공학석사 학위논문

RFID 기반 엔터프라이즈 애플리케이션 프레임워크를 위한 보안 모델

2007년 2월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

이 현 동

공학석사 학위논문

RFID 기반 엔터프라이즈 애플리케이션 프레임워크를 위한 보안 모델

지도교수 정 목 동

이 論文을 工學碩士 學位論文으로 提出함

2007년 2월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

이 현 동

이 논문을 이현동의 공학석사 학위논문으로 인준함

2007년 2월 23일

주 심 공학박사 권 기 룡 (인)

위 원 공학박사 송 하 주 (인)

위 원 공학박사 정 목 동 (인)

목 차

그 림 목 차

표 목 차

RFID 기반 엔터프라이즈 애플리케이션 프레임워크를 위한 보안 모델

이 현 동

부 경 대 학 교 대 학 원 컴 퓨 터 공 학 과

요약

다양한 기업 환경 내에서 보안서비스가 적용된 안전한 RFID 애플리케이션 개발 필요성이 대두 되고 있다. 안전한 RFID 애플리케이션 개발은 ALE, EPCIS 등의 표준화가 진행 중이어서 스펙의 변화에 적절하게 대처하기 어렵고, 레거시 시스템과의 통합 문제, 그리고 초기 개발 비용이 많이 든다는 문제점, 보안 전문지식의 부재로 인해서 중소규모의 기업이 개발하기에 어려운 상황이다.

이를 해결하기 위해서 본 논문에서는 안전한 RFID 애플리케이션을 쉽고, 효율적으로 개발할 수 있도록 도움을 주는 엔터프라이즈 애플리케이션 프레임워크(EAF)내에서 보안모델을 제안하고, 이를 이용하여 안전한 창고관리

시스템(WMS)을 구현하여 제안한 보안 모델의 효율성을 검증한다.

EAF의 보안모델은 기밀성, 무결성, 인증, 부인봉쇄, 권한부여(접근제어) 서비스를 제공한다. 높은 보안 강도 보다는 빠른 처리 속도가 요구 될 경우에는 ID/패스워드 기반 인증 서비스를 제공하고, 처리 속도 보다는 높은 보안 강도가 중요시 되는 경우 PKI 기반 인증 서비스를 제공한다. 권한부여는 RBAC 기반으로 한다.

EAF는 분산 컴포넌트 환경을 통합하고 인터넷 상에서 분산 컴퓨팅이 가능한 웹 서비스를 활용한다. 또한 보안전문 지식이 없는 개발자들도 쉽게 안전한 RFID 애플리케이션을 만들 수 있도록 보안 모델과 프레임워크 개념을 도입한다. 이를 바탕으로 RFID 애플리케이션을 재사용 및 확장 가능한 모듈을 통해서 적은 비용으로 쉽고, 효율적으로 개발할 수 있다. 제조업 및 유통업에서 많은 활용 가치가 있으며, 특히 물류 자동화 부분에 많은 역할을 할 것으로 기대한다.

Security Model for RFID-based Enterprise Application Framework

Hyun Dong Lee

Department of Computer Engineering, Graduate School,

Pukyong National University

Abstract

In a diverse enterprise environment, the need for developing secure RFID applications is increasing. Since ALE, EPCIS and other standardization is still on progress, it is difficult to adapt the change of specification. And the integration with the legacy system is also a problem. Moreover, due to expensive initial development investment and lack of security knowledge, it is difficult for medium level enterprise to develop secure RFID application.

To solve this problem, this thesis proposes security model in the

EAF(Enterprise Application Framework) that can help developing secure RFID application efficiently and easily, and implements secure WMS(Warehouse Management System) to verify the efficiency of the proposed security model.

Security model of EAF provides services including confidentiality, integrity, authentication, non-repudiation, and authorization(access control).

If an application needs high speed processing rather than security solidity, it provides ID/Password-based authentication service. On the contrary, if an application needs high security solidity, it provides PKI-based authentication service. Authorization management is based on RBAC.

