# Design and Implementation of an RFID-based Enterprise Application Framework based on Abstract BP and Kerberos

**Kyuhee An*, Kiyeal Lee*, and Mokdong Chung***

**Abstract:** Recently, RFID technology has attracted considerable attention in many industry fields. The RFID environment requires a standard architecture for the smooth exchange of data between heterogeneous networks. The architecture should offer an efficient standard environment, such as a communication environment based on Web Services, PKI or Kerberos-based security, and abstract business processes which could be used in the diverse domains. Therefore, in this paper, we propose an Enterprise Application Framework (EAF) which includes a standard communication protocol, security functions, and abstract level business processes. The suggested architecture is expected to provide a more secure and flexible security management in the dynamic RFID application environments, and is expected to provide an abstract business event for the development of business processes which could apply RFID technology to the existing systems.

**Keywords:** *RFID, EPCglobal Network, Framework, Business Process, Computer Security*

## 1. Introduction

RFID (Radio Frequency Identification) technology is attracting considerable attention in the ubiquitous environment. In particular, this technology, which could improve the efficiency of enterprise businesses, is a matter of common interest in the field of logistics.

In the ubiquitous environment, anyone could easily gain access to all shared information; as such, there are a number of potentially serious consequences. Therefore, provide security services, such as authentication, data protection, and authorization, are required to prevent the side effects which may arise due to security problems [4].

The EPCglobal Network should have a secure means to connect servers containing RFID relevant information to the items identified by EPC (Electronic Product Code) codes. The servers, called EPC Information Services, are connected to diverse participants via a set of network services. All participants in the EPCglobal Network will store relevant information in their own EPCIS servers [1, 2]. Even though the enterprise companies need to standardize RFID-related business processes, they do not have a proper standardized architecture for RFID business processes.

To provide these properties to the RFID environment, we propose an Enterprise Application Framework (EAF) which includes a standard communication protocol, security functions, and abstract level business processes.

The EAF architecture provides an integrated authentication model which applies RBAC to Kerberos for a more secure and adaptive authentication environment. Moreover, it offers RFID-related abstract business processes which might be used in diverse domains in view of its reusability and extensibility. Therefore, the proposed architecture is expected to provide a more secure and flexible security management in the dynamic RFID application environments. Also, EAF offers an abstract class as well as a concrete class to deal with a specific business; thus domain programmers could construct their own specific programs efficiently and easily using the derived class from the EAF abstract class and EAF concrete class.

Consequently, the developer will be able to build RFID applications efficiently using the abstract BP API offered by EAF even if they do not have much knowledge about the EPCglobal Network, RFID, Web Services, and/or security.

The remainder of this paper is organized as follows. In the next section, we will deal with related work. Section 3 presents an overview of the Enterprise Application Framework, while the details of the abstract business processes and security module are considered in section 4 and section 5, respectively. In section 6, we outline an example of constructing WMS based on EAF, and present the conclusion in Section 7.

Manuscript received October 4, 2005; accepted December 4, 2006.
This work was supported by the Regional Research Centers Program (Research Center for Logistics Information Technology), granted by the Korean Ministry of Education & Human Resources Development.
**Corresponding Author:** Mokdong Chung .
* Pukyong National University (mdchung@pknu.ac.kr)

## 2. Related Work

### 2.1 EPCglobal Network

The EPCglobal Network is a method by which RFID technology is used in the global supply chain by using

inexpensive RFID tags and readers to pass EPCs, and then leveraging the Internet to access large amounts of associated information that can be shared among authorized users. [3].

Figure 1 shows the overall structure of the EPCglobal Network which might occur in typical enterprise transactions.

