

ALE Application Framework for Constructing Effective RFID Application[†]

Kyuhee An

*Dept. of Computer Engineering
Pukyong National University
599-1 Daeyeon-3Dong, Nam-Gu, Busan,
608-737, Korea
heeya0101@hotmail.com*

Mokdong Chung

*Dept. of Computer Engineering
Pukyong National University
599-1 Daeyeon-3Dong, Nam-Gu, Busan,
608-737, Korea
mdchung@pknu.ac.kr*

Abstract - RFID technology could greatly improve the business efficiency. EPCglobal Network suggests a kind of interface, called ALE (Application Level Events), for an efficient RFID developing environment. Moreover authorization function should be available along with authentication for the security of the decentralized RFID environment. In this paper, we propose a framework for the development of secure RFID application based on ALE. Additionally, it contains more efficient accommodating authentication function, which adds GRBAC (Generalized Role Based Access Control) to the existing Kerberos authentication model.

Keywords: RFID Application Framework, Authentication, Authorization, Kerberos, GRBAC, RFID.

1 Introduction

Due to the notable improvement on work productivity, stock management, product tracking, and high integrity rate through the RFID technology, various companies have a lot of interest in the RFID technology. They, however, are reluctant to invest on this technology because the standardization of RFID is in process, and the unification of the current legacy system is essential for the effective RFID system [1, 2].

For this reason, EPCglobal Network suggests a kind of interface, called ALE (Application Level Events) in order to establish more effective RFID developing environment. Nevertheless, a lot of existing systems have limitations, which are not able to accommodate diverse business demands like RFID. In order to overcome this, the application is required of unification to the legacy

application or conversion to a new application. Although there are various standard interfaces such as J2EE, Web Services, and XML to support, absence of standard architecture results in pursuing only diversity [4, 5]. Besides, since the RFID platform demands a lot of data processing and is lacking in device computing capability in the decentralized environment, authentication protocol based on Single Sign-On, symmetric encryption and authorizing environment should be considered to provide a firm security in such conditions.

This paper focuses on the development of a framework, which can effectively define, request, and process EPC data desired by the user. It also suggests several functions for more effective developing environment of the RFID application, Web Services that is decentralized computing technology, and ALE application Framework (AAF) using Kerberos v5 and GRBAC (Generalized Role Based Access Control) for the security reasons.

The following is the structure of the remaining paper: section 2 deals with related research. Section 3 examines the structure and the characteristic of AAF. Section 4 shows a demonstrating system which applies to AAF. In section 5, the conclusion and the future research is discussed.

2 Related Work

2.1 EPCglobal Network: ALE

EPCglobal network shows new standard, called *Application Level Events (ALE)*, which is developed from the concept of a middleware, called *Savant*. The role of the ALE is to provide means to process the event data which have

[†] 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.

been collected by the RFID reader and to deliver them to the higher-level applications [3, 6].

On looking into the structure and components of the EPCglobal, RFID reader delivers identified tag data to the middleware, ALE Engine. Middleware is trying to filter out various redundant tag data, and transmit accumulated/filtered tag data index to EPCIS or applications.

2.2 Kerberos

Kerberos is a computer network authentication protocol which allows users communicating over the insecure network to prove their identities to one another in a secure manner. Kerberos prevents eavesdropping or replay attacks, and ensures the integrity of the data. Its designers aimed primarily at a client-server model, and it provides mutual authentication — both the user and the service verify each other's identity.

Kerberos v5 provides a number of improvements over version 4. Kerberos v5 [7] is intended to address the limitations of version 4 in two areas: environmental shortcomings and technical deficiencies.

2.3 GRBAC

Access control is one of the most important aspects of computer security. It has a great impact on integrity, confidentiality, availability. Traditional RBAC (Role-Based Access Control) is very useful, but it suffers from subject-centric limitations that restrict the policy designer to a subject-oriented viewpoint. GRBAC (Generalized Role Based Access Control) is an extension of RBAC that removes the subject-centric limitation, allowing the organizational power of roles for grouping environment states and objects, in addition to subjects [8].

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 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 use these commonalities to classify the objects into roles [8].

3 ALE Application Framework Architecture

3.1 ALE Application Framework

AAF is a framework for RFID application development, consists of Data Manager for the communication with other systems and EPC event transmission, Security Manager for the security issues, Event Manager for the management EPC event, Business Process Manager for the management business process, and GUI for the clients. This allows clients to develop and use the RFID application based on ALE efficiently and easily. Also, it offers diverse communicating environments and various platforms to the standard, and can get the contextual information on EPC data which is related to EPCIS, ONS, and EPCDS. Figure 1 shows AAF overall structure which is proposed in this paper.

