SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

Security for RFID-based Applications in Smart Home Environment

Divyan M. Konidala * Kwangjo Kim *

Abstract— These days, the concept of Smart Home or Ubiquitous Home Network System is becoming more popular. It is anticipated that Radio Frequency Identification (RFID) and Mobile RFID technologies would play a major role in such an environment. At the outset this paper describes some of the RFID-based applications that are applicable to smart home environment. We then identify the security threats and security requirements associated with deploying RFID-based applications in this environment A Home Server operating inside this environment is considered to be the brain of the Smart Home system. Therefore, in this paper we also propose a security architecture where RFID tagged devices and items, portable handheld RFID readers, and RFID-based applications would securely interact among themselves and with the Home Server.

Keywords: Radio Frequency Identification, RFID, Smart Home, Home Network System, Home Server, Secure RFID-based Applications, RFID Reader-enabled devices, RFID tagged consumer items, EPCglobal architecture framework

1 Introduction

1.1 RFID Technology

Radio Frequency Identification (RFID) [1] is a means to efficiently and quickly, auto-identify objects, assets, pets, and people. With the current bar-code technology, each item's bar-code label (Uniform Product Code - UPC) must be brought before the reader or laser, and labels must be scanned one by one. This leads to laborious, painstaking, human-error prone, and time consuming inventory checking. With RFID technology, passive RFID tags are attached to items and these tags contain tiny, but durable computer chips with very small antennas. Passive tags are powered-up from the interrogation Radio-Frequency (RF) signal of a reader. The tiny computer chips contain an Electronic Product Code (EPC) that uniquely identifies the object to which it is attached to, and the antennas automatically transmit this EPC number without requiring line-of-sight (i.e., visual) scanning, to RFID readers within a certain RF range. Therefore RIFD technology allows quick scanning of products in large bulks. Other advantages of RFID technology include: RFID tags can stand a harsh environment, long read ranges, portable database, multiple tag read/write, and tracking items in real-time, *etc.*

EPC number is composed of: EPC Manager number (identifies the company), Object class (similar to a stock-keeping unit, also called product number), Serial number (specific instance of the object class being tagged, objects own unique identifier). Further information about the product (product description, size, weight, manufacturing date, expiry date, directions to use, ingredients, packaging, shipments, product arrival and departure details, and various other data that are appropriate to share with supply chain partners and consumers) is stored on network of databases, called the EPC-Information Services (EPC-IS). EPC-IS assists geographically distributed supply chain partners and consumers to easily and efficiently access information on any product they are handling / purchased. Therefore, an unique EPC number acts like a pointer directing a RFID reader to the right EPC-IS from where the reader can download related data about the product it scanned.

VeriSign's white paper [2] gives a good description about RFID technology for supply chain management. RFID automates supply chain management; it greatly helps enterprises to maintain the accuracy of shipments sent and received by parties throughout distribution. It prevents product theft by capturing product arrival and departure at each point, enabling comprehensive distribution visibility that creates a record of the chain of custody for each product. It also helps in precise product recall.

1.2 RFID Technology and Smart Homes

Due to the above-mentioned advantages of RFID technology, few big companies like Wal-Mart, Proctor & Gamble Co., and Gillette *etc.*, are already using this technology for real-time tracking of inventory in their supply chain. Currently RFID tags are still expensive, but very soon it would become economical to tag products at the item level, leading to large-scale use of RFID tags on consumer goods. This would further lead to development and deployment of electronic appliances and devices that are RFID Reader-enabled, *e.g.,* RFID Reader-enabled book shelves, refrigerators, microwave, and washing machines, and RFID Reader-enabled mobile phones and PDAs (Mobile RFID Tech-

* International Research Center for Information Security (IRIS), Information and Communications University (ICU), 103-6, MunjiDong, YusungGu, Daejeon 305-714, Republic of Korea. {divyan, kkj}@icu.ac.kr

nology). With these devices and appliances, consumers are can make use of the RFID tags attached to their purchased items in their homes. For example, a RFID Reader-enabled refrigerator can list out (on a embedded display screen) all the RFID tagged items inside the refrigerator along with their related data such as item name, ingredients, manufacturing date, expiry date, *etc.* This example is just one of the many RFID-based applications that would very soon become common in a Smart Home environment.