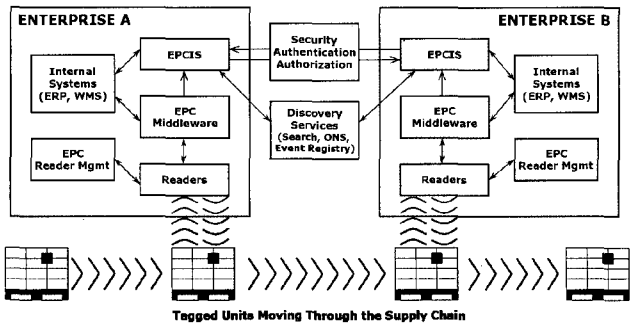



**Fig. 1. Structure of the EPCglobal Network**

To capture data, EPC tags carrying unique EPCs are affixed to containers, pallets, cases and/or individual units. Then, EPC readers strategically placed at gateways throughout the supply chain will read each tag as it passes and communicate the EPC and the time, date and location of the reading to the network. EPC Middleware will control and integrate the EPC tags, readers and local infrastructure at the individual site. Once the information has been captured as described above, the EPCglobal Network utilizes Internet technology to create a network for sharing that information among authorized trading partners in the global supply chain. Similar to Internet technology, the Object Naming Service (ONS) within the Discovery Services serves as White Pages that convert the EPC to a URL, which is then used to point local computers to a location where information associated with that EPC can be found. From there, actual access to data in the EPCglobal Network is managed at the local level by the EPC Information Services (EPC IS) where the company itself designates which trading partners have access to its information.

### 2.2 Partner Interface Processes (PIPs)

Partner Interface Processes (PIPs) are the result of extensive research to identify the business processes at every level of the supply chain [7]. They are a set of generic, standardized processes that could serve as the basis for real-world, business-to-business alignment. PIPs aim to encapsulate business processes by specifying the structure and format of business documents as well as the activities, actions, and roles for each trading partner.

PIPs are a specification and not an implementation; they give the trading partners that adopt RosettaNet the flexibility to implement the PIP specifications themselves or to purchase third-party products that reduce the development overhead. RosettaNet divides the entirety of the e-business supply chain domains into seven groups of core business processes, called "clusters", plus an eighth cluster that is used for administrative purposes. Each cluster is made up of two or more segments. Segments are groups of related functionality. Segments are further divided into PIPs, which define one or more Activities, which in turn specify Actions.

### 2.3 Kerberos

Kerberos is an authentication service developed as part of Project Athena at MIT [8]. Kerberos constitutes an attempt to address the following: Assume an open distributed environment in which users at a workstation wish to access services on servers in terms of distributed manner over the network. We would like to be able to restrict access to unauthorized users, and to be able to authenticate requests for services.

Rather than building elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers, and vice versa. Kerberos relies exclusively on symmetric encryption instead of public-key encryption. Two versions of Kerberos are in common use. Version 4 is still widely used, but Version 5 corrects some of the security deficiencies of Version 4 and has been issued as a proposed Internet Standard [8].

### 2.4 GRBAC (Generalized Role-Based Access Control)

Access control has a great impact on integrity, confidentiality, and availability. Traditional RBAC is very useful, but it suffers from subject-centric limitations that restrict the policy designer to a subject-oriented viewpoint. GRBAC is an extension of RBAC that removes the subject-centric limitations, allowing the organizational power of roles for grouping environment states and objects, in addition to subjects.

A subject role in GRBAC is analogous to a traditional RBAC role. Each subject is authorized to assume a set of subject roles. The GRBAC model allows policy designers to specify the system state through environment roles. An environment role can be based on any system state that the system can accurately collect. Object roles allow us to capture various commonalities among the objects in a system, and to use these commonalities to classify the objects into roles [6].

## 3. Overview of the EAF Framework

This section describes the EAF framework architecture for RFID enterprise application development and its functions.

### 3.1 Enterprise Application Framework Architecture

EAF (Enterprise Application Framework) is a framework that allows developers to develop their own domain specific RFID applications efficiently.

Figure 2 shows the overall EAF structure.

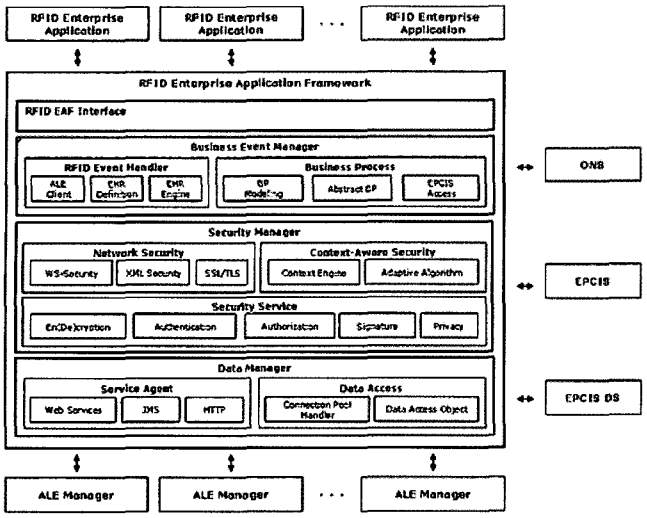



**Fig. 2.** Enterprise Application Framework

The EAF framework consists of three managers: Data Manager, which defines the communication between other systems and EPC event transmission, Security Manager, which defines the security issues, and Business Event Manager, which defines the management of EPC events.