EAF is taking advantage of Web Services that integrates remote component environment and is able to do remote computing over the Internet. Also, for those developers who have not much knowledge about high security requirement, this thesis imports security model and framework concept for them to build RFID application easily. Based on this, anyone can build RFID application efficiently with lower cost using general, reusable and extensible module. It is expected to do a lot of contribution to manufacturing industry and distribution industry enormously.

1. 서론

최근 사물에 태그를 부착하여 무선으로 사물의 정보를 확인하고(Identification) 주변 상황정보를 감지하는(Sensing), 전파식별(RFID, Radio Frequency Identification) 기술이 등장하여 미래 IT 시장을 선도할 기술 중 하나로 주목받고 있다.

사용자가 네트워크나 컴퓨터를 의식하지 않고, 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보통신 환경(유비쿼터스)의 핵심 기술인 RFID는 판독기, RF태그, 안테나를 통하여 사람, 상품 등을 비 접촉으로 인식해 태그에 기록된 정보를 판독하거나 기록하는 무선주파수 인식기술을 말한다. 바코드 시스템에 이은 RFID 기술은 정보의 획득과 보관이 완전 자동화될 수 있으며, 사람의 개입 없이 한 번에 수백 개의 태그를 인식함으로써 작업 시간의 대폭적인 단축이 가능하다[1,2,5]. 표1은 RFID와 바코드를 비교하고 있다.

표 1. RFID와 바코드 비교

RFID	바코드
읽기와 쓰기가 가능	읽기만 가능
도난방지기능의 오작동률이 낮음	도난방지기능의 오작동률이 높음
동시의 여러 개 아이템이 처리 가능	아이템을 하나씩 처리
온도, 물리적, 화학적 요소에 유연함	환경적인 제약이 있음
저장능력이 2의 128승 이상 가능 (바코드에 비해 6,000배 저장 능력)	저장 능력이 2의 7승
동일 상품에 개별 ID	동일 상품에 동일 ID

RFID 태그(tag)는 상품에 부착되어 ID와 Data를 가지고 다니는 역할을 수행한다. 능동형(건전지 내장)과 수동형(판독기로부터 동력을 얻음) 태그로 구분하며, 내장 칩의 저장용량, 인식거리 등에 따라서 가격이 전차만별이다.

RFID 리더(reader)는 태그의 정보를 해독하여 네트워크를 통해 호스트 컴퓨터와 교신하고, 호스트 컴퓨터의 지시를 받아 태그에 정보를 기록한다.

RFID 미들웨어(middleware)는 리더에서 계속적으로 발생하는 코드 데이터를 수집, 제어, 관리 하는 기능을 하며, 모든 구성 요소와 연결되어 계층적으로 조직화되고 분산된 구조의 미들웨어 네트워크를 구성하여 서로 통신한다. 또한 다양한 형태의 리더 인터페이스, 다양한 코드 및 망 연동, 여러 응용 플랫폼에 대해서도 운용성을 보장한다.

RFID 기술의 도입과 응용은 물류, 유통, 국방, 조달, 건설, 교통, 제조, 서비스 등 전 산업분야에 걸쳐 큰 영향을 미칠 것으로 예상되고 있으며, 기존 산업구조와 인간의 생활방식까지도 변화시킬 수 있는 아주 중요한 산업 응용 기술로서 각광을 받고 있다.

웹 서비스는 조직 간 애플리케이션 통합, 비즈니스 파트너 간 통합을 위한 솔루션으로 플랫폼에 독립적이며, 상호운용성 있는 서비스를 제공한다[21]. 또한 컴포넌트 기반이므로 특정산업에 무관하게 어떤 비즈니스에도 적용되며, 레거시 시스템뿐만 아니라 다른 웹 서비스와 통신이 가능해서 물류 IT 내의 이질적인 환경에 적합하다[12].

