AUTO-ID LABS

Security Assessment of EPCglobal Architecture Framework

Divyan M. Konidala, Woan-Sik Kim, and Kwangjo Kim

Auto-ID Labs White Paper WP-SWNET-017

Divyan M. Konidala
PhD. Candidate,
Information and Communications University

Woan-Sik, Kim
Senior Researcher,
Korea Telecom

Kwangjo Kim
Professor,
Information and Communications University

Contact:

E-Mail: divyan@icu.ac.kr

CAIS Lab, R504, Information and Communications University (ICU), 103-6,
MunjiDong, YuseongGu, Daejeon 305732, Republic of Korea

Internet: http://caislab.icu.ac.kr

Abstract

This paper focuses on RFID-based supply chain management system that adheres to the EPCglobal Architecture Framework specification. We approach this framework with a security point-of-view and the main idea is to secure this framework for a safe and secure RFID-based supply chain management system. At the outset this paper briefly describes the EPCglobal Architecture Framework and provides an example supply chain scenario. The framework is composed of entities like RFID Tag, RFID Reader, RFID Middleware, Electronic Product Code Information Service (EPCIS) Repository, EPCIS Accessing Application, Object Naming Service, and Subscriber Authentication. We analyze the various security threats that affect each of these entities and their communication interfaces. Some of these threats include cloned fake RFID tags, unauthorized access and/or modification of RFID tag information and its electronic pedigree (EPCIS data), and eavesdropping, spoofing and Denial of Service attack on EPCglobal Subscriber's network. Finally, we propose possible security requirements and needed security solutions to ward off these threats.

Keywords: Radio Frequency Identification, RFID, EPCglobal, EPCglobal Architecture Framework, RFID Security, RFID Tags, Security Assessment of RFID System, Secure Supply Chain, Anti-counterfeiting

1. Introduction

Radio Frequency Identification (RFID) is a means to efficiently and quickly, auto-identify objects, assets, pets, and people, *etc*. With the current bar-code technology, each product'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 objects/products 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.

The most anticipated application of RFID is the automation of supply chain management. So far, few big companies like Wal-Mart, Proctor & Gamble Co., Hewlett-Packard, Prada, and Gillette *etc.,* are using RFID technology for real-time tracking and tracing of inventory in their supply chain. One of the major tasks of RFID-based supply chain management system is to establish, and maintain electronic pedigrees of every individual item within the supply chain. This system greatly assists the stakeholders (associated with a particular supply chain) by providing them with real-time retrieving and updating capability of all the related information (physical location, chain of custody, arrival / departure information, time spent at each location, *etc.*) about items in their custody and also grants them authorized access to the other electronic pedigrees. As a result all the stakeholders have a quick and easy, user-friendly, and efficient means to Track and Trace items within the supply chain. Accurate tracking and tracing of items alleviates the problem of counterfeit items being introduced into the supply chain, and also detects lost and stolen items.

EPCglobal Inc^{TM} [1] is leading the development of industry-driven standards for the Electronic Product Code^{TM} (EPC) to support the use of Radio Frequency Identification (RFID) in supply chain management. VeriSign's white paper entitled “The EPCglobal Network: Enhancing the Supply Chain” [2] gives a detailed description about RFID technology and its advantages for supply chain management. Some of these advantages are as follows: RFID automates supply chain management, enabling enterprises to realize significant savings to the top and bottom line. RFID technology 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. The capability to pinpoint the custodian of the product when it was lost allows the manufacturer or retailer to take preventative measures for the future. As a result, it helps in precise product recall and prevents product counterfeiting.

Having said this, RFID-based supply chain management system still suffers from many security threats and weak points. It can be seen that an item's electronic pedigree plays a vital role in achieving most of the aforementioned advantages of RFID-based supply chain management system, but securing this electronic pedigree from unauthorized access, and illegal modification and fabrication, remains a bigger challenge. Nowadays there is a growing concern about cloned RFID tags, which can be used to introduce counterfeit products into the supply chain. Also the stakeholders or EPCglobal Subscribers (*e.g.,* manufacturer, distributor, and retailer) of a supply chain must secure their network components, which include RFID Tags, RFID Readers, RFID Middleware, Electronic Product Code Information Services (EPCIS) Repository, EPCIS Accessing Application, and Local Object Naming Service (Local ONS) in order to prevent eavesdropping, spoofing, DoS attacks, and EPCIS data corruption. This paper addresses the above-mentioned issues and proposes security details that must be considered to alleviate these inherent threats to RFID-based supply chain management system.

We composed this paper based on the following specification and ratified standards from EPCglobal Inc^{TM}.

- **EPCglobal Architecture Framework Version 1.0. [3]:** 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.
- **EPC^{TM} Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz – 960MHz Version 1.0.9. [4]:** This EPCglobal Board Ratified standard defines the physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), radio-frequency identification (RFID) system operating in the 860 MHz - 960 MHz frequency range. The system comprises RFID Readers, and RFID Tags.
- **EPCglobal Certificate Profile [5]:** The authentication of entities (subscribers, services, physical devices) operating within the EPCglobal network serves as the foundation of any security function incorporated into the network. It is expected, however, that the X.509 authentication framework will be widely employed within the EPCglobal network. To ensure broad interoperability and rapid deployment while ensuring secure usage, this document defines a profile of X.509 certificate issuance and usage by entities in the EPCglobal network. The profiles defined in this document are based upon two Internet standards, defined in the IETF's PKIX Working Group, that have been well implemented, deployed and tested in many existing environments.

Section 2 describes the RFID-based supply chain management system that adheres to EPCglobal Architecture Framework specification. We explain the various entities of this framework and also an example supply chain scenario. Section 3 provides a detailed security assessment of this framework which includes the security threats, security requirements, and security solutions that apply to each of these entities and their communication interfaces. Section 4 provides conclusion and our future work.

2. EPCglobal Architecture Framework

Throughout this paper we consider “EPCglobal Architecture Framework” [3] to be the typical RFID-based supply chain management system, which most of the EPCglobal Subscribers would deploy in their organization. An end-user EPCglobal Subscriber is any organization that employs EPCglobal Standards, Interfaces and EPCglobal Core Services as a part of its supply chain management system. Figure 1 depicts the EPCglobal Architecture Framework.