EAF can be applied to various platforms because it is based on the standard environment, including EPCglobal Network, Web Services, XML, and so on. This framework supports efficient communication interfaces between external systems through several communication protocols, and it offers a Kerberos-based security service. Moreover, it supports abstract business processes which might be used in the diverse domains, and the domain programmer could make RFID enterprise applications easily due to the inheritance of abstract BP in the EAF framework. The suggested architecture is expected to provide a more secure and flexible security management in the dynamic RFID application environments.

## 3.2 Function of EAF

### *3.2.1 Data Manager*

Data Manager incorporates a function to access external systems using several communication protocols, such as Web Service, JMS, Socket, and so forth. It includes the Data Access module, which is in charge of input and output processing of data by accessing the databases, and it offers flexibility in the changing of the external system by utilizing the Service Agent module. This module provides a function for gaining access to EPCIS, EPCIS DS and ONS, and/or other outer systems.

### *3.2.2 Security Manager*

Security Manager provides an appropriate authentication model to the distributed service environment connected to the network. In the RFID platform, an authentication mechanism to the entire platform, rather than to each system, is required; moreover, every service in the platform should be available by one authentication technique. Since the device computing power of the RFID platform environment is not sufficient, it is difficult to apply a complex computing algorithm, such as a pure public-key encryption algorithm. We need a light version of PKI such as SPKI/SDSI. In this module, we utilized Kerberos-based security services. In addition to this, flexibility and effective authentication, and an authorization granting environment are provided by applying RBAC.

### *3.2.3 Business Event Manager*

Business Process Manager implements various business process functions in the RFID applications. RFID Event Handler processes the EPC events received from the middleware, and transforms them into higher level business events. The Business Process module is in charge of requests and the processing of the RFID event for the RFID application. EAF offers an abstract business process which might be used in the diverse domain applications. Therefore, domain specific programmers produce their own domain specific systems by extending abstract BPs and their own added codes.

# 4. EAF Abstract Business Model

## 4.1 Common Business Classification

In this paper, we classified the business processes (BP) by major functions, especially from the viewpoint of SCM (Supply Chain Management), WMS (Warehouse Management System), and CRM (Customer Relationship Management), all of which represent typical logistical business. We classified the overall business processes into six categories in the top level function, and each business function may be divided into sub-functions which consist of a BP hierarchy as shown in Figures 3 to 8.

### *4.1.1 Product Information Management*

Product Information Management is the function by which static supply chain information relating to a specific product is managed. This function updates the product information periodically, and requests detailed information on a specific product. Figure 3 shows Product Information Management.

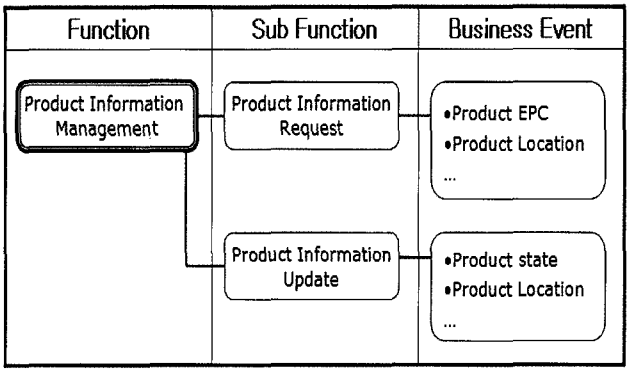



**Fig. 3.** Product Information Management

#### *4.1.2 Total Inventory Management*

Total Inventory Management is the function by which business events relating to the entire inventory are managed. This function forecasts the demand of the customer, determines the quantity to be sold and product supplements, and so on. Figure 4 shows Total Inventory Management.