1.1 연구의 필요성

RFID 시스템의 장점으로 인해서 다양한 기업 환경에서 보안서비스가 적용된 RFID 애플리케이션을 쉽고 효율적으로 개발하려는 필요성이 대두되고 있다. 하지만 안전한 RFID 애플리케이션 개발은 ALE(application level event), EPCIS(electronic product code information service)등의 표준화가 진행 중이어서 스펙의 변화에 적절하게 대처하기 어렵고, 레거시 시스템과의 통합 문제, 그리고 초기 개발 비용이 많이 든다는 문제점, 보안 전문지식의 부재로 인해서 중소규모의 기업이 개발하기에 어려운 상황이다.

그리고 RFID 애플리케이션은 개인의 프라이버시와 상업적으로 가치 있는 대량의 실시간 정보의 이동으로 인해서 기밀성, 무결성, 인증, 권한부여, 부인봉쇄의 보안 서비스 적용이 필요하다고 많은 사람들이 인식을 하고 있지만, 현재는 RFID 태그와 리더 간의 보안에 초점이 맞춰진 상황이며, RFID 애플리케이션에서의 보안은 많은 연구가 이루어지고 있지 않다.

1.2 연구의 목적

본 연구는 분산 컴포넌트 환경을 통합하고 인터넷 상에서 분산 컴퓨팅이 가능한 웹 서비스를 활용한다[8]. 또한 보안전문 지식이 없는 개발자들도 쉽게 안전한 RFID 애플리케이션을 만들 수 있도록 보안 모델과 프레임워크 개념을 도입한다. 이를 바탕으로 보안서비스가 적용된 안전한 RFID 애플리케이션을 재사용 및 확장 가능한 모듈을 통해서 적은 비용으로 쉽고, 효율

적으로 개발할 수 있다. 제조업 및 유통업에서 많은 활용 가치가 있으며, 특히 물류 자동화 부분에 많은 역할을 할 것으로 기대한다[20].

1.3 연구의 방법 및 범위

본 논문에서는 EPCglobal 네트워크 및 RFID 애플리케이션의 보안 요구사항을 분석하고, 프레임워크 개념과 기존의 여러 보안 응용 기술인 인증, 권한 부여, 데이터 암복화를 활용하여 안전한 RFID 애플리케이션을 쉽고, 효율적으로 개발할 수 있도록 도움을 주는 엔터프라이즈 애플리케이션 프레임워크(EAF)와 EAF 내에서 보안모델을 제안한다. 그리고 제안한 EAF의 보안모델을 이용하여 안전한 창고관리 시스템(WMS)을 구현하고 제안한 보안모델의 효율성을 검증한다.

EAF의 보안모델은 기밀성, 무결성, 인증, 부인봉쇄, 권한부여(접근제어) 서비스를 제공한다. 높은 보안 강도 보다는 빠른 처리 속도가 요구 될 경우에는 ID/패스워드 기반 인증 서비스를 제공하고, 처리 속도 보다는 높은 보안 강도가 중요시 되는 경우 PKI 기반 인증 서비스를 제공한다. 권한부여는 RBAC 기반으로 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 다루고, 3장에서는 엔터프라이즈 애플리케이션 프레임워크(EAF), 4장에서 EAF의 보안 모델, 5장에서는 보안 서비스가 적용된 안전한 RFID 애플리케이션 구현 사례를 소개한다. 마지막으로 6장에서는 결론 및 향후 연구 방향을 논한다.

2. 관련 연구

2.1 RFID(radio frequency identification) 기술

RFID 시스템은 사물에 부착된 태그(IC칩)로부터 무선 주파수를 이용하여 사물의 정보 및 주변 환경정보를 비접촉식으로 수집하여 저장, 가공, 추적함으로써 측위, 원격처리, 관리 및 정보교환을 가능하게 하는 기술이다[23].

자동인식기술(automatic identification)의 하나로서 바코드 및 스마트카드와 유사한 기능을 수행한다. 그러나 원거리에서 인식이 가능하고, 충돌방지 기능이 있어 동시에 여러 개를 인식할 수 있다는 기술적 장점 때문에 바코드, 스마트카드 등에 비해 활용범위가 넓다. 스마트카드에 비해서는 가격이 저렴하고. 바코드에 비해서는 월등히 많은 정보를 축적할 수 있다[29].

