World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:10, 2007

Security Enhanced RFID Middleware System

Jieun Song, Taesung Kim, Sokjoon Lee, and Howon Kim

***Abstract*—**Recently, the RFID (Radio Frequency Identification) technology attracts the world market attention as essential technology for ubiquitous environment. The RFID market has focused on transponders and reader development. But that concern has shifted to RFID software like as high-valued e-business applications, RFID middleware and related development tools. However, due to the high sensitivity of data and service transaction within the RFID network, security consideration must be addressed. In order to guarantee trusted e-business based on RFID technology, we propose a security enhanced RFID middleware system. Our proposal is compliant with EPCglobal ALE (Application Level Events), which is standard interface for middleware and its clients. We show how to provide strengthened security and trust by protecting transported data between middleware and its client, and stored data in middleware. Moreover, we achieve the identification and service access control against illegal service abuse. Our system enables secure RFID middleware service and trusted e-business service.

***Keywords*—**RFID Middleware, ALE (Application Level Events), Security.

I. Introduction

In today's intense competition of business market, companies are increasingly forced to reduce costs, rather than increase price, in order to ensure return on investments. Because the efficiency has become a necessary condition in supply chain for survival, RFID technology is expected to enhance the operational efficiency of supply chain management by embedding small silicon chips (RFID tags) in products or packaging. An RFID tag provides a unique identification number (an electronic product code or an individual serial number) that can be read by contact-less readers, which enables automatic real-time tracking of items as they pass through the supply chain. Depending on the RFID tag, it may contain addition storage for application specific use (such as product descriptions, certifications or temporary storage related to process support) or generic functionality embedded into the hardware [1].

RFID technology is already adapted and deployed in a wide area of applications, including supply chain management, retail, anti-counterfeiting, security and healthcare. For example, Benetton has already been forced to reconsider its plans to embed RFID tags in every new garment bearing Benetton's Sisley[3] brand name and Tesco (a UK supermarket chain) in Cambridge was forced to abandon their experiments with an RFID based "smart shelf" technology developed by Gillette[5]. Through the automatic data collection, RFID technology can achieve greater visibility and product velocity across supply chains, more efficient inventory management, easier product tracking and monitoring, reduced product counterfeiting. For reasons of these, VDC forecasts that the global market for RFID middleware is expected to reach an estimated $43 million in 2005. This represents an annual growth rate of 162%. RFID middleware will account for roughly 3% of RFID systems revenues by 2007, or $135 million [4] [6].

However, the most common middleware systems have limitations not to consider security solutions against attack in globally networked RFID environment perfectly. While, due to high sensitivity of data and service transaction within the RFID network, security considerations must be addressed.

In order to guarantee trusted e-business based on RFID technology, we propose a security enhanced RFID middleware system. Our proposal is compliant with EPCglobal ALE (Application Level Events), which is standard interface for middleware and its clients. We show how to provide strengthened security and trust by protecting transported data between middleware and stored data in middleware. Moreover, we achieve the identification and service access control against illegal service abuse.

We present background material in section 2, summarizing EPCglobal RFID middleware features and network architecture relevant to our work. In section 3, we describe attacks and security considerations in EPCglobal RFID network. We consider the problems of data translation and service authority via untrusted application system or middleware clients. We propose security architecture and techniques for enhanced middleware system, i.e., optional data protection and access-control features from the EPCglobal standard in section 4. We conclude in section 5 with avenues for further research.

II. EPCglobal RFID Middleware System

A. EPCglobal Network Architecture

The EPCglobal Network™ is a set of global technical standards aimed at enabling automatic and instant identification of items in the supply chain and sharing the information throughout the supply chain [3]. The set of standards focuses on UHF (Ultra High Frequency) tags and aims to provide a numbering system for unique identification and define how data is stored and transferred. The EPCglobal Network™ consists of five fundamental elements: the ID System (EPC Tags and Readers), Electronic Product Code (EPC), EPC Middleware,

Manuscript received November 15, 2005; revised November 30, 2005. Jieun Song, Taesung Kim, Sokjoon Lee and Howon Kim are with the Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea (e-mail : happybirds, taesung, junny, khw@etri.re.kr).

Object Name Service (ONS)[9] and EPC Information Services (EPCIS). The EPC, which sits on the tags, is basically a number designed to uniquely identify an individual object in the supply chain. The EPC is communicated to readers and then ONS translates the EPC to internet addresses, where further information on the object may be found. To handle the vast amount of exchanged information, RFID middleware manages the data in a way that reduces network traffic and provides a software interface standards – ALE for services enabling data exchange between an EPC reader or network of readers and information systems. EPCIS enables users to exchange EPC-related data with trading partners through the EPCglobal network.