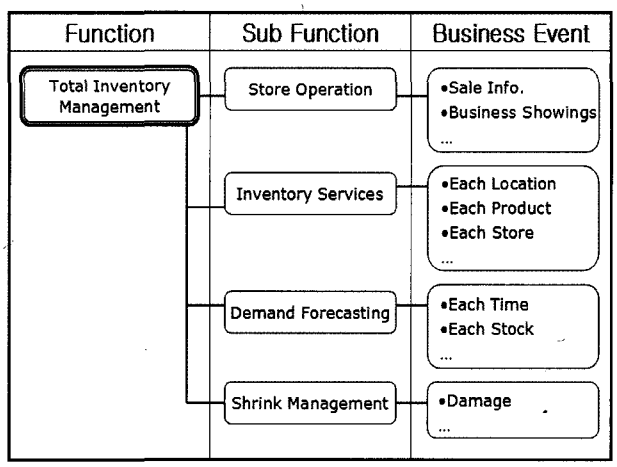



**Fig. 4.** Total Inventory Management

#### *4.1.3 Order Management*

Order Management is the function by which the overall supply chain is managed. This function manipulates the business processes of the transportation, shipping, loading, warehousing, management of packaging, and so on. Figure 5 shows Order Management

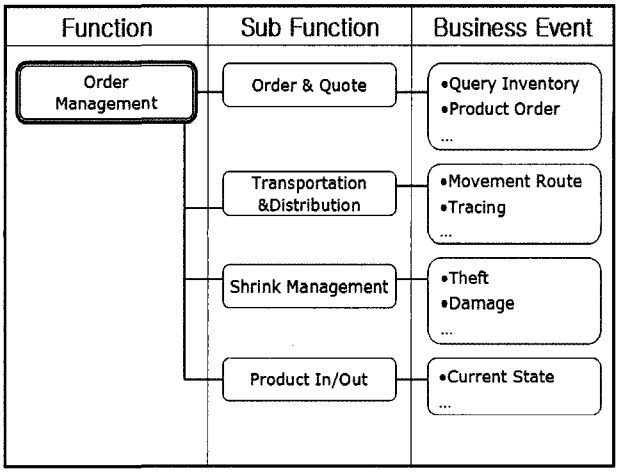



**Fig. 5.** Order Management

#### *4.1.4 Partner Management*

Partner Management is the function by which information on trading partners is managed. This function manipulates the business process of the product information such as the treatment of trading partners, distribution information, and trading cost, etc. Figure 6 shows Partner Management.

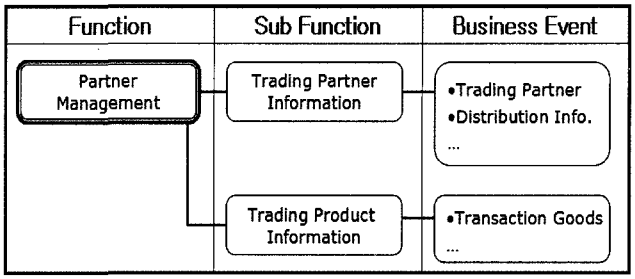



**Fig. 6.** Partner Management

#### *4.1.5 Manufacturing Management*

Manufacturing Management is the function by which the product is managed. This function handles the business processes of tagging, the initialization of product information, packaging information, and so forth. Figure 7 shows Manufacturing Management.

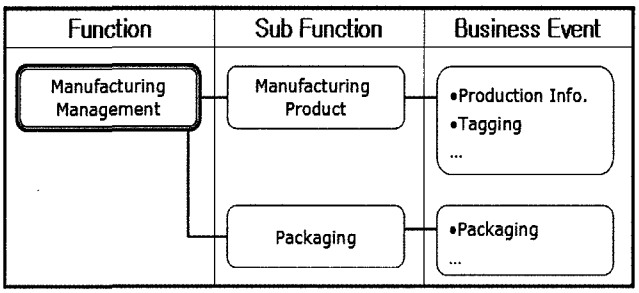



**Fig. 7.** Manufacturing Management

#### *4.1.6 Service and Event Management*

Service and Event Management is the function by which additional services for service enhancement are managed. This function addresses such business processes as the processing of the sold product and other additional services. Figure 8 shows Service and Event Management.

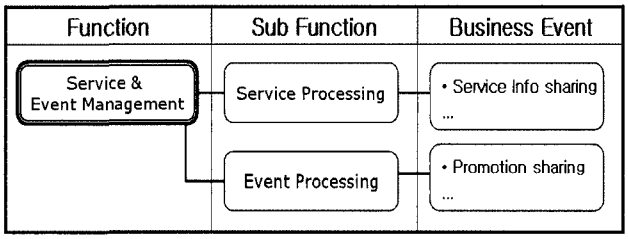



**Fig. 8.** Service and Event Management

### 4.2 Abstract Business Process

The classified business events suggested in this paper provide Java abstract class API. EAF offers an abstract class as well as a concrete class to deal with a specific business, thus the domain programmers could construct their own specific programs efficiently and easily using the derived class from the EAF abstract class and the EAF concrete class.