In a smart home, different information gadgets, home appliances and other Internet-based applications communicate with each other forming a ubiquitous home network system, in order to make life easier in many ways, and more entertaining. Smart homes distribute information and commands among the networked devices in the home via wired and wireless communications. A Home Server or a Home Gateway operating inside this environment is considered to be the brain of the home network system. A home server supports all networking needs in the home, *e.g.,* interacting with the home telephone, stereo system, air-conditioning system, kitchen appliances, motion detection sensors, security system, lights, windows, doors, blinds, and other network-enabled devices. It also connects the home's local area network to the Internet, which allows the home network to communicate with the external world by telephone or through the Internet, sending messages or alarms to the residents of the house. This communication makes it possible to program the smart home from inside or outside the house.

In this paper we explore the possibilities of deploying RFID-based Applications in a smart home environment and specifically focus on various security related issues.

1.3 EPCglobal Inc^{TM} Class-1 Gen-2 UHF Tags

EPCglobal [3] is leading the development of industry-driven standards for the EPC to support the use of RFID in supply chain management. We composed this paper referring to the following specification and ratified standard from EPCglobal:

EPCglobal Architecture Framework Version 1.0. [4]: This specification broadly defines the principles, standards, and components necessary to successfully develop and implement the EPCglobal Network, upon which trading partners or EPCglobal Subscribers will be able to rely to more efficiently manage their supply chain and operate their businesses.

EPCglobal Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.0.9. [5]: This EPCglobal Board Ratified standard defines the physical and logical requirements for a passive backscatter, Interrogator-talks-first (ITF), RFID system operating in the 860 MHz - 960 MHz frequency range. The system comprises RFID Readers, and RFID Tags.

While Gen-2 ultrahigh-frequency (UHF) tags are suitable to tag cases and pallets, there is an ongoing debate among the supply chain stakeholders and RFID tag manufacturers whether to use high-frequency (HF) 13.56 MHz tags or UHF 915 MHz tags for item-level tagging. The former has a shorter read range but tends to perform better on items that cause RF interference. Still, advances in tag design are showing that UHF tags can be resilient to RF interference at close range to the interrogator. [6] claims that from items to pallets, Gen-2 UHF tags are all we need. However, EPCglobal will develop its own HF standard [7]. The memory structure, security and simplified command set used with the UHF Gen-2 could be incorporated in an HF air-interface protocol to make it more useable and interoperable. Therefore, in this paper we assume that all the items are tagged with EPCglobal Class-1 Gen-2 UHF tags.

NOTATION	DESCRIPTION
$Rc\#$	Shopping Transaction Receipt Number
EPC_1	Electronic Product Code of Item 1
$APwd_1$	Tag Access Password of Item 1
$INFO_1$	All the Related Information on Item 1
HS	Home Server
C	Consumer / User
F	RFID Reader-enabled Refrigerator
ID_X	Identity No. of RFID Reader-enabled Device X
$Config_X$	Configuration Details RFID Reader-enabled Device X
ONS	Object Naming Service
EIS	EPC-Information Services
URL_1	URL of EPC-IS, related to Item 1
Kr_A	Private Key of an Entity A
Ku_A	Public Key of an Entity A
E_{Ku_A}	Encryption using Public Key of A
Sig_{Kr_A}	Digital Signature using Private Key of A
Dt	Date
Tm	Time

Table 1: Notations

1.4 Notations

Table 1 provides the list of notations we used in this paper:

2 Shopping Tagged Consumer Items

Scenario I: *Alice visits a discount department store and purchases items that are having RFID tags attached to them. She wants to utilize the RFID tags attached to the purchased items in her smart home environment. But while carrying these items to her home, she might be snooped upon by a thief, Charlie. Charlie has a powerful RFID reader, using which, from a distance he can scan the RFID tagged items inside Alice's bag, to check if she is carrying any items that are worth stealing. On the other hand, Alice may be carrying a RFID tagged MP3 player with her at all times and this tag have a unique EPC number. If Charlie happens to be a stalker, he can track and trace Alice at different locations based on this unique EPC number. Therefore consumers carrying RFID tagged items have to be*

protected from both Information and Location privacy violation.