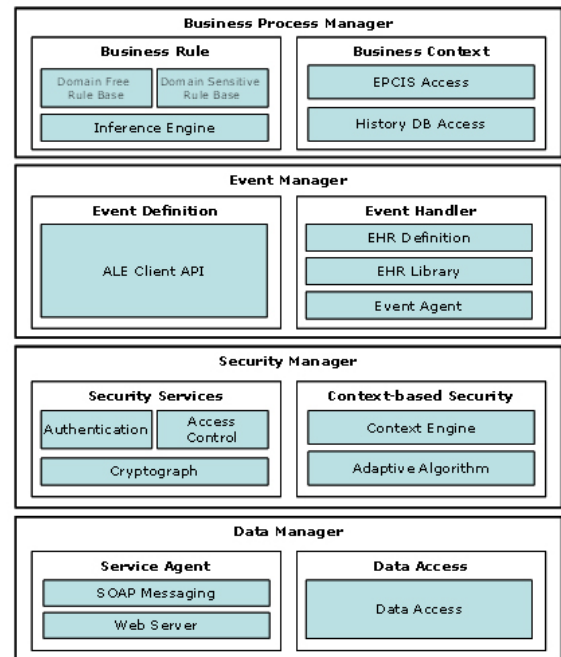


Fig. 1. ALE Application Framework

3.2 ALE Application Framework

3.2.1 Data Manager Module

Data Manager offers function to access outer systems through databases and Web Services. It includes Data Access module, which is in charge of input and output processing of the data by approaching the database, and gives maximum flexibility to the change of outer system by

Web Service module. It also supports various networking protocols such as JMS and Socket without difficulty. It delivers user-defined EPC event (ALE: ECSpec) to middleware through Event Definition of Event Manager, transmits it to Event Handler of Event Manager in order to receive and process the result (ALE: ECRReport), and communicates with EPCIS or other legacy systems.

3.2.2 Security Manager Module

Security Manager provides accommodating authentication model with the distributed service environment connected to the network. In RFID platform, authentication mechanism to the entire platform, not the authentication to each system, is required; moreover, every service in the platform should be available in individual authentication. Since the device computing capacity of the data and distributing environment can be deficient due to the properties of the RFID platform environment, it is difficult to use a complex computing algorithm, such as public-key encryption algorithm. Consequently, considering this condition, it applies to Kerberos, which is an authentication protocol based on the symmetric-key and the concept of Single Sign-On. In addition, effective authentication and authorization granting environment are provided by applying GRBAC, and access control model using Kerberos for the authorization and authentication should coexist in the distribution environment.

3.2.3 Event Manager Module

Event Manager implements the function of defining and processing the EPC event. It includes Event Definition which defines the EPC event desired by a client and Event Handler which processes the event received from the middleware. The Event Handler generates the Logical Event as a semantic-added stage to add valuable contexts to the events received from the middleware through pre-defined rules, and transmits it to the Business Process Manager.

3.2.4 Business Process Module

Business Process Manager implements the function of various business processes in the applications. This module includes Business Rule which implements business logic and processes, and Business Context which grants context to business processes. Business process is defined as flow of XML schema form according to the requirement of user, and process Logical Event to receive meaningful expression from Event Handler.

3.2.5 Graphical User Interface

AAF offers a business process modeling tool, provides lots of flexibility with the users who are not specialists in ALE or RFID system. Thus, users easily define desired EPC event, process its result and the flow of BP processing, and deliver the result to the users. Figure 2 and 3 show typical modeling tools for ECSpec and Business Processes, respectively.

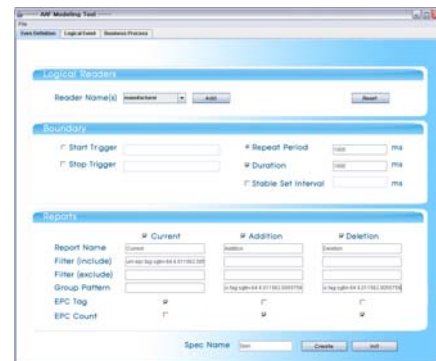


Fig. 2. Modeling Tool: ECSpec

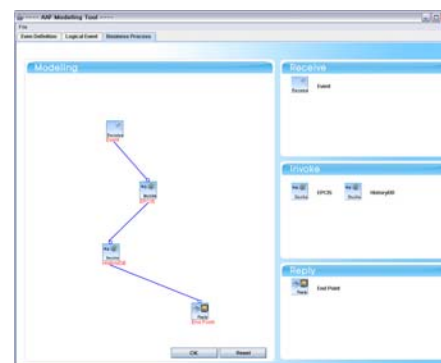


Fig. 3. Modeling Tool: Business Process

Modeling Tool produces ECSpec through the set up of user input for request EPC event to RFID middleware. And it can handle ECRReport to Logical Event. Logical Event helps smooth processing of Business Process. Also user can model BP flow using Logical Event.

