# Secure Approach to Deploy RFID-based Applications in Smart Home Environment

Divyan M. Konidala, Zeen Kim, Chan Yeob Yeun, Jin Li, Kwangjo Kim

International Research Center for Information Security
Information and Communications Univ.

## Abstract

The concept of a Smart Home is becoming more and more popular. It is anticipated that Radio Frequency IDentification (RFID) technology would play a major role in such an environment. We can find many previously proposed schemes that specifically target: authentication between the RFID tags and readers, and user privacy protection from malicious readers. We all have also heard of this very popular application, where a refrigerator/bookshelf can scan all the RFID-tagged items put in it and can list out the details of these items on it's display screen. Realizing such an application is not as straight forward as it seems to be, and to the best of our knowledge, there has been no published work on how to securely deploy such RFID-based applications in a smart home environment. Therefore at the outset this paper describes some of the RFID-based applications that are applicable to smart home environment. We then identify their related security threats and security requirements and also propose a secure approach, where RFID-tagged consumer items, RFID-reader enabled devices (*e.g.,* refrigerator), and RFID-based applications would securely interact among themselves. At the moment, our approach is not fully comprehensive, but it sheds light on very important security issues related to RFID-based applications that are actually needed and beneficial for consumers.

## I. Introduction

### 1. RFID Technology

Radio Frequency IDentification (RFID) [1] is a means to efficiently and quickly, auto-identify objects, and assets. With RFID technology, passive-RFID tags are attached to consumer items. To prevent corporate espionage, and leakage of sensitive tag data to malicious RFID readers, most of the tags contain only its unique Electronic Product Code (EPC) number and all the information associated with that EPC number (*e.g.,* item description, shipments, product arrival and departure details, *etc.*) is stored on a network of databases, called the EPC-Information Services (EPC-IS), which assists geographically distributed supply chain partners and consumers to easily and efficiently access information on any product they are handling. A unique EPC number acts like a pointer directing a RFID reader to the right EPC-IS from where the reader can download related information about the product it scanned. There exists an Object Naming Service (ONS), which provides a global lookup service to translate an EPC number into one or more Internet URLs of EPC-IS, where further information on the item is retrieved. VeriSign [2] describes many advantages of RFID technology for supply chain management.

### 2. Smart Home

Currently RFID tags are still expensive, but very soon it would become economical for large-scale use of tags on consumer goods. This would lead to development and deployment of electronic appliances and devices that are RFID Reader-enabled, *e.g.,* RFID Reader-enabled book shelves, and refrigerators. A display screen on a RFID Reader-enabled refrigerator can list out the details of all the RFID-tagged items inside the refrigerator, such as item name, manufacturing date, expiry date, *etc.* In a smart home environment, different information gadgets, and home appliances communicate with each other, in order to make life easier in many ways. A Home Server or a Home Gateway operating inside this environment is considered to be the brain of this home network system. A home server supports all networking needs in the home. It makes it possible to program the smart home from inside or outside the house.

### 3. EPCglobal C-1 Gen-2 UHF Tags

EPCglobal Inc [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 based on the following standards: (i) EPCglobal Architecture Framework [4], (ii)

EPCglobal Class-1 Generation-2 UHF RFID Protocol [5]. In this paper we assume that all the items are tagged with EPCglobal C-1 Gen-2 UHF tags.

Table 1: Notations

| 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 Related Information on Item 1 |
| $ID_X$ | Identity No. of RFID Reader-enabled Device X |
| $Config_X$ | Configuration Details RFID Reader-enabled Device X |
| $URL_1$ | URL of EPC-IS, related to Item 1 |
| $Kr_A$ | Private Key of an Entity A |
| $Ku_A$ | Public Key of an Entity A |
| $E_{KuA}$ | Encryption using Public Key of A |
| $Sig_{KrA}$ | Digital Signature using Private Key of A |

## II. Shopping Tagged Consumer Items

***Scenario I:*** *Alice visits a department store and purchases RFID tagged items. But while carrying these items to her home, a thief, who has a powerful RFID reader, 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 a stalker can track and trace Alice at different locations based on the EPC number of MP3 player. Therefore consumers need both Information and Location privacy.*

### 1. Protecting Consumer Privacy

As per EPCglobal standard [5], manufacturer of the items can also embed C-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 itself. 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 memory bank stores the access password and it is permanently locked by the manufacturer; as a result the access password can be neither read nor modified. Based on the access password and locking feature available with UHF tags, we propose the following approach: 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. Juels [6] summarized many previously proposed security models for tag-reader mutual authentication, which allows the tag to respond to only authorized and genuine readers. 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.

## III. Interacting with Smart Home Environment

***Scenario II:*** *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 access passwords. Based on the EPC numbers, home server identifies the appropriate EPC-IS and establishes a Virtual Private Network (VPN) with it. Using the access passwords as proof of purchase, home server downloads related information (product description, manufacturing date, expiry date, directions to use, 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. Therefore, by the time Alice reaches home with the purchased tagged items, the home server is ready with all the information about the items.*

### 1. Secure Communication: Mobile Phone and Home Server

The communication channel between the mobile phone and the home server can be easily eavesdropped, and prone to man-in-the-middle (MIM)

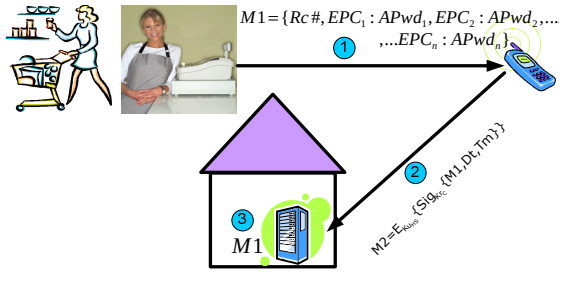


Figure 2: Secure Communication: Mobile Phone and Home Server

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, where PKI-based digital signature and encryption scheme is used. This can be easily understood by looking at fig. 2. Here we use date Dt, and time Tm of shopping transaction as a nonce to ward off replay attack.