2.1 Protecting Consumer Privacy

Killing the Tag: As per EPCglobal standard [5], manufacturer of the items can embed Class-1 Gen 2 UHF Tags with Kill Password. Whenever a RFID reader send this Kill Password to the tag, the tag is killed and rendered permanently unusable and unreadable. Therefore, once a tagged item is purchased by Alice, the trustable clerk at the point-of-sale (cashier) can obtain the tag's kill password from the store's EPC-IS and kill the tag permanently. But with this approach Alice cannot make use of the tag capabilities at her smart home environment, *e.g.,* RFID enabled refrigerator or book shelf, *etc.*

Locking the Tag: As per EPCglobal standard [5], manufacturer of the items can embed Class-1 Gen-2 UHF Tags with a unique 32-bit value Access Password. A RFID reader submits the access password to the tag and the tag verifies if this access password is the same with the one embedded within. If the access passwords tally, the tag allows the reader to perform on it, the mandatory commands such as Read, Write, and Lock. A tag's chip has four memory banks: Reserved, EPC, TID, and User. Reserved memory bank is used to store the Kill Password and Access Password, EPC memory bank for EPC number, TID memory bank for tag's unique manufacturer identity number, and User memory bank for additional user data. The reserved memory bank is permanently locked by the manufacturer; as a result the access password can neither be read nor modified by any reader.

To prevent corporate espionage, illegal access and leakage of sensitive tag data, most of the tags contain only its unique EPC number and all the data associated with that EPC number is stored with the EPC-IS. Access to EPC-IS is secure, and restricted to only authorized supply chain stakeholders. Therefore stores may lock all the memory banks except the EPC memory bank, because the EPC number is used to retrieve the data associated with that item and also to retrieve its corresponding access password (from EPC-IS). Tag's access password is thus used for "reader to tag" authentication and also allows the reader to access the locked memory banks within the tag, permission to change the lock status of the memory banks (except the reserved memory bank), and write data into the tag, etc.

Based on the above-mentioned access password and locking features available with UHF tags, we propose the following approach, where the tag need not be killed permanently in order to protect consumer privacy. Once a tagged item is purchased by Alice, the trustable clerk at the point-of-sale can retrieve the tag's access password from the store's EPC-IS and using this access password, the clerk can lock all the memory banks of the tag including the EPC memory bank. Alice can download and store the EPC numbers and their corresponding access passwords into her mobile phone. This can be made possible via Bluetooth or Infra-Red (IR) communication between the Alice's mobile phone and the point-of-sale terminal. Alice can securely send this downloaded information to her Home Server. With this proposed approach, adversary Charlie can no longer get any information (including the EPC number) from the RFID tags possessed by Alice, as all the memory banks of the tags are locked and Charlie does not have the access passwords. When Alice reaches home the RFID reader in the home communicates with the home server and obtains the EPC numbers and their corresponding access passwords. The procedure on how the RFID reader in the home unlocks the tags' memory banks is discussed in the subsequent sections.

Ari Juels [8] summarized many previously proposed security models for tag-reader mutual authentication, but unlike these models, the main advantage of our proposed approach is that it does not require implementation of any special cryptographic functions/keys within the tag. There is also no need for the tag and the reader to synchronize security keys/hash values. We in fact propose to slightly change the way in which the already existing access password scheme for EPCglobal Class 1 Gen 2 UHF tags can be utilized to protect consumer privacy.

3 Interacting with Smart Home Environment

Scenario II: *After purchasing the RFID tagged items from the store, Alice can download and store the EPC numbers and their corresponding access passwords into her mobile phone. This can be made possible via Bluetooth or Infra-Red (IR) communication between the Alice's mobile phone and the point-of-sale terminal. Alice uses her mobile phone to establish a secure Mobile Virtual Private Network (MVPN) with her home server, in order to send the EPC numbers and their corresponding access passwords. Based on the EPC numbers, home server identifies the appropriate EPC-IS and establishes a Virtual Private Network (VPN). Using the access passwords as proof of purchase, home server downloads related information (product description, size, weight, manufacturing date, expiry date, directions to use, ingredients, warranty certificate,* etc.*) associated with the EPC numbers. EPC-IS must provide only that information, which is relevant to the consumer who purchased the items.*