3.3 Consolidating Authentication and Authority Management Model

3.3.1 Authority Management Model using GRBAC

Figure 4 is a generalized access control model which controls various authorizations according to the diverse

services using GRBAC. This model is a foundation of Access Control Module (ACM) in the consolidating authentication model of Section 3.3.2.

[Subject, Environment, Object, Operation, permission]

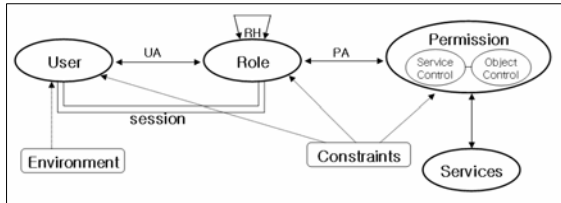


Fig. 4. Suggested GRBAC Model

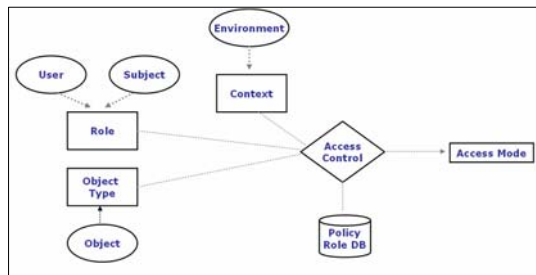


Fig. 5. Logical Access Control Model

- User (Subject Role): User is a client of RFID system. Other users may exist according to the domain developed by using AAF. User may be hierarchical structure according to mission or responsibility of the organization or single-level in nature.
- Role: Role is the task function or name related to responsibility and authority within the domain of the system.
- Permission: Services Control of Permission determines whether the specific service of the client is permitted to access to the service. Object Control determines an access security level about service object where the approach is permitted.
- Environment (Environment Role): Environment has many real-world instances (contextual-information). Access Control determines whether the specific access mode is approved according to the permitted service. And it permits the approach at that object role which allows us to capture various commonalities among the objects in a system.
- Services (Object Role): Services is outer systems of EPCglobal Network or other partner company. Each Service and information of service has a hierarchy structure according to security level.
- Constraints: More strengthened and detailed access control will be executed through various constraints. The requirement for access control is as follows.

Firstly, ACM verifies if the user is approved; then it checks the role to process the corresponding authority and the service to access. The users (subject) must be classified to verify them according to the hierarchy such as Administrator, Plain User, Guest and so on. And then user identity can be mapped to roles by ACM. Also ACM considers environmental information of users. Environment can contain user’s request time, location, boundary and etc.. If the access of the service is permitted, it determines whether the specific accessing operation is approved. Also determine the range of object of service. Permission decides accept or deny, and access level.

Figure 5 shows logical access control model which is proposed to determine an access authority.

3.3.2 Consolidation Authentication and Authority Management Model based on Kerberos

Figure 6 shows the consolidated authentication model which is proposed in this paper. This model extends Kerberos v5 using Access Control Server based on GRBAC.

This model consists of Client, Authentication Server (AS) to authenticate the client, Ticket-Granting Server, and Access Control Manager (ACM).

Database includes information on user, environment, and services for the management of authentication or access control. Also it contains access policy.

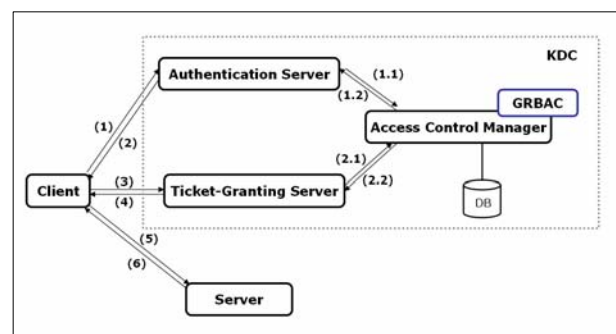


Fig. 6. Consolidation Authentication Model

Consolidated authentication model accomplishes the authentication protocol as follows. Kerberos provides the

data structure so as to permit selectively the ticket and the authentication [9]. The suggested protocol includes the accessing action to the Authentication in step (3). Table 1 illustrates authentication protocol based on Kerberos and GRBAC.