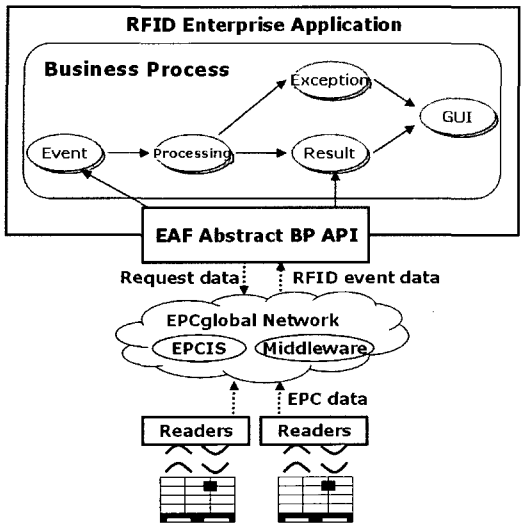



**Fig. 9.** Abstract Business Process API

Consequently, the developers can build RFID applications efficiently by using the abstract BP API offered by EAF even if they do not have much knowledge of the EPCglobal Network, RFID, Web Services, and/or security. Therefore, the developers can reuse the common business functions of logistics through the abstract business process API, and they simply apply their own suitable classes to each domain by inheriting these abstract APIs. Figure 9 shows the overall diagram of abstract business process application.

### 4.3 Example of Business Process (Warehousing)

Figure 10 shows the overall procedure of the abstract business process API which might occur in an RFID-assisted warehousing application.

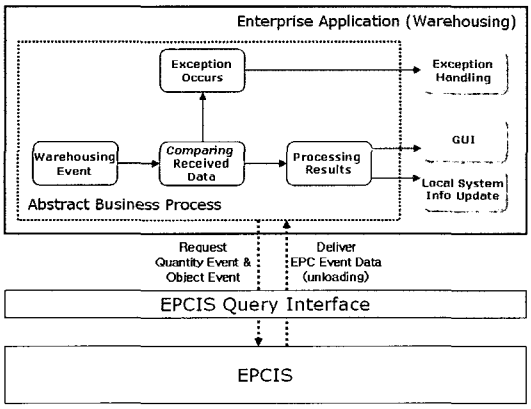



**Fig. 10.** Example of the Warehousing Business Process

The abstract business process (BP) has the function of requesting the necessary EPC related business event for a warehousing application. As shown in Figure 10, the Abstract Business Process requests a quantity event and an object event for the processing of goods.

The abstract business process deals with the common business events defined in section 4.1 using the received EPC event data. A common business event related to the warehousing becomes aware of a warehousing event, and compares the received product list with the expected product list. If the product lists of both are identical, it gathers data and delivers to the user product-detailed information, such as product list, time, and other related information. If the lists are not equal, it creates an exception on the loss of the product. Then the domain programmer implements abstract functions, i.e. the gray boxes in the Enterprise Application in Figure 10, to develop their own specific RFID applications according to this result.

Figure 11 shows an example of the Retailer and Distributor processes. The Retailer and Distributor systems inherit Warehousing abstract BP in order to process Retailer and Distributor business events related to the warehousing. Warehousing abstract BP provides several common concrete methods as well as common abstract methods with the domain specific programmers. Therefore, the domain specific programmers of the Retailer and Distributor systems produce their own domain specific systems by extending abstract BPs and their own added codes. This environment is effective in developing applications since it is easier and faster to develop RFID related applications using this technology.

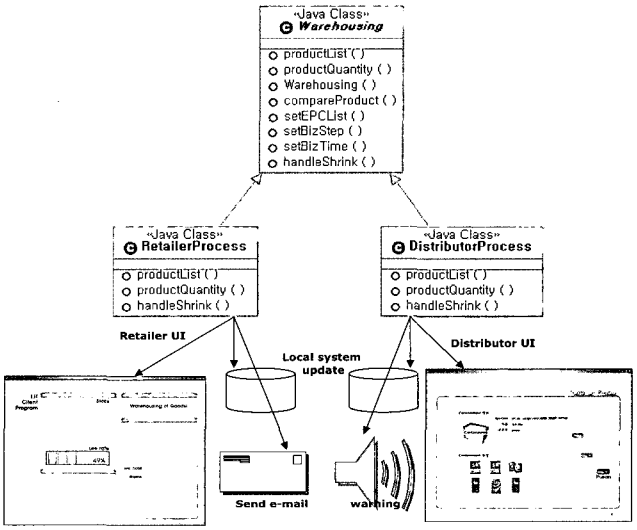



**Fig. 11.** Example of Retailer and Distributor Systems using Warehousing Abstract BP

## 5. EAF Security Model

### 5.1 Authority Management Model using RBAC

Figure 12 is an access control model which controls various authorizations according to the diverse services using RBAC. This model is the foundation of the Access Control Server (ACS).