3.1 Secure Communication: Mobile Phone & Home Server

Alice's mobile phone can establish a MVPN with the home server, before sending the EPC numbers and their corresponding access passwords. Otherwise the communication channel between the mobile phone and the home server can be easily eavesdropped, and prone to man-in-the-middle (MIM) attacks, replay attacks, Denial of Service (DOS) attacks, data manipulation and corruption. A MVPN can be implemented based on IP Security (IPSec) protocols. We can incorporate the following features: Encryption algorithm - AES (128, 192, 256 bit), Hash algorithm - SHA1, User authentication - X.509v3 Digital Certificates, Public key

algorithm - RSA Cryptography Standard PKCS #1 1024 bit, Key management - PKCS#8 for private key format. Both mobile phone and the home server belong to Alice, so they can very securely issue digital certificates and cryptographic keys among themselves. We suggest another simple approach, which is easy to understand by looking at the figure 1. Here we use Dt, and Tm as a nonce to ward off replay attack.

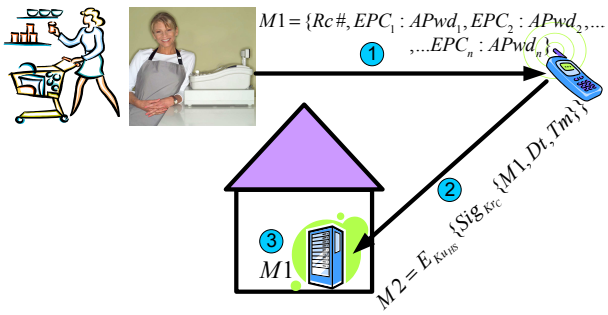

Figure 1: Secure Communication: Mobile Phone & Home Server

3.2 Secure Communication: Home Server & EPC-IS

After obtaining the EPC numbers from Alice's mobile phone, home server now needs to contact the appropriate EPC-IS to download the related information associated with the EPC numbers. As per the EPCglobal Architecture Specification [4], there exists a Object Naming Service (ONS), which can assist the home server to locate the EPC-IS. ONS, provides a global lookup service to translate an EPC number into one or more Internet Uniform Reference Locators (URLs) where further information on the item may be found. Root ONS provides the initial point of contact for ONS lookups. In most cases, delegates the remainder of the lookup operation to a Local ONS within the control of the enterprise.

The home server can establish a VPN with the EPC-IS, before sending the EPC numbers and their corresponding access passwords. Otherwise the communication channel between the mobile phone and the home server can be easily eavesdropped, and prone to man-in-the-middle (MIM) attacks, replay attacks, Denial of Service (DOS) attacks, data manipulation and corruption. Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and thus Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and used, such techniques can provide secure communications over unsecured networks. We can use VPN protocols like: IPSec or Secure Sockets Layer / Transport Layer Security (SSL/TLS). Both home server and the EPC-IS can trust Alice's mobile operator or any trusted third part to issue digital certificates and cryptographic keys. We suggest another simple approach, which is easy to understand by looking at the figure 2.

The clerk at the point-of-sale gives away the access passwords to only those consumers who purchased the tagged items. EPC-IS already has the list of EPC numbers and their corresponding access passwords, therefore when the home server sends the access passwords to EPC-IS it proves that Alice / home server indeed purchased the tagged items. EPC-IS