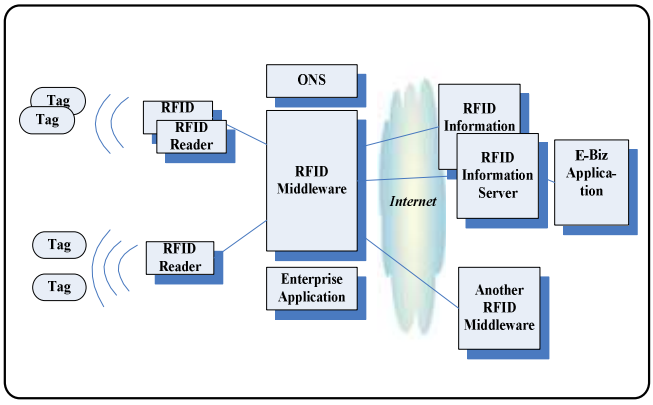

Fig. 1 EPCglobal Network Architecture

The more detailed description of each of these elements is as follows.

1) EPC: The EPC is a globally unique serial number that identifies an item in the supply chain. This allows enquiries to be made about a single instance of an item, wherever it is within the supply chain.
2) The ID System: The ID System consists of EPC tags and EPC readers. EPC tags are RFID devices that consist of a microchip and an antenna attached to a substrate. The EPC is stored on this tag, which is applied to cases, pallets and/or items. EPC tags communicate their EPCs to EPC readers using Radio Frequency Identification. EPC readers communicate with EPC tags via radio waves and deliver information to local business information systems using EPC Middleware.
3) EPC Middleware: EPC Middleware manages real-time read events and information, provides alerts, and manages the basic read information for communication to EPC Information Services as well as a company's other existing information systems. EPCglobal is developing a software interface standard for services enabling data exchange between an EPC reader or network of readers and information systems.
4) EPCIS: EPC Information Services enables users to exchange EPC-related data with trading partners through the EPCglobal Network.
5) Discovery Services: The Discovery Services is a suite of services that enables users to find data related to a specific EPC and to request access to that data. The Object Naming Service (ONS) is one component of the Discovery Services.

B. ALE (Application Level Events)

The EPC Network Architecture defines an interface through which clients (e.g., enterprise applications) may obtain filtered, consolidated EPC data from a variety of sources [8]. Within the EPC network architecture, this interface and the functionality it implies is called "Application Layer Events" or ALE.

1) It provides a means for clients to specify, in a high-level, declarative way, what EPC data they are interested in.
2) It provides a standardized format for reporting accumulated, filtered EPC data that is largely independent of where the EPC data originated or how it was processed.
3) It abstracts the sources of EPC data (e.g., Readers, Barcode scanners) into higher-level notions of "location", thus hiding from clients the details of exactly what physical Readers were used to gather EPC data from a particular location.

A compromise of ALE services undermines an enterprises ability to acquire accurate and timely information about the presence. So ALE service provider, that is; middleware system must describe and support the security technologies as like data protection or access control of ALE service.

III. Middleware Security Considerations

A. Security Assets and Threats

We descript security threats for the scope of middleware, which support ALE service. In special we focus on the weakness between ALE provider and its clients [7]. We show the security assets and enabled attacks in the following Table I.

TABLE I
EPCGLOBAL NETWORK ARCHITECTURE

Asset ID	Asset Type	Threats
A1	Transported Data : Messaging between ALE service provider and ALE client	- Eavesdropping : unauthorized access to message contents - Forgery/Modification : alter message contents - Replay Attack : message replay or other means delivers unauthorized messages
A2	Transported Data : Messaging between ALE service provider and ALE report receiver	- Eavesdropping - Forgery/Modification - Replay Attack - Denial of service : Lower Service availability or performance : DoS
A3	Stored Data : Data resident in implementation of ALE interface	- Corrupts ALE Service/ Configuration - Corrupts ALE Service Credentials

		- Send notification report illegal receiver - Call service API illegally - Abuse stored tag data

B. Security Requirements

In order to protect security asset against threats as the upside, the RFID middleware system need to provide security countermeasures. So the following functions are urgently needed for providing trust services to e-business based on RFID.

1) Identification and Authentication: The ALE service provider must identify the clients and authenticate to prevent illegal clients access the service.
2) Data Transport Protection: In order to protect the data transported between ALE service provider and clients the ALE service provider build the security functions for the integrity, confidentiality, freshness and so on.
3) Service Access Control: Unauthorized users may try to access the ALE service (e.g., stored tag data, ALE service configuration, reader management, middleware resource management, notification report accepter) and it brings the untrusted and confused e-business application systems.