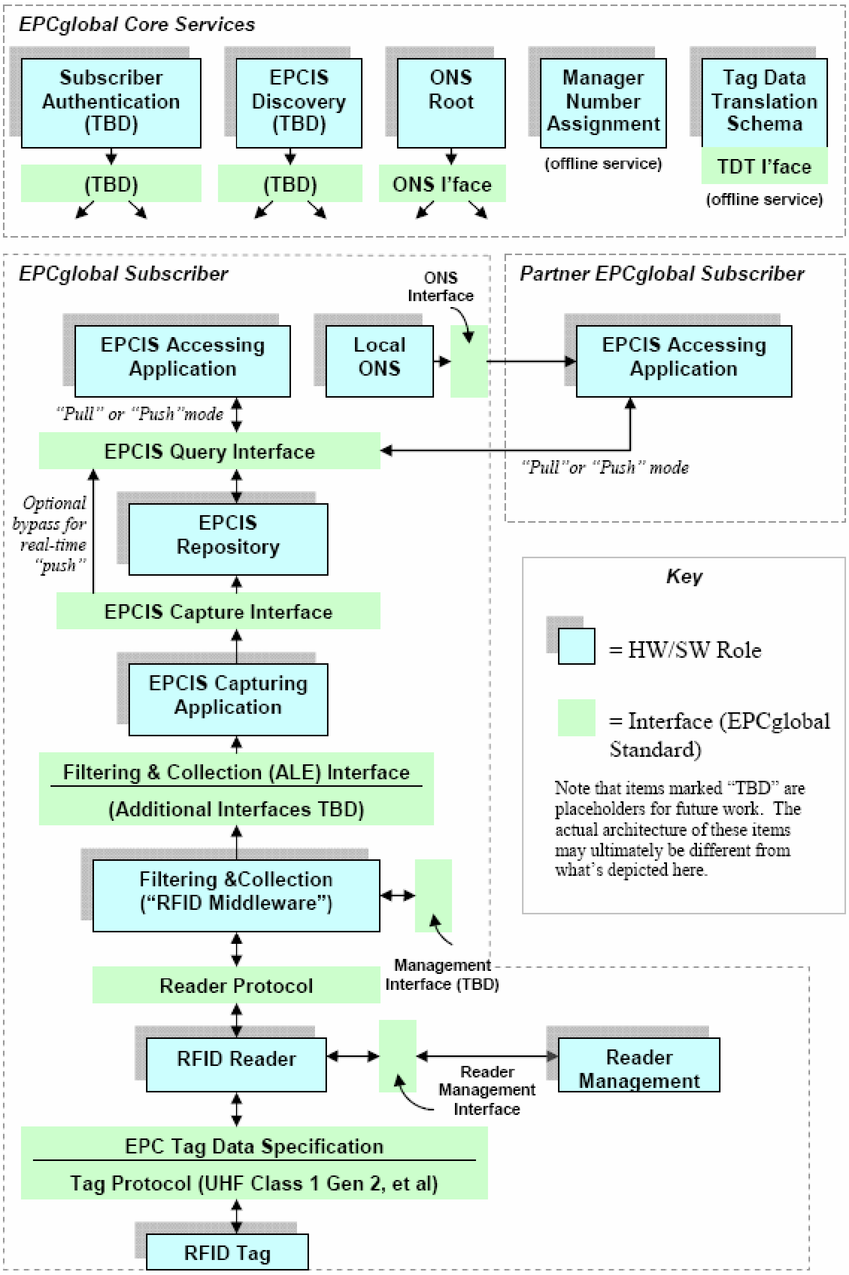
EPCglobal Core Services
Subscriber Authentication (TBD)
(TBD)
EPCIS Discovery (TBD)
(TBD)
ONS Root
ONS I'face
Manager Number Assignment
(offline service)
Tag Data Translation Schema
TDT I'face
(offline service)
EPCglobal Subscriber
ONS Interface
EPCIS Accessing Application
Local ONS
"Pull" or "Push" mode
EPCIS Query Interface
Optional bypass for real-time "push"
EPCIS Repository
EPCIS Capture Interface
EPCIS Capturing Application
Filtering & Collection (ALE) Interface
(Additional Interfaces TBD)
Filtering &Collection ("RFID Middleware")
Management Interface (TBD)
Reader Protocol
RFID Reader
Reader Management Interface
Reader Management
EPC Tag Data Specification
Tag Protocol (UHF Class 1 Gen 2, et al)
RFID Tag
Partner EPCglobal Subscriber
EPCIS Accessing Application
"Pull" or "Push" mode
Key
= HW/SW Role
= Interface (EPCglobal Standard)
Note that items marked "TBD" are placeholders for future work. The actual architecture of these items may ultimately be different from what's depicted here.

Figure 1: EPCglobal Architecture Framework [3]

2.1. Overview

In Figure 1, the plain green bars denote interfaces governed by EPCglobal standards, while the blue "shadowed" boxes denote roles played by hardware and software components of typical RFID-based supply chain management system architecture. This figure is self-descriptive following the data flow (supply chain processing) from the bottom of the figure to the top. We approach EPCglobal Architecture Framework with a security point-of-view and to maintain clarity and simplicity, we group the H/W and S/W roles proposed in the framework into six main entities, namely:

- RFID Tag
- RFID Reader
- RFID Middleware (includes EPCIS Capturing Application)
- Electronic Product Code Information Service (EPCIS) Repository
- EPCIS Accessing Application
- Local Object Naming Service (ONS)

Similarly we consider only those EPCglobal Core Services that have some significance with respect to our security assessment:

- ONS Root
- Subscriber Authentication

To clearly understand the RFID-based supply chain management system, we also consider four supply chain stakeholders or EPCglobal Subscribers:

- Manufacturer (EPCglobal Subscriber)
- Distributor (EPCglobal Subscriber)
- Retailer (EPCglobal Subscriber)
- Consumer (Not a EPCglobal Subscriber)

Figure 2 depicts our simplified version of EPCglobal Architecture Framework and shows how this RFID-based supply chain management system can be deployed by the EPCglobal Subscribers.