그림 1은 RFID 시스템 구성도를 나타낸다.

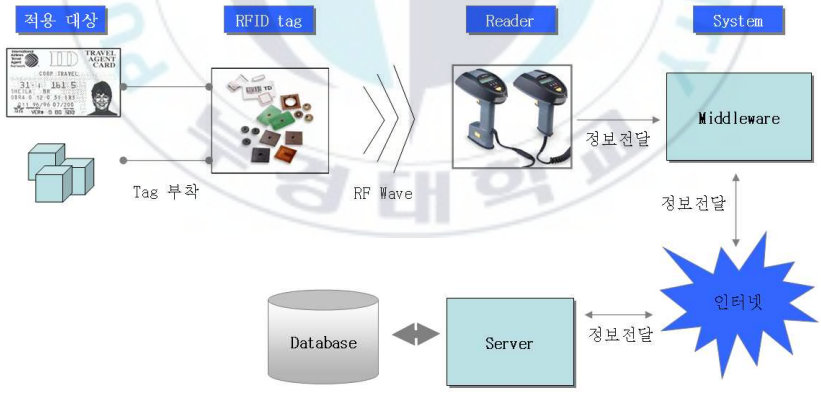

그림 1. RFID 시스템 구성도

안테나에서 지속적으로 전파를 발산하고, ID와 데이터가 저장된 태그가 전파의 범위에 들어가게 되면 태그가 데이터를 안테나로 전송하고, 판독기가 태그의 정보를 판독하여 네트워크로 연결된 DB정보를 교신한다.

2.2 EPCglobal 네트워크 구조

RFID와 관련된 국제 표준화는 EPCglobal을 중심으로 활발히 이루어지고 있다. EPCglobal에서는 제안한 EPCglobal 네트워크는 태그 처리를 위한 모든 과정을 정의하고 있다.

리더는 정해진 주파수를 이용하여 태그를 인식하고, 이것을 미들웨어로 전달한다. 미들웨어로 전달된 데이터를 필터링하여 Capturing Application에 전달하게 되고, 전달된 데이터는 비즈니스 처리를 위한 가공이 이루어진 후 EPCIS에 전달되거나 Accessing Application에서 처리된다.

EPCGlobal 네트워크의 컴포넌트와 구조를 살펴보면, RFID 리더는 RFID 태그가 리더가 읽을 수 있는 범위에 존재할 때 태그를 읽는다. 그리고 리더는 읽힌 태그를 미들웨어에 전송한다. ALE 엔진이라 불리는 미들웨어는 ALE 인터페이스에 의해 정해진 룰에 따라 태그를 필터링 한다[3,7,8]. 필터링 된 데이터는 ECPIS Capturing Application으로 전송되는데, EPCIS Capturing Application은 전송된 태그 데이터를 저장하고 비즈니스 처리와 관련된 데이터를 가공한다. 가공된 데이터는 EPCIS Accessing Application이나 EPCIS Repository에 전송한다. EPCIS Repository는 EPC 코드와 관련된 현재 및 과거 데이터를 다른 외부 시스템과 공유하는 역할을 한다.

EPCIS Accessing Application은 창고관리 시스템(WMS), 출석관리 시스템(AMS)과 같은 기업 비즈니스 프로세스를 수행한다. 그림 2는 EPCglobal 네트워크의 구조를 나타낸다[6].