Currently most widely deployed middleware products do not consider the security requirements and do not provide capability.

IV. Security Enhanced Middleware System

A. Secure Middleware System Architecture

In this section, we propose a security enhanced RFID middleware system architecture to support trust and secure ALE service. This enhanced middleware consists of Reader Communication Component, ALE Service Security Component, ALE Service Processing Component and ALE Client Interfaces as shown in Figure 2. Reader Communication Component assists with the reader communication adapter, reader management /monitor and simple filtering/event generator functions for RFID event data. This component conducts reader communication directly. It enables to configure and manage the readers and remove the noise from low data by simple filtering. ALE Service Processing Component operates information related to RFID tag got from reader based on ALE service request of clients. This component consists of Event Cycle Registry/Scheduling, ALE Request Event Capturing, Tag Event Data Collect/ALE Filtering and ALE Event-Response Reporting functions. If this component captures ALE service request from ALE clients, it operates tag data collection and filtering in according to ECSpec defined in request message. The ECSpec describes an event cycle and one or more reports that are to be generated from it. The Event Cycle Registry/Scheduling module process the event scheduling in based on the ECBoundarySpec within ECSpec, which specifies how the beginning and end of event cycles are to be determined.

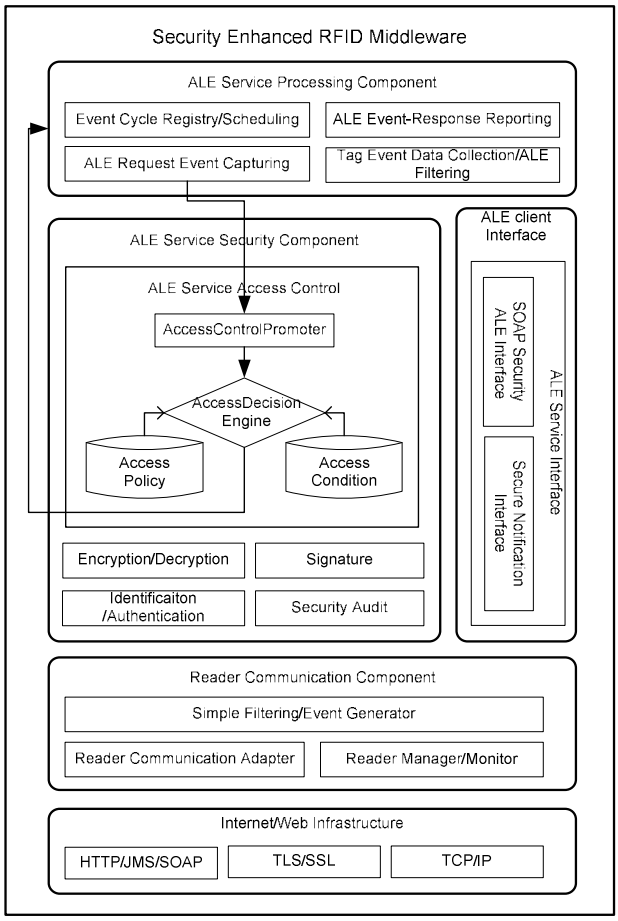

Fig. 2 Security Enhanced RFID Middleware Architecture

Our proposed ALE Service Security Component provides authentication, data secrecy, security audit and access control functions. For these, it is basically required digital signature, encryption functions, and X.509 certificate for authentication or private key. In addition to these, access control policy is needed to give differentiated ALE service. And ALE Client Interface is ALE Service Interface standard supports SOAP ALE Security and Secure Notification Interface. We will descript functions in aspect of technique in more detail security as like the following sub-sections.

B. Identification and Authentication

The X.509 certificate may be used as security token for identification and authentication method. On the remote site which could be Information Server, Enterprise Server, or another Middleware, the security token is used to separate service requester from non-permitted clients. Moreover, the security token may be used for identity of subject to determine service authority.

C. Transported Data Protection

The data to be transported between ALE provider and his clients is ALE service request/response message and notification report message. The former is exchanged in based on SOAP(Simple Object Access Protocol) between both entities and includes the context to reserve or release ALE service

resource, get ALE event information, generate event trigger, and so on. The later is output message of ALE layer, which is data about an event cycle communicated from ALE provider to a client. This is communicated to the Application Business Logic Layer later. Both types of messages are provided with data integrity, confidentiality and freshness for trust e-business service.

Until the most recent, the most common approach of legacy middleware system is to build Transport Layer Security Protocol such as SSL/TLS. However, that approaches are a little heavy-handed, because they often secure the entire wire protocol rather than just the SOAP message sent over the protocol. Further, for many message-based integration projects, several intermediary steps are necessary before messages arrive at their target end point, and transport-level security leaves the messages unsecured at each intermediary checkpoint. This is the same problem in case of the report message.