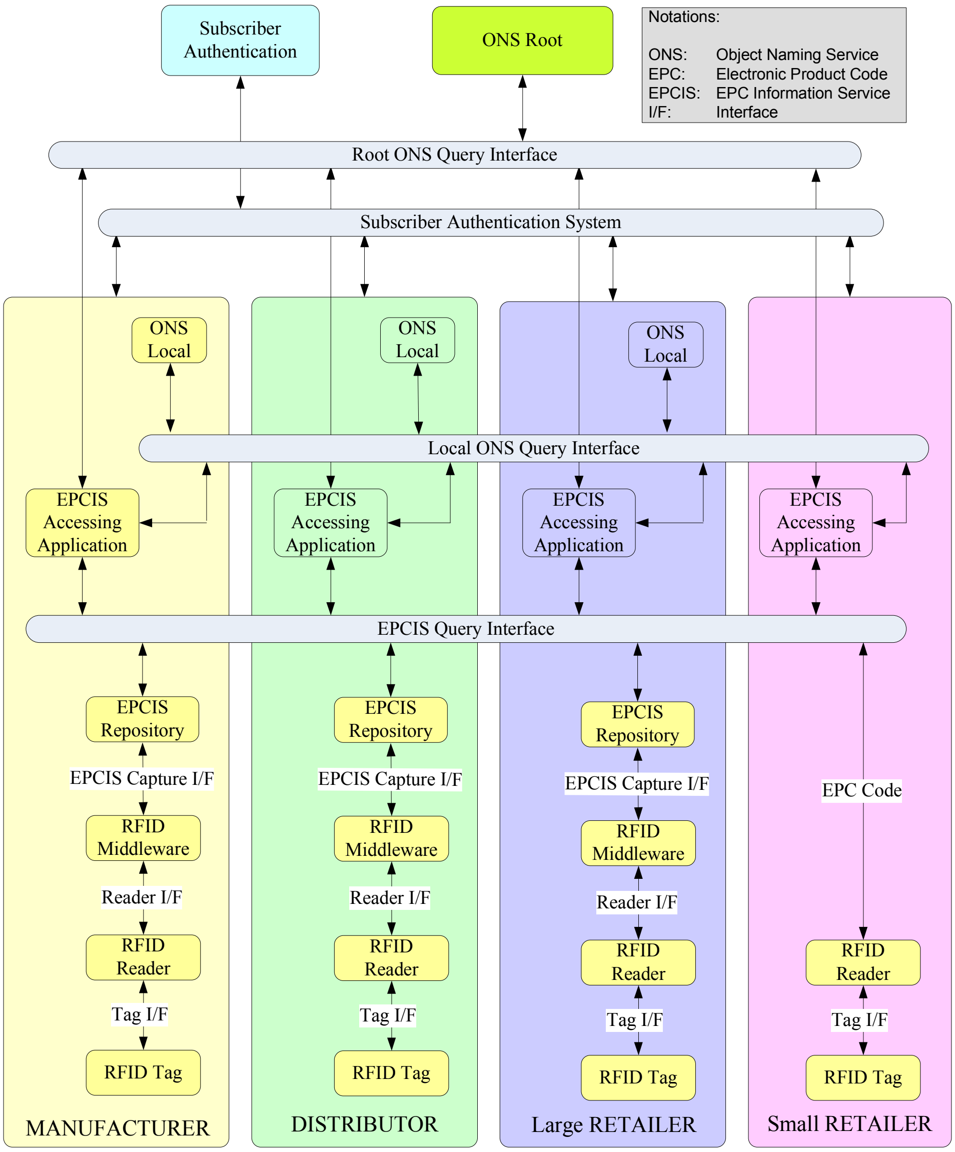

Figure 2: Simplified EPCglobal Architecture Framework

The EPCglobal Architecture Framework specification provides a detailed description of the entities and their interfaces; we summarize some of these details below:

- **RFID Tag:** Every RFID tag contains its unique Electronic Product Code (EPC) number. EPC is a globally unique serial number that identifies an item in the supply chain. EPC number contains: EPC Manager number (identifies the company), Object class (product number), Serial number (specific instance of the object class being tagged, objects own unique identifier). EPCglobal allocates manufacturers specific blocks of EPC numbers, and manufacturers then add their own product codes and serial numbers to their assigned manufacturer numbers to create unique identifiers - EPCs.
- **RFID Reader:** Make multiple observations of RFID tags while they are in the read zone.

- **Reader Interface:** Defines the control and delivery of raw tag reads from Readers to the Filtering & Collection role. Events at this interface say “Reader A saw EPC X at time T.”
- **RFID Middleware:** As mentioned before, for simplicity of our security assessment we consider EPCIS Capturing Application as an integral part of RFID Middleware. RFID Middleware filters and collects raw tag reads, over time intervals delimited by events defined by the EPCIS Capturing Application (*e.g.* tripping a motion detector). The filtered and collected tag read data from RFID Middleware to the EPCIS Capturing Application role may say “At Location L, between time T1 and T2, the following EPCs were observed,” where the list of EPCs has no duplicates and has been filtered by criteria defined by the EPCIS Capturing Application.

  EPCIS Capturing Application supervises the operation of the lower EPC elements, and provides business context by coordinating with other sources of information involved in executing a particular step of a business process. The EPCIS Capturing Application may, for example, coordinate a conveyor system with Filtering & Collection events, may check for exceptional conditions and take corrective action (*e.g.*, diverting a bad case into a rework area), may present information to a human operator, and so on. The EPCIS Capturing Application understands the business process step or steps during which EPCIS data capture takes place. Here, the Filtering & Collection-level event and the EPCIS-level event may be so similar that no actual processing at the EPCIS Capturing Application level is necessary, and the EPCIS Capturing Application merely configures and routes filtered and collected tag read data directly to an EPCIS Repository.
- **EPCIS Capture Interface:** The interface through which EPCIS data is delivered to enterprise-level roles, including EPCIS Repositories, EPCIS Accessing Applications, and data exchange with partners. Events at this interface say, for example, “At location X, at time T, the following contained objects (cases) were verified as being aggregated to the following containing object (pallet).”
- **EPCIS Accessing Application**: Responsible for carrying out overall enterprise business processes, such as warehouse management, shipping and receiving, historical throughput analysis, and so forth, aided by EPC-related data. The EPCIS Accessing Application may use the Object Name Service (ONS) to locate the EPCIS service (EPCIS Accessing Application) of the EPCglobal Subscriber who is the EPC Manager of the object in question.
- **EPCIS Query Interface:** Provides means whereby an EPCIS Accessing Application can request EPCIS data from an EPCIS Repository or an EPCIS Capturing Application, and the means by which the result is returned. Provides a means for mutual authentication of the two parties. Reflects the result of authorization decisions taken by the providing party, which may include denying a request made by the requesting party, or limiting the scope of data that is delivered in response.
- **EPCIS Repository:** Records EPCIS-level events generated by one or more EPCIS Capturing Applications, and make them available for later query by EPCIS Accessing Applications.