Table.1. Authentication protocol based on Kerberos and GRBAC

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} SR _c]
(1.1) AS → ACS :	ID _c AD _c Times
(1.2) ACS → AS :	ID _c SR _c Times
Ticket _{tgs}	= Ek _{tgs} [Flags K _{c, tgs} Realm _c ID _c AD _c Times SR _c]
Ticket Granting Service Exchange	
(3) C → TGS:	Options ID _v Times Nonce ₂ Ticket _{tgs} Authenticator _c
(4) TGS → C:	Realm _c ID _c Ticket _v Ek _{c, tgs} [K _{c, v} Times Nonce ₂ Realm _v ID _v AA _c]
(2.1) TGS → ACS :	ID _c Realm _c TS ₁ SR _c Operation
(2.2) ACS → TGS :	ID _c TS ₁ AA _c
Authenticator _c	= Ek _{c, tgs} [ID _c Realm _c TS ₁ SR _c Operation]
Ticket _v	= Ek _v [Flags K _{c, v} Realm _c ID _c AD _c Times AA _c]
Client/Server Authentication Exchange	
(5) C → V:	Options Ticket _v Authenticator _c
(6) V → C:	Ek _{c, v} [TS ₂ Subkey Seq#]
Authenticator _c	= Ek _{c, v} [ID _c Realm _c TS ₂ Subkey Seq# AA _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 _v	Server granting ticket
Authenticator _c	Authenticating information
SR _c	Subject role
AA _c	Authority
AS	Authentication Server
TGS	Ticket Granting Server
ACM	Access Control Server

At the step (4) and (5), the result is delivered after processing authorization according to the requirement of the suggested GRBAC. Afterward, TGS transmits the authority to the client along with the ticket (6). At the Server, the client is verified by checking the ticket and the authentication, and its result is delivered to the client.

4 A Typical Warehouse Management System using AAF

4.1 Implementation environment

OS	Windows 2003 Server / Windows XP
RFID Reader	Alien 900 MHz
EPC Tag	GTIN-64

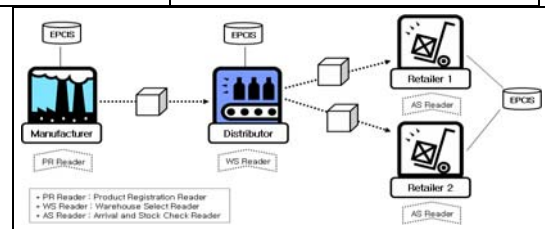


Fig. 7. WMS System Architecture

WMS consist of Manufacturer, Distributor and several Retailers. Each constituent has EPCIS and readers. The product of Manufacturer is delivered to Distributor, and Distributor distributes it to the suitable Retailer. We assumed a Manufacturer, a 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 AAF.

4.2 A Scenario

- (1) Manufacturer delivers the product to the Distributor and saves its related information in EPCIS through the Manufacturer PR reader.
- (2) After saving the information of the received products in EPCIS, Distributor finds out the appropriate Retailer (destination) to the products using WS reader.
- (3) Retailer finds out the content of the current stock with the aid of AS reader. Figure 8 illustrates the GUI of Distributor.

Figure 9 shows information about the deliver to Retailers when the receive products at Distributor.

Figure 10 shows the Retailer's GUI to mark product information of store goods in a Retailer's warehouse.



Fig. 9. Distributor's GUI

5 Conclusion

This paper proposed development of RFID-based application framework, which can effectively define, request, and process EPC data desired by the user, and fits the RFID application for the authentication protocol. It also suggested several functions for more effective developing environment of the RFID application, Web Services that is decentralized computing technology, and adaptive AAF security services using Kerberos v5 and GRBAC for the security reasons.

AAF can be used in the elevation of productivity, quality, and maintenance in the specific fields. Furthermore, each service has authentication sever that makes it unnecessary to detailed log-in process, and it presents the authority managing model using GRBAC in order to manage the authority in each service.

In the future, we need to study business process related research and EAI (Enterprise Application Integration). And we need research on the definite access control policy, requirements of user and etc.

6 References

- [1] EPCglobal US, <http://epcglobalus.gs1us.org/portal/server.pt>.
- [2] Verisign, "The EPC Network : Enhancing the Supply Chain," White Paper, 2004.
- [3] EPCglobal, The Application Level Events (ALE) Specification, Version 1.0 of February 8, 2005.
- [4] Matjaz Juric, PROFESSIONAL J2EE EAI, WROX PRESS, 2002.
- [5] K.C. Oh, et al., "Application Framework Implementation Plan for Quality Enhance with a Software Development Productivity," Army Computerization Agency, 2004.
- [6] Verisign, <http://www.verisign.com>.
- [7] William Stallings, Cryptography and Network Security, Pearson Education, Inc. Prentice Hall, 2003.
- [8] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman., "Role-based access control models," IEEE Computer, Vol. 29, No. 2, February 1996, pp. 38 - 47.
- [9] Michael J. Covington, et al., "Generalized Role-Based Access Control for Securing Future Applications," National Information Systems Security Conference, October 16-19, 2000, pp.115-125.
- [10] J.Kohl and C.Neuman. "The Kerberos Network Authentication Service (V5)," RFC 1510, September, 1993.