In the result, to get a finer level of control and avoid the intermediary security issues, data security is processed at the message level rather than at the transport level. What this means is securing the message itself, independently of the transport. It have also advantage although the intermediary or end point has the correct security infrastructure and is trusted, the message will remain secure and unreadable and can be forwarded to the next end point. To secure the ALE service message and report message, we recommend the message level security mechanism, rather than transported security protocol.

D. Service Access Control

The ALE service middleware must support access control mechanism to limit which clients may interact with the readers under the control of an ALE service provider, and to restrict what data those clients may obtain. It is assumed that each client using the ALE interface has an associated client identity which the ALE service provider authenticates. That is, we assume that in previous, clients hold credentials with which they prove their identities to the ALE service and authenticate themselves to ALE middleware. We present the access control policy such as following Fig. 3.

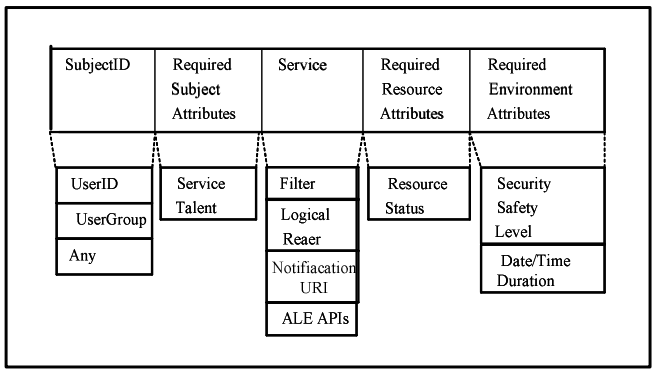

Fig. 3 Service Access Control Policy

Access Control Policy consists of the five elements, which are Subject ID, Required Subject Attributes, Service, Required Resource Attributes, and Required Environment Attributes. The Subject ID may be ALE Client ID or Group ID and so on. And Required Subject Attributes is the requirement condition in which subject can be provided with service. This value is filled with service talent or role of Subject. And for service and required resource attribute, each of them means available service types and needed condition. The service assets for access are filter, logical reader, notification URI, ALE APIs. The Filter attribute limits stored tag data control and limitation of logical reader and ALE APIs prevent to corrupt ALE Service/Configuration. And Notification URI control attribute limit unauthorized client to receive the notification report message. In the last, required environment attribute include security safety level and effective duration. The security safety level may be checked optionally in order to provide service only when the condition of network or system is secure and trust over the threshold value.

V. Conclusion

We have proposed how to provide strengthened security and trust in ALE service middleware. We considered the security attacks and countermeasures. Our enhanced middleware architecture includes the security service component and interface as well as fundamental ALE service engine component. Our proposed ALE Service Security Component provides authentication, data secrecy, security audit and access control functions. We build the secure middleware system, which makes only permitted client systems communicate through secure data protection mechanism. Moreover, our system supports the access control function that enables the each requester to be provided only authorized service. These features give strengthened security and trust to the e-business process in RFID network environment.

We suggest that we can and should make an analysis of the threats and weaknesses in character of RFID network in detail and consider intrusion detection mechanism. The balanced security and performance of RFID middleware system might eliminate critical barriers to economic growth by ensuring trust e-business service and eliminate sources of risk and distrust.

References

[1] Whiting R., "RFID growth poses a data management challenge," Computing, 26 Feb. 2004, pp.29-30. Publisher: VNU Business Publications, UK.
[2] Benetton Explains RFID Privacy Flap, RFID Journal, June 23, 2003, http://www.rfidjournal.com/article/articleview/471/1/1/
[3] EPCglobal Web site. www.epcglobalinc.org, 2005.
[4] J. Collins. Marks & Spencer expands RFID retail trial. RFID Journal, 10 February 2004.
[5] Tesco Pushes on with Full-scale RFID Rollout. http://www.computing.co.uk/news/1160636, January, 2005.
[6] S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T., June 2003.United States Food and Drug Administration. Combatting counterfeit drugs: A report of the Food and Drug Administration, 18 February 2004. Available at http://www.fda.gov/oc/initiatives/counterfeit/report02 04.html.
[7] Filtering and Collection Threat Analysis. Technical report, EPCGlobal Inc, July 2004.
[8] The Application Level Events (ALE) Specification, Version 1.0, EPCGlobal Inc, September 2004.
[9] EPCglobal Object Name Service (ONS) 1.0. Technical report, EPCGlobal Inc, April 2004.