- **ONS Query Interface:** Provides a means for looking up a reference to an EPCIS service (EPCIS Accessing Application) or other service that is provided by the EPC Manager of a specific EPC.
- **Local ONS:** Fulfills ONS lookup requests for EPCs within the control of the enterprise that operates the Local ONS; that is, EPCs for which the enterprise is the EPC Manager.
- **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 operated by the EPC Manager for the requested EPC. It may completely fulfill ONS requests in cases where there is no local ONS to which to delegate a lookup operation. Provides a lookup service for 64-bit Manager Index values as required by the EPC Tag Data Specification.
- **Subscriber Authentication:** Authenticates the identity of an EPCglobal Subscriber. Provides credentials that one EPCglobal Subscriber may use to authenticate itself to another EPCglobal Subscriber, without prior arrangement between the two Subscribers. Authenticates participation in network services through validation of active EPCglobal Subscription.

2.2. Supply Chain Scenario

In this section we give an example scenario of a RFID-based supply chain process between a manufacturer and its distributor. Figure 3 depicts the flow of this supply chain scenario.

2.2.1. Manufacturer's End

Step 1:

- Embedding unique EPC numbers within the RFID tags and attaching these tags on each individual product items, cases, cartons, pallets and containers.
- At the end of each above-mentioned stage, RFID tags are scanned with RFID readers.

Step 2:

- RFID readers scan the RFID tags and send their respective EPCs to the RFID Middleware.
- RFID Middleware associates each EPC number with some related information (*e.g.*, one can of cola, manufacture date, expiration date, *etc.*).

Step 3:

- The EPC number and its associated information are stored in the EPCIS repository. As a result each RFID tag's EPC number in the EPCIS repository represents some details about the items, cases, cartons, and containers to which they are attached to.
- The container is sent to the distributor.

2.2.2. Distributor's End

Step 4:

- The container with a tag arrives at the warehouse of the distributor. RFID reader is used to scan the tag attached to the container.

Step 5:

- The EPC number of the container (EPC-C) is sent to the RFID Middleware.
- RFID Middleware associates this EPC-C with some related information (*e.g.*, EPC-C, arrival location, arrival date, arrival time, *etc.*).

Step 6:

- The EPC-C and its associated information are stored in the EPCIS repository of the distributor.

Step 7 & 8:

- Let us assume that the distributor is only aware of the EPC-C, but has no clue on what products it contains. EPCIS Accessing Application of the Distributor (EAA-D) is used to find out further details of EPC-C.

Step 9 & 10:

- Therefore, the EAA-D sends the EPC-C to the Root ONS.
- The Root ONS analyzes the EPC Manager Number, which is a part of the EPC-C, and returns the URL of the Local ONS run by the manufacturer (EPC number Manager of EPC-C).

Step 11 & 12:

- EAA-D sends the EPC-C to the Local ONS of the manufacturer. The Local ONS directs EAA-D to the EPCIS Accessing Application of the Manufacturer (EAA-M).

Step 13, 14, 15, & 16:

- EAA-D sends EPC-C to EAA-M. The EAA-M uses the EPC-C to query the EPCIS repository of the manufacturer, and returns relevant information associated (*e.g.*, EPC-C, cola cans, 50 pallets, 20 cartons per pallet, 15 cases per carton, 6 items per case, *etc.*) with EPC-C to EAA-D.
- EAA-D also informs EAA-M to update its EPCIS repository with the arrival information (*e.g.*, EPC-C, arrival location, arrival date, arrival time, *etc.*) of EPC-C at the distributor's

warehouse. As a result the manufacturer is now aware of the fact that his container has safely reached the intended distributor.

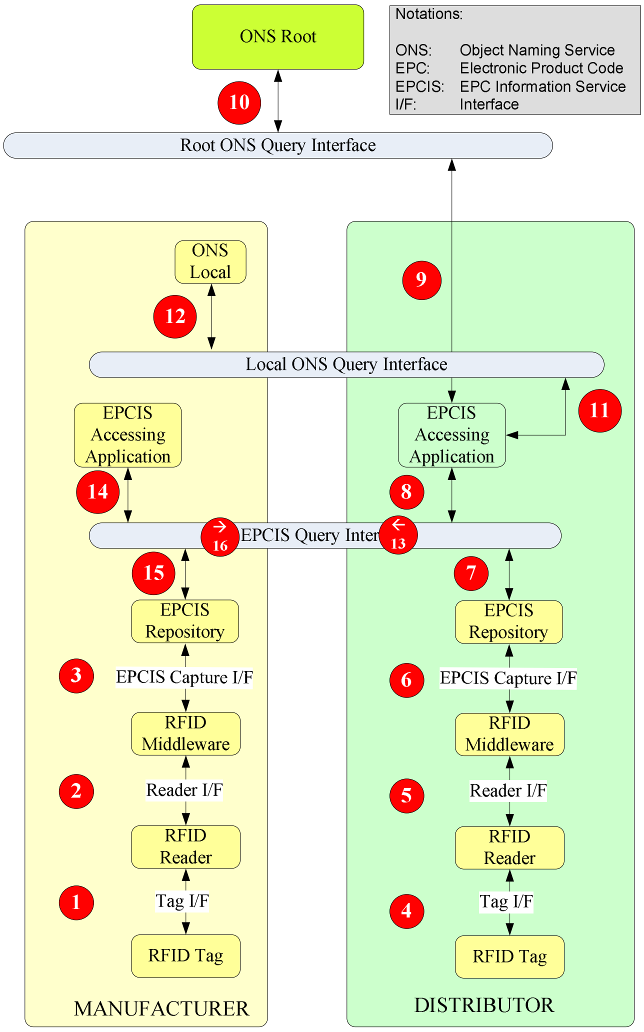

Figure 3: Supply Chain Scenario

3. Security Assessment of EPCglobal Architecture Framework

In this section we provide security assessment on the entities described in our simplified version of EPCglobal Architecture Framework (Fig. 2). We analyze the security threats at each entity and suggest the corresponding security solutions to overcome these threats. The following tables provide a summary of this security assessment. Detailed explanation of the assessment is given in the next section. Figure 4 depicts the entire Security Assessment of

EPCglobal Architecture Framework, including the security threats, and security requirements and solutions.

