into the EPC Standard," 23 January 2006, http://www.rsasecurity.com/rsalabs/node.asp?id=3048

[4] Cohen, J.E. "DRM and Privacy," Communications of the ACM 46 (4), April 2003, 47-49.

[5] Damiani, M.L., Bertino, E., Catania, B., and Perlasca, P. "GEO-RBAC: Spatially Aware RBAC," ACM Transactions on Information and System Security (TISS), 10 (1), February, 2007.

[6] Du, T., M. Wong, W. Cheung, and S.C. Chu, "A Privacy and Security Framework for the EPC Network Infrastructure," BA Working Paper Series no. WP-06-02, The Chinese University of Hong Kong, 2006.

[7] Engels, D., EPC-256: The 256-bit Electronic Product Code™, Representation, *Auto-ID Center Massachusetts Institute of Technology Technical Report*, February 1, 2003.

[8] EPCglobal, EPC^{TM} Radio-Frequency Identity Protocols: Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, Version 1.0.9, January 2005

[9] EPCglobal, EPC Information Services (EPCIS) Version 1.0 Specification, ratified standard, April 12, 2007 (http://www.epcglobalinc.org/standards/epcis/epcis_1_0-standard-20070412.pdf; visited August 28, 2007)

[10] EPCglobal, "EPCglobal Architecture Framework", Final Version, 1 July 2005, (http://www.epcglobalinc.org/standards/architecture/architecture_1_0-standard-20050701.pdf; visited August 28, 2007)

[11] EPCglobal, *EPCTM Tag Data Standards Version 1.1 Rev.1.24, Standard Specification*, 01 April 2004, (www.epcglobalinc.org).

[12] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., and Chandramouli, R. "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, 4 (3), August 2001, pp 224–274.

[13] Garfinkel, S.L., Juels, A., and Pappu, R. "RFID Privacy: An Overview of Problems and Proposed Solutions," IEEE Security & Privacy, May/June 2005, 34-43

[14] 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

[15] Jajodia, S., Samarati, P., Sapino, M. L., and Subrahmanian, V.S., "Flexible Support for Multiple Access Control Policies," ACM Transactions on Database Systems 26 (2), June 2001, 214-260.

[16] Juels, A., and Weis, S.A. "Defining Strong Privacy for RFID," 7 April 2006, http://www.rsasecurity.com/rsalabs/node.asp?id=3046

[17] Juels, A. "RFID Security and Privacy: A Research Survey," 28 September 2005, http://www.rsasecurity.com/rsalabs/node.asp?id=2937

[18] Juels, A., Rivest, R.L., and Szydlo, M. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," CCS'03, October 27-30, 2003; http://www.rsasecurity.com/rsalabs/node.asp?id=2060

[19] Karimi J., Somers T.M., Gupta Y.P., "Impact of Environmental Uncertainty and Task Characteristics on User Satisfaction with Data", Information Systems Research 15 (2), 175-193

[20] Laudon, K., Markets and privacy, *Communications of the ACM***,** 39, 9, (September 1996), 92-104.

[21] Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research 15 (4), 2004, 336-355.

[22] McGinity, M., RFID: is this game of tag fair play? *Communications of the ACM***,** 47, 1, (January 2004), 15-18.

[23] Monczka R.M., Peterson K.J., Hanfield R.B. and Ragatz G.L., "Success Factors in Strategic Supplier Alliances: The Buying Company Perspective", Decision Sciences, Summer 1998, 29, 3, 553-577

[24] OASIS, eXtensible Access Control Markup Language (XACML) version 2.0, Dec 2004 (http://www.oasis-open.org)

[25] OASIS, Security Assertion Markup Language (SAML) version 2.0, 15 Mar 2005 (http://www.oasis-open.org)

[26] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002, Organization for Economic Co-operation and Development, www.copyright.com.

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

[28] Regan, P., *Legislating privacy: Technology, social values and public policy*, Chapel Hill: Uniersity of North Carolina Press, 1995.

[29] Schoeman, F., *Philosophical dimensions of privacy*, Cambridge: Cambridge University Press, 1984.

[30] Sheehan, K.B. "Toward a Typology of Internet Users and Online Privacy Concerns," The Information Society 18, 2002, 21-32.

[31] Uo, Y., Suzuki, S., Nakamura, O., and Murai, J. Name service on the EPC network, *Auto-ID Labs Workshop*, 2004.

[32] Volokh, E., Personalization and privacy, *Communications of the ACM*, 43, 8, August 2000, 84-88.