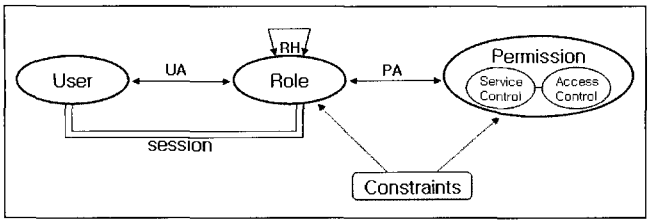



**Fig. 12.** RBAC Model

- User: User is a client of the RFID system. Other users may exist according to the domain developed by using EAF.
- Role: Role is a task function or a name related to responsibility and authority within the domain of the system.
- Permission: Service Control of Permission determines whether the specific service of the client is permitted to access the service or not. Access Control determines whether the specific access mode is to be approved within the permitted service or not.
- Constraints: Stronger and more detailed access control will be executed through various constraints, such as constraints on the service accessing location and time of the client. (For example, accessing the service on holidays or at night from outside of the warehouse)

The requirement for access control is as follows.

[IDc, role, target_service, access]

First, ACS verifies whether the user has been approved; then it checks the role to process the corresponding authority and the service to access. If the access of the service is permitted, it determines whether the specific accessing action is approved. The overall procedure is shown in Figure 13.

```
Access_Request (ID, role, target_service, access)
    IF (role_member (ID, role)) AND
       role_target (target_service, access, role)) THEN
          return accept
    ELSE return reject

role_member (ID, role)
    IF (authorized ID by role) THEN
          return true
    ELSE return false

role_target (target_service, access, role)
    IF (associated target_service with role) THEN
       IF (associated access with role) THEN
             return true
       ELSE return false
    ELSE return false
```

**Fig. 13.** Overall procedure of Authentication Model

## 5.2 Authentication and Authority Management Model based on Kerberos

Figure 14 shows the integrated authentication model which is proposed in this paper. This model consists of a Client, Authentication Server (AS), Ticket-Granting Server, and Access Control Server (ACS).

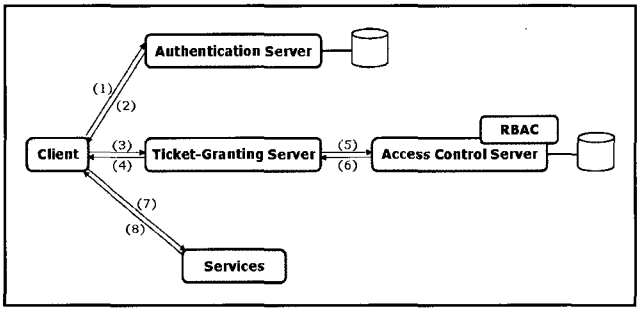



**Fig. 14.** Integrated Authentication Model

The integrated authentication model accomplishes the authentication protocol as follows. The suggested protocol includes the accessing action to the Authentication in step (3). Table 1 illustrates authentication protocol based on Kerberos and RBAC.