3.1. RFID Tag

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Tag Snatching	Tamperproof Tag, Tamperproof Packaging	Physical Security	
Unauthorized Tag Data Access & Manipulation	Reader to Tag Authentication	Tag's Access Password, Give out ONLY EPC number	Radio Shielded Enclosure
Cloned Tags	Tag-Reader Mutual Authentication	Challenge-Response schemes based on hash functions, symmetric keys, & tag's access password	Authorized access to tags storage facility

3.1.1. Security Threats:

- **Tag Snatching:** RFID tags attached to a genuine product can be removed and pasted on a fake product, which can then be introduced into a supply chain. A shoplifter can remove a tag attached to a product, thus making it unreadable and walk away with the stolen product undetected.
- **Unauthorized Tag Data Access:** As a part of corporate espionage, tags can be illegally accessed beyond the perimeter of a particular warehouse by using powerful RFID readers.
- **Tag Data Manipulation:** Malicious RFID reader can either corrupt or manipulate the data contained in a tag. Such a reader can write into the memory banks of a tag to suit the adversary's requirements.
- **Tag Cloning:** RFID tag gives out its data (EPC, TID, user data) to any interrogating RFID reader. This reader can either be genuine or malicious. If the tag gives out its data to a malicious RFID reader, then it would be very easy to create a fake tag that gives out the same information.

3.1.2. Security Requirements & Solutions:

- **Tamperproof Tag (Physical Security):** The manufacture of the tags must make sure that the act of snatching a tag should cause a considerable damage to the tag itself and the tag must be rendered permanently unusable.
- **Tamperproof Packaging (Physical Security):** The manufacturer of the products must make sure that the tag is attached to the product in such a way that the act of snatching the tag causes a significant damage to the product package itself, which can be vividly noticeable. Setting up CCTVs in the shopping mall would provide additional security in this regard.
- **Tag Access Password:** EPCglobal UHF Class 1 Gen 2 tag [5] has the facility to lock its memory banks with a 32-bit Access Password. This access password is read/write blocked. Only when a RFID reader presents the right access password, will it be able to access the tag's memory banks (*e.g.*, tag's user data). The manufacturer of the products must make sure that all the tags are coded with unique access passwords and that all the memory banks are locked (Kill and Access Password memory banks are permanently locked - cannot be read or modified by any reader). This Reader to Tag authentication would prevent tag data manipulation threat.
- **Give out Only EPC number:** It must be made sure that the tag gives out ONLY its EPC number to any interrogating RFID reader. A malicious RFID reader would not have the authorization to access the EPCIS Services in order to gain any sensible information about the EPC code.
- **Mutual Authentication:** The above-mentioned Reader to Tag authentication is useful to identify a genuine RFID reader (only this reader has the knowledge of the access password). But in order to differentiate between a genuine and a cloned tag we must also need Tag to Reader authentication. Therefore mutual authentication between the tag and the reader plays a very crucial role. Currently, EPCglobal UHF Class 1 Gen 2 tag standard [5] does not provide any mechanism for tag-reader mutual authentication.
- **External noise / radio Shielded Enclosure (Physical Security):** Processing all the pallets, cases, and items in a shielded enclosure would prevent unauthorized tag data access and interferences from outside the enclosure. The enclosure can be shielded by installing RFID reader-signal jamming equipment on the outside.

3.2. Tag Interface

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Eavesdropping, Replay Attack, Spoofing, MIM Attack	Cover-coding tag's data & access password. Tag-Reader mutual authentication	Data XOR Encoding, Symmetric-Key Encryption Challenge-Response schemes based on hash functions, symmetric keys, & tag's access password	External noise / radio shielded enclosure
DoS Attack: RF Jamming			External noise / radio shielded enclosure

3.2.1. Security Threats:

- **Eavesdropping:** Malicious RFID reader listening to the communications between the tag and the reader in order to retrieve the tag's sensitive data or access password.
- **Replay Attack:** Malicious RFID reader captures a previous successful session between the genuine RFID reader and the tag, only to replay it back at the later stage. This attack is mounted so that even though a particular product is stolen from the supply chain, this attack can still make it look like the product is still present in the chain without raising any alarms. This attack can also be mounted to introduce counterfeit products into the supply chain.
- **Spoofing (Man-in-the-Middle Attack - MIM Attack):** Malicious RFID reader hijacks the communication session between the genuine RFID reader and the tag and impersonates as one of them in order to retrieve the tag's sensitive data or access password.
- **Denial of Service (DoS) Attack:** RF jamming, where the RF channel between the genuine RFID reader and the tag is distributed with a random noisy signal generated by a malicious source, thus bringing down the entire RFID system.

3.2.2. Security Requirements & Solutions:

- **External noise / radio shielded enclosure (Physical Security):** Already discussed in the above sub-section titled "RFID Tag".
- **Give out Only EPC:** It must be made sure that the tag gives out ONLY its EPC code to any interrogating RFID reader. A malicious RFID reader would not have the authorization to access the EPCIS Services in order to gain any sensible information about the EPC code.
- **Cover-coding Tag's Access Password:** Tag's access password should never be sent in the open (unencrypted form) from genuine RFID reader to the tag. EPCglobal UHF Class 1 Gen 2 tag [5] generates a random 16-bit (RN161) number and sends it to the RFID reader. The reader uses (RN161) and performs XOR operation with the first half (16-bits) of the 32-bit access password and sends the result to the tag. The tag performs another XOR operation with (RN161) on the obtained result in order to verify the first half of the 32-bit password from the reader. This process is repeated again when the tag sends another random 16-bit (RN162) number to the reader to verify the second half of the 32-bit access password. This approach is called the cover-coding. Unfortunately this approach is not all secure because both (RN161) and (RN162) are sent in the unencrypted form. Therefore any eavesdropper, malicious reader or man-in-the-middle attack can easily capture (RN161) and (RN162) and obtain the access password. Therefore we need a better cover-coding approach to obscure the access password.
- **Mutual Authentication:** Already discussed in the above sub-section titled "RFID Tag".