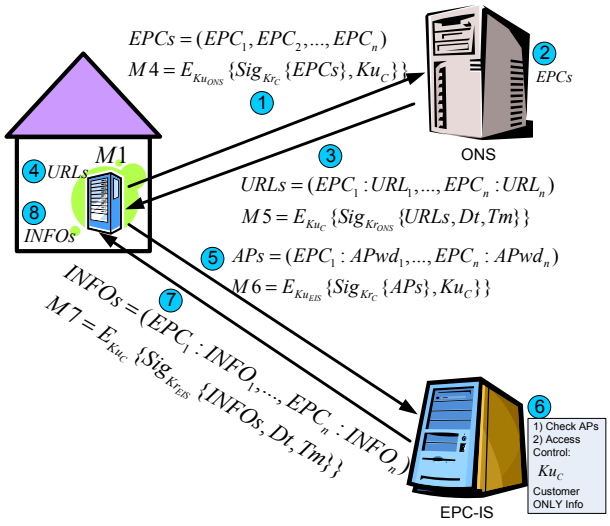

Figure 2: Secure Communication: Home Server & EPC-IS

Scenario III: *By the time Alice reaches her home with the purchased tagged items, the home server is ready with all the information about the items. Alice stacks the tagged items in the RFID Reader-enabled refrigerator. The RFID reader in the refrigerator realizes that some of the tagged items do not respond with their EPC numbers, which means that these are newly added items and their memory banks are all locked. The RFID reader securely communicates with the home server to retrieve the access passwords and unlocks the tags' memory banks. Whenever Alice requests for listing the items in the refrigerator, the RFID reader collects all the EPC numbers from the tags and sends them to the home server. Home server would retrieve the information associated with these EPC numbers and displays the same on the display screen attached to the refrigerator.*

3.3 Secure Communication: RFID Reader - enabled Appliance & Home Server

RFID Reader-enabled appliance must identify, authenticate and establish a VPN with the home server. Apart from the previously mentioned threats we should also consider a threat where any malicious powerful RFID reader positioned outside the smart home, may impersonate as a genuine RFID reader-enabled appliance inside the home. Therefore, whenever a new RFID reader-enabled device is brought into the house, both the RFID reader and the home server under the supervision of Alice must establish public/private keys and digital certificates among themselves. With this approach, if a malicious reader wants to establish keys

and certificates, the home server must send an alarm to Alice and seek her consent. For this, we suggest a simple approach, which is easy to understand by looking at the figure 3.