**Table 1.** Authentication Protocol based on Kerberos and RBAC

| Authentication Service Exchange |
|---|
| (1) C → AS : Options ‖ $ID_c$ ‖ $Realm_c$ ‖ $ID_{tgs}$ ‖ Times ‖ $Nonce_1$ |
| (2) AS → C : $Realm_c$ ‖ $ID_c$ ‖ $Ticket_{tgs}$ ‖ $Ek_c[K_{c,tgs}$ ‖ Times ‖ $Nonce_1$ ‖ $Realm_{tgs}$ ‖ $ID_{tgs}]$ |
| $Ticket_{tgs} = Ek_{tgs}[Flags ‖ K_{c,tgs} ‖ Realm_c ‖ ID_c ‖ AD_c ‖ Times]$ |
| **Ticket Granting Service Exchange** |
| (3) C → TGS : Options ‖ $ID_s$ ‖ Times ‖ $Nonce_2$ ‖ $Ticket_{tgs}$ ‖ $Authenticator_c$ |
| (4) TGS → ACS : $Ek_{acs,tgs}[ID_c ‖ ID_s ‖ access_c ‖ TS_4]$ |
| (5) ACS → TGS : $Ek_{acs,tgs}[ID_c ‖ ID_s ‖ authority_c]$ |
| (6) TGS → C : $Realm_c$ ‖ $ID_c$ ‖ $Ticket_s$ ‖ $Ek_{c,tgs}[K_{c,s}$ ‖ Times ‖ $Nonce_2$ ‖ $Realm_s$ ‖ $ID_s]$ |
| $Ticket_{tgs} = Ek_{tgs}[Flags ‖ K_{c,tgs} ‖ Realm_c ‖ ID_c ‖ AD_c ‖ Times]$ |
| $Ticket_s = Ek_s[Flags ‖ K_{c,v} ‖ Realm_c ‖ ID_c ‖ AD_c ‖ Times ‖ authority_c]$ |
| $Authenticator_c = Ek_{c,tgs}[ID_c ‖ Realm_c ‖ TS_1 ‖ access_c]$ |
| **Client/Services Authentication Exchange** |
| (7) C → S: Options ‖ $Ticket_s$ ‖ $Authenticator_c$ |
| (8) S → C: $Ek_{c,s}[TS_2 ‖ Subkey ‖ Seq\#]$ |
| $Ticket_s = Ek_s[Flags ‖ K_{c,v} ‖ Realm_c ‖ ID_c ‖ AD_c ‖ Times ‖ authority_c]$ |
| $Authenticator_c = Ek_{c,tgs}[ID_c ‖ Realm_c ‖ TS_2 ‖ Subkey ‖ Seq\# ‖ access_c]$ |

| Notations | |
|---|---|
| $ID_c$, $ID_{tgs}$ | Identifier of Client, TGS |
| $AD_c$ | Network address of C |
| $TS_k$, Times | Timestamp |
| $K_{a,b}$ | Session key between a and b |
| $Ticket_{tgs}$ | Authentication granting ticket |
| $Ticket_s$ | Service granting ticket |
| Authenticator | Authenticating information |
| AS | Authentication Server |
| TGS | Ticket Granting Server |
| ACS | Access Control Server |

In steps (4) and (5), the result is delivered from the processing of the authorization according to the requirement of the suggested RBAC. Afterward, TGS transmits the authority to the client along with the ticket of step (6). At the Service, the client is verified by checking the ticket and the authentication and its result is delivered to the client [6].

## 6. Constructing Secure WMS using EAF

### 6.1 Development Environment

This section describes an RFID application - the secure WMS (Warehouse Management System) based on the EAF framework, which consists of Manufacturer, Distributor and several Retailers. Manufacturer, Distributor and Retailers have their own EPCIS and readers. The products of Manufacturer are delivered to Distributor, and Distributor distributes them to suitable Retailers. We assumed one Manufacturer, one Distributor, and two Retailers for the experiment, and used four readers and several RFID tags. Moreover, we developed GUI to confirm the result based on EAF. The secure WMS system architecture is shown in Figure 15.

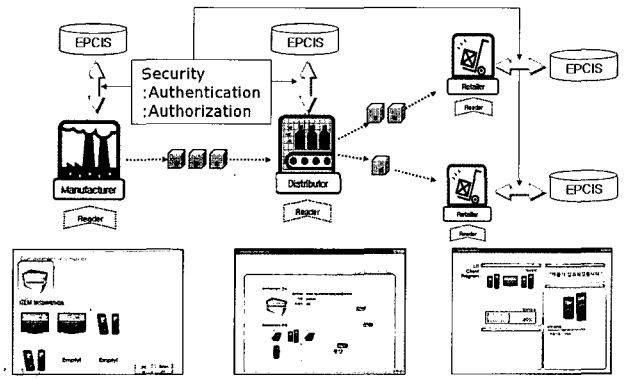



**Fig. 15.** Secure WMS System Architecture

The development environment is shown in table 2.