3.3. RFID Reader

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Malicious RFID reader in the vicinity	Reader authentication, & authorization	X.509 Authentication Framework - digital certificates, digital signatures, public-key authentication	X.509 based Public Key Infrastructure
Hacked / compromised RFID reader	Do not retain data with RFID readers	Plug unused communication ports	External noise / radio shielded enclosure

3.3.1. Security Threats:

- **Malicious RFID Reader:** Adversaries can place malicious RFID readers inside a particular warehouse in order to carryout corporate espionage, illegally access RFID tag's information, and to mount many attacks that have been previously discussed.
- **Compromised RFID Reader:** It could be possible that a genuine RFID reader could be compromised by an adversary and this reader is simultaneously leaking information to the adversary.

3.3.2. Security Requirements & Solutions:

- **Authenticate and Authorize RFID Readers:** It must be made sure that every RFID reader in the vicinity must be authenticated, authorized and well accounted for before the supply chain process begins. This would ensure detection of malicious readers. Authentication and authorization can be done by verifying RFID readers' digital certificates, digital signatures, and public key authentication (X.509 authentication framework).We suggest that "RFID Management" component can take up this task of authenticating and authorizing all the RFID readers in the system.
- **Constant Supervision of RFID Readers (Physical Security):** All RFID readers must be placed very securely without being distracted by malicious noise signals and provide appropriate physical security by which only authorized personnel can access or configure them.
- **Avoid Retaining Data with the RFID Reader:** It must be made sure that the RFID reader does not retain any data retrieved from the tag. We must plug all the unused communication ports and keep monitoring for any data leakage to the outside.

3.4. Reader Interface

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Eavesdropping, Replay Attack, Spoofing, MIM Attack	Secure communication channel, Reader-Middleware mutual authentication	SSL-TLS / EAP -TLS (wire / wireless comm.), X.509 Authentication Framework - digital certificates, digital signatures, public key authentication	SSL & EAP Protocol, X.509 based public key infrastructure

3.4.1. Security Threats:

- **Eavesdropping:** The communication channel between the RFID Middleware and the Reader can be eavesdropped in order to extract sensitive RFID data, and tag's access password.
- **Spoofing, Man-in-the-Middle and Replay attacks:** Already discussed in the above sub-section titled "Tag Interface". But in this case, we take into account any adversary (not just a malicious RFID reader) trying to mount these attacks on the communication channel between the RFID Middleware and the Reader.

3.4.2. Security Requirements & Solutions:

- **Secure Network, Mutual Authentication, & Authorization:** RFID Middleware and RFID Reader must mutually authentication each other and a secure communication tunnel must be established between them. We can use services like SSL-TLS (Secure Socket Layer - Transport Layer Security: for wired communications), EAP-TLS (Extensible Authentication Protocol: for wireless communications), X.509 certificates, digital signatures, and public key authentication (X.509 authentication framework).

3.5. RFID Middleware

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Intrusion, Viruses, DoS attack, Insider attacks	Application server security measures	System authentication, authorization, & access control, Access Control List (ACL), Ant-virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup, Service packs & Patches	Restricted access control to the premises, CCTV Cameras
Spurious data attacks: Buffer Overflow	Code review, bounds checking	Use of programming language that offer bounds checking (Java, .NET)	
Spurious data attacks: Code Injection	Input validation, Input encoding, Output encoding	Accepting RFID data in the exact predefined format	

3.5.1. Security Threats:

RFID Middleware can be considered as an application server; therefore the following application server security threats are also applicable to RFID Middleware.

- **Application Server Threats:** Intrusion, viruses, DoS attack, *etc*.
- **Spurious Data attack:** Data Injection, and Buffer Overflow.
- **Insider Attacks:** Disgruntled employees, and saboteurs.

3.5.2. Security Requirements & Solutions:

- System authentication, authorization, and access control, Access Control List, Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup
- Spurious Data attacks can be prevented by accepting RFID data only if it is in the exact predefined format, code review, Use of programming languages that offer bounds checking (Java, .NET), input validation, input encoding, and output encoding.
- Physical Access Control: Restricted access control to the premises, CCTV cameras.

3.6. EPCIS Capture Interface

The security threats, security requirements and solutions are very similar to those mentioned in the above sub-section titled “Reader Interface”. But in this case we need to protect the communication channel between the RFID Middleware and the EPCIS Repository, where attacks can be mounted to extract sensitive EPCIS data.

3.7. EPCIS Repository

EPCIS Repository can be considered as a database server, therefore the security threats related to database server are also applicable to EPCIS Repository. These security threats, security requirements and solutions are very similar to those mentioned in the above sub-section titled “RFID Middleware”, but with the following additional considerations.

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Intrusion, Viruses, DoS attack, Insider attacks	Application server security measures	System authentication, authorization, & access control, Role-based Access Control (RBAC), Ant-virus S/W, Firewall, Intrusion detection, system, Security audit, Activity logs, Data backup, Service packs & Patches	Restricted access control, to the premises, CCTV Cameras
Spurious data attacks: SQL Injection	Validate & sanitize input data before passing it to SQL Query	Use stored or extended procedures to avoid granting access to tables. Strict access control policy, audit, & check the logs.	

3.7.1. Security Threats:

- **Database Server Threats:** Intrusion, viruses, DoS attacks, *etc.*
- **Spurious Data attack:** SQL Injection
- **Insider Attacks:** Disgruntled employees, and saboteurs.

3.7.2. Security Requirements & Solutions:

- System Authentication, Authorization, Access control, Role-based Access Control List (RBAC), Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup, Service packs & Patches
- SQL Injection attack can be prevented by checking for buffer overflows, validate and sanitize input data before passing it to SQL Query , disable script execution by any outside sources, setup appropriate access rights to database, and strict access control policy, audit and check the logs.
- Physical Access Control: Restricted access control to the premises, CCTV cameras.

3.8. EPCIS Query Interface

The security threats, security requirements and solutions are very similar to those mentioned in the above sub-section titled “Reader Interface”. But in this case we need to protect the communication channel between EPCIS Query Interface and EPCIS Repository, & EPCIS Accessing Application, where attacks can be mounted to extract sensitive EPCIS data. These threats could *e.g.,* allow an adversary to access the EPCIS data being retrieved/sent from/to EPCIS Repository (or EPCIS Accessing Application)and corrupt the EPCIS repository database.

3.9. EPCIS Accessing Application

EPCIS Accessing Application can be considered as an application server; therefore the security threats related to application server are also applicable to EPCIS Accessing Application. These security threats, security requirements and solutions are very similar to those mentioned in the above sub-section titled “RFID Middleware”, but with the following additional considerations.