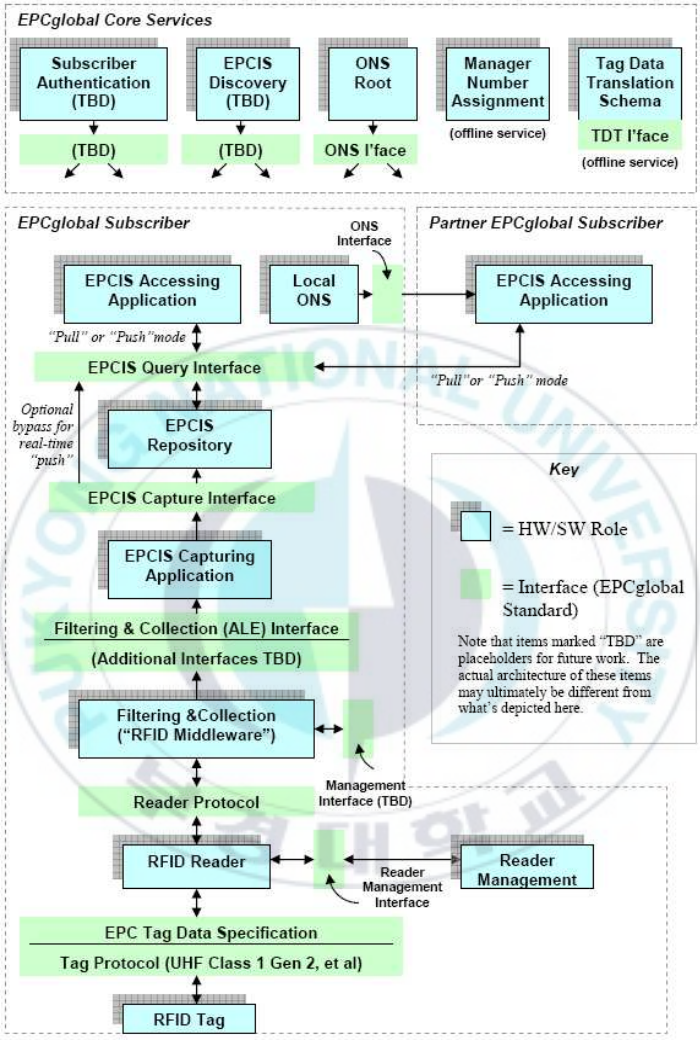

그림 2. EPCglobal 네트워크 구조(출처:[6])

2.3 인증(authentication)

인증 서비스는 자신의 신분과 행위를 증명하는 행위를 의미한다. 이미 실생활에서는 우리가 주민등록증이나 운전면허증, 사원증 등을 통해서 자신의 신분을 밝힐 수가 있다. 사이버 공간에서 어떠한 종류의 서비스를 구현하든 가장 중요하고 기본적으로 도입해야 하는 보안 개념이라고 할 수가 있다. 인증은 주로 위장(masquerade), 스푸핑(spoofing) 과 같은 위협에 대해 효과적으로 대응할 수가 있다. 인증 방법에는 사용자명과 패스워드, 공개키 기반 구조(public key infrastructure: PKI), SPKI/SDSI(simple public key infrastructure / simple distributed security infrastructure) 등이 있다.

2.3.1 사용자 명과 패스워드(ID/password)

컴퓨터 또는 네트워크에 로그인하는 사용자 개인을 식별하는데 사용되는 문자 집합(ID)과 식별된 사용자의 신원(identity)을 확인하는데 사용되는 비밀 문자 집합(password)으로 인증이 이루어지는 시스템이다.

사용자 명과 팩스워드 인증은 구현하기 쉽고, 인증 속도가 빠르다는 장점이 있는 반면에 평문 패스워드를 사용하면 통신상에 노출될 위험이 존재하고, 인간의 기억에 의존하므로 망각하기 쉬우며, 패스워드 추측 공격(password guessing attack)에 약점이 존재하는 등의 다양한 종류의 보안 취약점이 존재한다.

2.3.2 공개키 기반 구조(PKI)

PKI는 개인키 관리 및 인증하기 위한 인증기관의 운영을 통하여 대칭키 암호방식의 운영상 한계극복을 가능하게 하고, 키의 분실이나 분배상의 어려움에 대한 해소 방안을 제시하였으며, 웹상의 비즈니스나 안전한 거래를 보증하기 위한 대안으로 등장하였다[4,9,25].