## 2. Secure Communication: Home Server and 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. The home server can establish a VPN with the EPC-IS, before sending the EPC numbers and their corresponding access passwords. 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, where PKI-based digital signature and encryption scheme is used to secure the communication between the home server and EPC-IS. This can be easily understood by looking at fig. 3. 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.

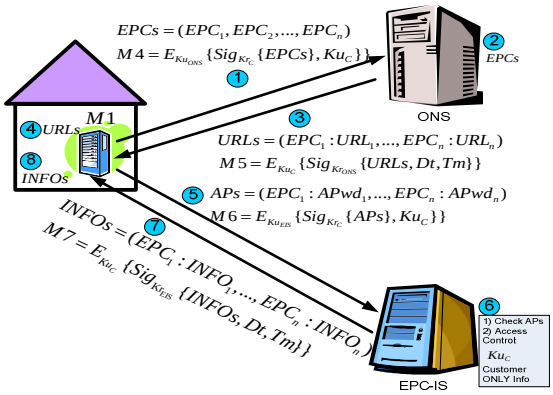

Figure 3: Secure Communication: Home Server and EPC-IS

## 3. Secure Communication: RFID Reader-enabled Appliance and Home Server

RFID Reader-enabled appliance must identify, authenticate and establish a VPN with the home server. 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. For this, we suggest a simple approach, which is easy to understand by looking at fig 4. 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 fig 5.

***Scenario IV:*** *All 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.*

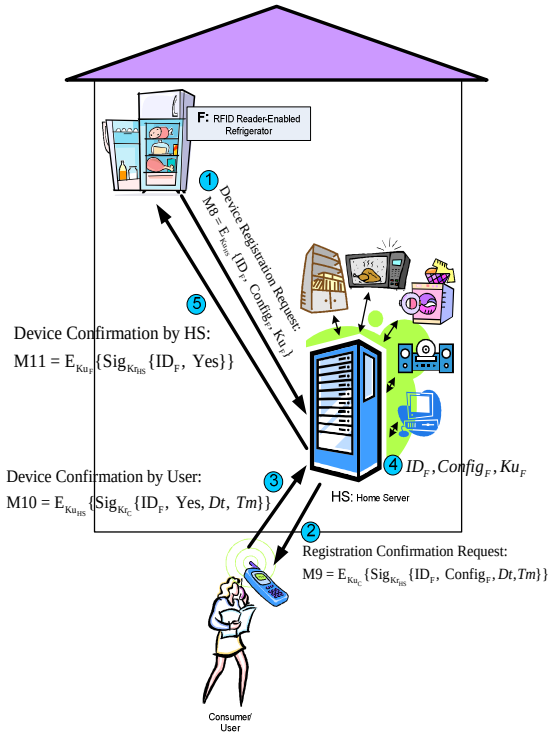


Figure 4: Secure Communication: RFID-Reader Enabled Appliance and Home Server

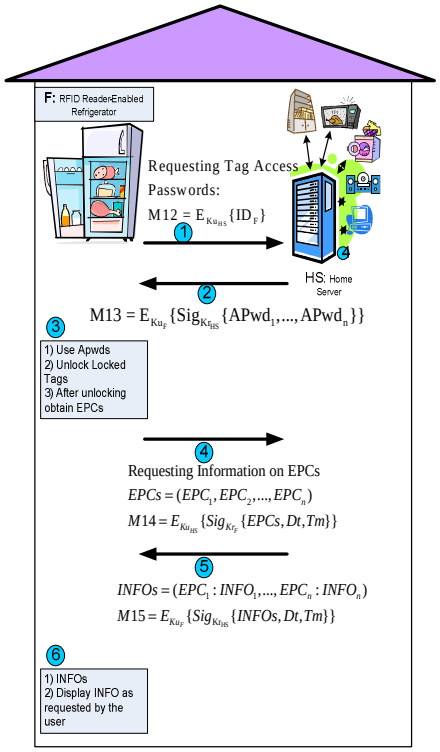


Figure 5: Unlocking RFID tags by RFID Reader-enabled Device

## 4. Protecting Smart Home Residents Privacy

Once the RFID reader in the refrigerator unlocks the tags, it can assign a different tag ID and write this pseudo 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 pseudo ID to the home server, which maintains the reference between the EPC number and its new pseudo ID number. From now on whenever the RFID reader inside the refrigerator queries the tags in the refrigerator, they all respond with their new pseudo IDs completely different from their original EPC numbers. And only this new pseudo ID will be used in the smart home environment. Even if a malicious RFID reader gets these unique pseudo IDs he cannot obtain any information by sending pseudo IDs to EPC-IS, as the EPC-IS has no knowledge about these new pseudo IDs.

# IV. 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. 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 secure approach.

# 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,
[3] EPCglobal Web site, 2005, http://www.EPCglobalinc.org
[4] EPCglobal Specification, "The EPCglobal Architecture Framework", http://www.epcglobalinc.org/standards/
[5] EPCglobal Ratified Standard, "EPC 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] Ari Juels (2005), "RFID Security and Privacy: A Research Survey", RSA Laboratories.