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Unauthorized access to EPCIS data	EPCglobal Subscriber authentication, authorization, access control	X.509 Authentication Framework - digital certificates, digital signatures, public key authentication	X.509 based public key infrastructure
Intrusion, Viruses, DoS attack, Insider attacks	Application server security measures	System authentication, authorization, & access control, Access Control List (ACL), Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup, Service packs & Patches	Restricted access control to the premises CCTV Cameras
Spurious data attacks: Buffer Overflow	Code review, bounds checking	Use of programming language that offer bounds checking (Java, .NET)	
Spurious data attacks: Code Injection	Input validation, input encoding, output encoding	Accepting RFID data in the exact predefined format	

3.9.1. Security Threats:

- Unauthorized Access to EPCIS Data: Some of the EPCIS data must be available to only authorized EPCglobal Subscribers. Therefore it becomes essential for EPCIS Accessing Application to categorize EPCglobal Subscribers based on their credentials (roles and capabilities) and provide only the EPCIS data that is related and relevant to them.

3.9.2. Security Requirements & Solutions:

- EPCglobal Subscriber Authentication, Authorization, & Access Control: EPCIS Accessing Application verifies the EPCglobal Subscribers' X.509 certificates, digital signatures, and public key authentication (X.509 authentication framework).

3.10. Object Name Service (ONS)

Security Threat	Security Requirement	Security Solution
ONS cache poisoning, File Corruption, Unauthorized Updates, IP Address Spoofing, Server to Server threat, Data Interception, Server to Client threat	Similar to Secure DNS (*e.g.*, DNS Security Extensions - DNSSEC)	Origin authentication of DNS data, Data integrity, Authenticated Denial of Existence, Digital Signatures, Digital Certificates, Data Confidentiality, Firewall, Access Control List

Object Name Service (ONS) can be considered as a DNS (Domain Name System) server; therefore the security threats related to DNS server are also applicable to ONS.

3.10.1. Security Threats:

- File Corruption, Unauthorized Updates, ONS cache poisoning, IP address spoofing, Server to Server threat, Data interception, and Server to Client threat

3.10.2. Security Requirements & Solutions:

- Similar to Secure DNS (*e.g.*, DNS Security Extensions - DNSSEC)

- Good system administration: secure backing-up of the files, proper read and write permissions applied. Access Control Lists.
- Origin authentication of DNS data, Data integrity, Authenticated Denial of Existence, Digital Signatures, Digital Certificates, and Data Confidentiality.
- Firewall & Intrusion Detection System.

3.11. Subscriber Authentication Service

Security Threat	Security Requirement	Security Solution	Needed Infrastructure
Unauthorized EPCglobal Subscribers	Providing credentials, EPCglobal Subscriber authorization & authentication	X.509 Authentication Framework - digital certificates, digital signatures, public key authentication	X.509 based public key infrastructure
Eavesdropping	Secure communication channel	SSL-TLS / EAP -TLS	SSL & EAP Protocol

Subscriber Authentication Service can be considered as an application server, therefore the security threats related to application server are also applicable to Subscriber Authentication Service. These security threats and security requirements & solutions are very similar to those mentioned in the above sub-section titled “RFID Middleware", but with the following additional considerations.

3.11.1. Security Threats:

- Unauthorized EPCglobal Subscribers: Some of the EPCIS data must be available to only authorized EPCglobal Subscribers. Therefore it becomes essential to authorize, and authenticate EPCglobal Subscribers based on their credentials and provide only the EPCIS data that is related and relevant to them.
- Intrusion, viruses, eavesdropping, DoS, *etc*.

3.11.2. Security Requirements & Solutions:

- Subscriber Authentication Service, authenticates the identity of an EPCglobal Subscriber, provides credentials that one EPCglobal Subscriber may use to authenticate itself to another EPCglobal Subscriber, without prior arrangement between the two Subscribers, and authenticates participation in network services through validation of active EPCglobal Subscription.
- System Authentication, Authorization, Access control, Access Control List (ACL), Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup, Service packs & Patches.