**Table 2.** Development Environment of EAF

| Platform/Tools/Spec | Version | Description |
|---|---|---|
| MS Windows OS | 2003 Server | Platform |
| J2SDK | 1.5 | Java Development Kit |
| JWSDP | 1.6 | Web Services Development Pack |
| Tomcat for JWSDP | 5.0 | Web Application Server |
| MySQL | 3.23.57 | Database |
| JCE | 1.2.2 | Java Cryptography Extension |
| ALE | 1.0 | ALE Spec |
| Alien | 900MHz | RFID Reader |
| GTIN-64 | | EPC Tag |

### 6.2 Scenario

(1) [*Authentication*] A User who wants to use the Manufacturer application sends his/her ID and password information.
Later, this ID/Password-based authentication mechanism will be replaced by the RBAC-based Kerberos authentication model which is currently under construction.
(2) The Manufacturer application obtains information on login and authority from databases.
(3) The User puts product data on EPCIS.
(3-1) [*Access Control*] If there is no permission to use EPCIS, putting data on EPCIS would be denied by the Manufacturer application.
(3-2) [*Access Control*] If permission is granted, the Manufacturer application finds the session key which was made between the Manufacturer application and EPCIS.
(4) [*Encryption*] The Manufacturer application encrypts data using the session key.
(4-1) [*Key Agreement*] If there is no session key, the Manufacturer application will make a session key by communicating with EPCIS.
(5) The Manufacturer application sends the encrypted form of data to EPCIS.
(6) EPCIS decrypts the received data that was encrypted by the Manufacturer application, and inputs the data into itself.

## 7. Conclusions

In this paper, we proposed an Enterprise Application Framework (EAF) which provides an efficient development environment for RFID application. The EAF architecture offers an efficient standard environment, such as a communicating environment based on Web Services, Kerberos-based security, and an abstract business process which could be used in diverse domains.

Domain specific programmers can produce their own domain specific systems by reusing common BPs, and by extending abstract BPs and their own added codes. Furthermore, they can develop applications enabling them to offer a stronger authentication environment by using the RBAC-based Kerberos Model.

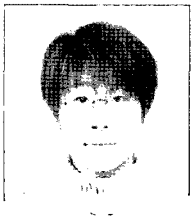
Consequently, developers could build secure RFID applications efficiently using abstract BP API and the RBAC-based Kerberos security module offered by EAF even if they do not have much knowledge of the EPCglobal Network, RFID, Web Services, and/or security.

In the future, we will extend Security Manager and Data Manager n accordance with the RFID environment. Thus, we will extend the authentication by using GRBAC in order to manage the authority in each service. Also, we should extend the business processes into the wider area, and verify the efficiency of the EAF framework by utilizing it in the related field.

## Reference

[1] EPCglobal, The Application Level Event (ALE) Specification, Version 1.0, 2005.
[2] EPCglobal, EPC Information Services (EPCIS) Version 1.0 Specification, Last Call Working Draft Version, March, 2006.
[3] EPCglobal, The EPCglobal Architecture Framework, EPCglobal Final Version, July, 2005.
[4] Securing RFID Data for the Supply Chain, http://www.versign.com/epc.
[5] Kyuhee An and Mokdong Chung, "ALE Application Framework for Constructing Effective RFID Application," EEE'06, USA, 2006, pp. 215-220.
[6] M. J. Convington, et al., "Generalized Role-Based Access Control for Securing Future Applications," In the Proceedings of the 23rd National Information Systems Security Conference (NISSC), Baltimore, 2000, pp. 115-125.
[7] RosettaNet,http://portal.rosettanet.org/cms/sites/RosettaNet.
[8] William Stallings, Cryptography and Network Security, Pearson Education, INC. Prentice Hall, 2003.

**Kyuhee An**
She received the BS degree in Computer Multimedia Engineering from Pusan University of Foreign Studies in 2004 and an MS degree in Computer Engineering from Pukyong National University in 2007, respectively. She is currently a member of the Computer Security & Artificial Intelligence Lab at Pukyong National University.



**Kiyeal Lee**
He received the BS degrees in Computer Multimedia Engineering from Pukyong National University in 2006 and 2008, respectively. He is currently a member of the Computer Security & Artificial Intelligence Lab at Pukyong National University.

**Mokdong Chung**
He received the Ph.D. degree in Computer Engineering from Seoul National Univ. in 1990. He was a professor at Pusan University of Foreign Studies from 1985 to 1996. And he has been a professor at Pukyong National University since 1996. His research interests are in the areas of OOP technology, computer security for application, intelligent Agent, E/M-commerce security, web application and context aware computing. He is a member of IEEE, KISS, KIPS, KIISC, and KMMS.