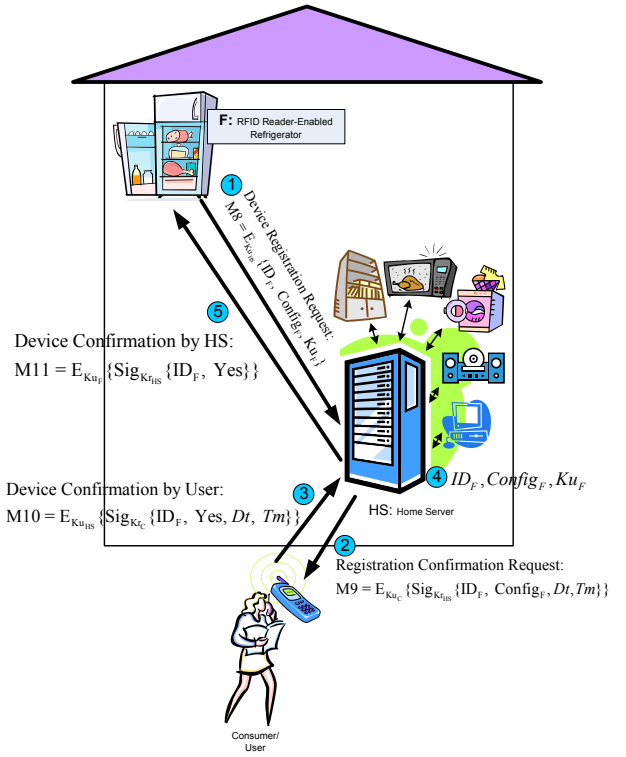

Figure 3: RFID Reader-enabled Device Registration Process

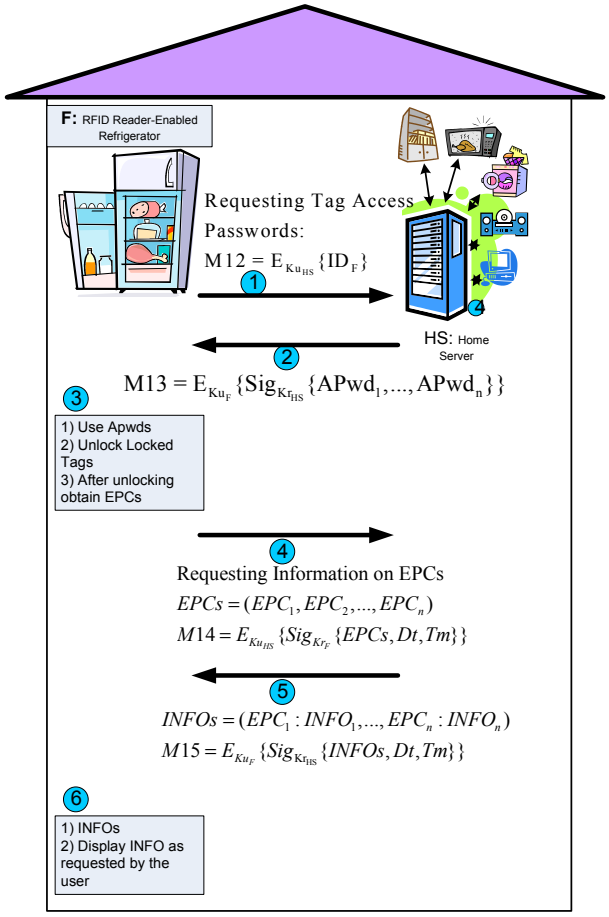

Figure 4: Unlocking RFID tags by RFID Reader-enabled Device

RFID reader in the refrigerator does not get any EPC number from the newly added items in the refrigerator as their memory banks are all locked. In such a situation, RFID reader communicates with the home server and requests for all the RFID tag access passwords that have been downloaded by the server (from EPC-IS) but not yet activated in the smart home. Home server sends all those access passwords (must be few in number) to the RFID reader and the reader checks each of these passwords with every locked tag until a particular tag responds with its EPC number. With this approach a tag can be unlocked without knowing its EPC number initially. This approach, can be easily understood by looking at the figure 4.

Scenario IV: *Alice has a RFID reader-enabled refrigerator, which stores many tagged items. All these tagged items emit their EPC number when queried by the RFID reader inside the refrigerator. But this poses a threat. A malicious powerful RFID reader positioned outside the smart home, may be able to query the tagged items in the refrigerator and retrieve their EPC numbers. Then the malicious reader may communicate with EPC-IS and retrieve information associated with these EPC numbers. This leads to privacy violation*

3.4 Protecting Smart Home Residents Privacy

To alleviate the above mentioned problem, we propose the following approach: Once the RFID reader in the refrigerator unlocks the tags, it can assign a different unique tag ID and write this tag ID into the User memory bank of the tag. After which, except the user memory bank, the RFID reader must also lock all the other memory banks including the EPC memory bank. The reader notifies the new tag ID to the home server, which maintains the reference between the EPC number and its new tag ID number. From now on whenever the RFID reader inside the refrigerator queries the tags in the refrigerator, they all respond with their new tag IDs completely different from their original EPC numbers. And only this new tag ID will be used in the smart home environment. Even if a malicious RFID reader gets these unique tag IDs he cannot obtain any information from EPC-IS, as the EPC-IS has no knowledge about these new tag IDs.

4 Conclusion

In this paper we considered various RFID-based application scenarios that are suitable for Smart Home environment. Based on these scenarios we identified some of the security and privacy threats related to deployment of RFID-based applications in a smart home environment. We identified the need for protecting the consumer privacy and proposed "Locking the Tag" approach, in order to protect consumer privacy. We also proposed security measures to provide authentication,

data confidentiality, and data integrity between the following communicating entities: consumer's mobile phone, home server, Electronic Product Code - Information Services, RFID Reader-enabled household appliances and devices. Our future work includes thorough performance analysis of our proposed architecture.

References

[1] Patrick J. Sweeney II, "RFID for Dummies", Wiley Publishing,Inc., ISBN: 0-7645-7910-X, 2005.

[2] VeriSign, "The EPCglobal Network: Enhancing the Supply Chain", White Paper 2005, http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf

[3] EPCglobal Web site, 2005, http://www.EPCglobalinc.org

[4] EPCglobal Specification, "The EPCglobal Architecture Framework", http://www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf

[5] EPCglobal Ratified Standard, "EPC^{TM} Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.0.9", http://www.epcglobalinc.org/standards/

[6] Impinj RFID Technology Series Whitepaper, "UHF Gen 2 for Item-Level Tagging", REV 1.0 02-06, February 2006, http://www.impinj.com/files/MR_GP_ED_00003_ILT.pdf

[7] Mary Catherine O'Connor, "EPCglobal Developing HF Tag Standard", News Report, RFID Journal, May 2006, http://www.rfidjournal.com/article/articleview/2320/1/1/

[8] Ari Juels (2005), "RFID Security and Privacy: A Research Survey", RSA Laboratories.