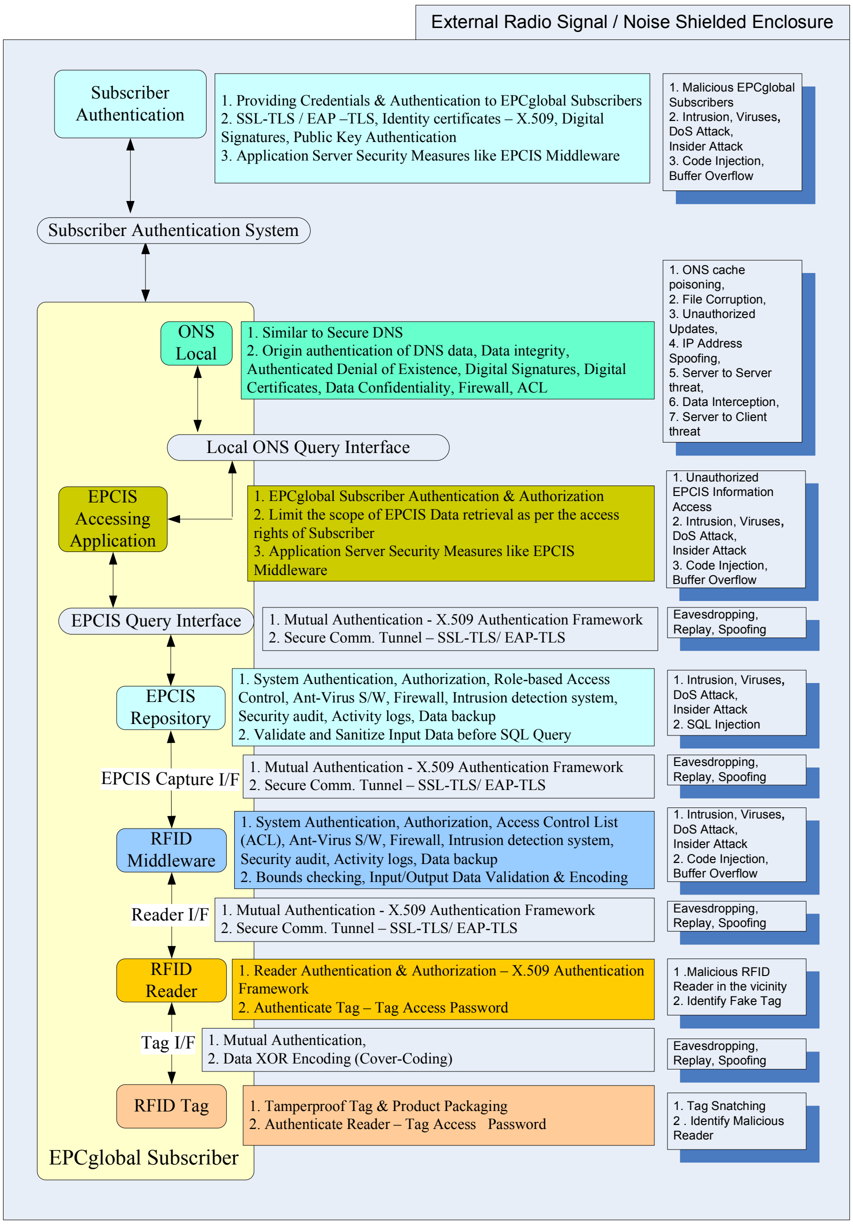
External Radio Signal / Noise Shielded Enclosure
Subscriber Authentication
1. Providing Credentials & Authentication to EPCglobal Subscribers
2. SSL-TLS / EAP –TLS, Identity certificates – X.509, Digital Signatures, Public Key Authentication
3. Application Server Security Measures like EPCIS Middleware
1. Malicious EPCglobal Subscribers
2. Intrusion, Viruses, DoS Attack, Insider Attack
3. Code Injection, Buffer Overflow
Subscriber Authentication System
ONS Local
1. Similar to Secure DNS
2. Origin authentication of DNS data, Data integrity, Authenticated Denial of Existence, Digital Signatures, Digital Certificates, Data Confidentiality, Firewall, ACL
1. ONS cache poisoning,
2. File Corruption,
3. Unauthorized Updates,
4. IP Address Spoofing,
5. Server to Server threat,
6. Data Interception,
7. Server to Client threat
Local ONS Query Interface
EPCIS Accessing Application
1. EPCglobal Subscriber Authentication & Authorization
2. Limit the scope of EPCIS Data retrieval as per the access rights of Subscriber
3. Application Server Security Measures like EPCIS Middleware
1. Unauthorized EPCIS Information Access
2. Intrusion, Viruses, DoS Attack, Insider Attack
3. Code Injection, Buffer Overflow
EPCIS Query Interface
1. Mutual Authentication - X.509 Authentication Framework
2. Secure Comm. Tunnel – SSL-TLS/ EAP-TLS
Eavesdropping, Replay, Spoofing
EPCIS Repository
1. System Authentication, Authorization, Role-based Access Control, Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup
2. Validate and Sanitize Input Data before SQL Query
1. Intrusion, Viruses, DoS Attack, Insider Attack
2. SQL Injection
EPCIS Capture I/F
1. Mutual Authentication - X.509 Authentication Framework
2. Secure Comm. Tunnel – SSL-TLS/ EAP-TLS
Eavesdropping, Replay, Spoofing
RFID Middleware
1. System Authentication, Authorization, Access Control List (ACL), Ant-Virus S/W, Firewall, Intrusion detection system, Security audit, Activity logs, Data backup
2. Bounds checking, Input/Output Data Validation & Encoding
1. Intrusion, Viruses, DoS Attack, Insider Attack
2. Code Injection, Buffer Overflow
Reader I/F
1. Mutual Authentication - X.509 Authentication Framework
2. Secure Comm. Tunnel – SSL-TLS/ EAP-TLS
Eavesdropping, Replay, Spoofing
RFID Reader
1. Reader Authentication & Authorization – X.509 Authentication Framework
2. Authenticate Tag – Tag Access Password
1 .Malicious RFID Reader in the vicinity
2. Identify Fake Tag
Tag I/F
1. Mutual Authentication,
2. Data XOR Encoding (Cover-Coding)
Eavesdropping, Replay, Spoofing
RFID Tag
1. Tamperproof Tag & Product Packaging
2. Authenticate Reader – Tag Access Password
1. Tag Snatching
2 . Identify Malicious Reader
EPCglobal Subscriber

Figure 4: RFID-based Supply Chain Management System Security Architecture

4. Conclusion and Future Work

This paper carries out a through security assessment of the RFID-based supply chain management system that adheres to the EPCglobal Architecture Framework specification. We identified the security threats that affect each of the entities in the framework and proposed some security requirements and needed security solutions. Securing this framework would lead to a secure and safe RFID-based supply chain management system.

The electronic pedigree of the items within the supply chain, and EPCglobal Subscriber's network can be protected by undertaking the following measures: “Subscriber Authentication” a core service of the framework can issue X.509 certificates and public-private security keys to the EPCglobal Subscribers and this helps in mutual authentication, authorization and establishing secure communication channels among the communicating EPCglobal Subscribers. Similarly all the resource rich entities like RFID reader, RFID Middleware, EPCIS Repository, EPCIS Accessing Application, and ONS can authenticate, authorize and establish secure communication channels by using X.509 Authentication Framework and technologies like SSL-TLS and EAP-TLS. We also need to protect application servers (RFID Middleware, EPCIS Accessing Application) and database servers (EPCIS Repository) by installing system authentication and role-based access control, firewall, intrusion detection system, anti-virus software, and input data and SQL query validation. But the threats from cloned RFID tags, malicious snooping RFID readers, and unauthorized tag's data access and manipulation can only be prevented by incorporating a tag-reader mutual authentication scheme.

Our future work includes developing a secure approach where the consumer can use his/her mobile phone (Mobile RFID technology) to scan a particular tag attached to an item and then connect to the manufacturer's EPCIS Accessing Application in order to verify if the product is genuine or fake. In this way consumers can participate in the fight against counterfeit products by easily detecting and notifying authorities if they come across any counterfeit products.

References

[1] EPCglobal IncTM, http://www.epcglobalinc.org/

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

[3] EPCglobal Architecture Framework Version 1.0 (2005), EPCglobal Specification, http://www.epcglobalinc.org/standards/

[4] EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz – 960MHz Version 1.0.9 (2005), EPCglobal Ratified Standard, http://www.epcglobalinc.org/standards/

[5] EPCglobal Certificate Profile (2006), EPCglobal Ratified Standard, http://www.epcglobalinc.org/standards/