PKI는 인증기관(CA)에서 공개키와 개인키로 포함하는 인증서(certificate)를 발급받아 네트워크상에서 안전하게 비밀통신을 가능하게 하는 기반 구조이며, 공신력 있는 제3의 인증기관에 의한 거래 주체의 인증, 거래 정보의 무결성과 기밀성, 거래의 부인방지의 기능을 담당하는 공개키 기반 인프라이다. X.509는 국제전기통신연합(ITU-T)의 표준 디렉터리 서비스(directory service)인 X.500의 일부로써 사용자에게 공개키 기반구조의 인증 서비스를 제공하기 위한 프레임워크를 정의하고 있다. 표 2는 PKI 구성 요소를 나타낸다.

표 2. 공개키 기반 구조 구성 요소

구분	내용
인증기관	- 객체로서 인증서 등록, 발급, 조회 시 인증서의 정당성에 대한 관리를 총괄
디렉토리	- 인증서 및 인증서 취소 목록을 저장하고 사용자에게 서비스 하는 역할(LDAP를 이용) - 인증서는 서명 검증의 응용을 위해 디렉토리에 저장됨
등록대행기관	- 인증서 등록 및 사용자 신원 확인을 대행하는 기관
사용자	- 인증서를 신청하고 인증서를 사용하는 주체

X.509 방식의 핵심은 각 사용자와 관련 있는 공개키 인증서이다. 이들 사

용자인증서는 몇몇 신뢰기관(Certificate Authority)에 의해 생성되고 디렉토리에 위치시킨다. 그림 3은 X.509 인증서 구조를 나타낸다.

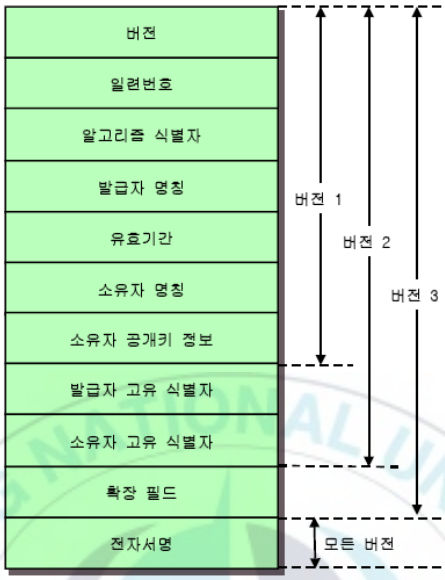

그림 3. PKI(X.509) 인증서 구조

- 버전(version): 인증서 형식의 버전을 나타내며, 버전1 부터 버전3 까지 세 가지 종류로 구분된다.
- 일련번호(serial number): 발급자인 인증기관(CA) 내에서 인증서 별로 식별할 수 있도록 고유하게 부여하는 정수 값이다.
- 알고리즘 식별자(algorithm identifier): 인증서에 서명하기 위해서 사용되는 알고리즘의 식별자이다.
- 발급자 명칭(issuer name): 인증서를 생성하고 서명한 인증기관의 명칭이다.

- 유효 기간(period of validity): 인증서의 유효함을 보장하는 두 개의 날짜(즉, 시작일과 종료일)로 구성된다.
- 소유자 명칭(subject name): 인증서가 가리키는 사용자에 대한 명칭이며, 대응하는 개인키를 가지고 있는 소유자에 대한 실체를 알려준다.
- 소유자 공개키 정보(subject public key info): 소유자의 공개키에 대한 값과 키가 사용되는 알고리즘의 식별자를 나타낸다.
- 발급자 고유 식별자(issuer unique identifier): 발급자 명칭이 다른 개체에 재사용될 경우에 인증기관을 고유하게 식별하는데 사용되는 필드이다. 버전2 에서 추가된 내용이다.
- 소유자 고유 식별자(subject unique identifier): 소유자 명칭이 다른 개체에 재사용될 경우에 소유자를 고유하게 식별하는데 사용되는 필드이다. 버전2 에서 추가된 내용이다.
- 확장 필드(extensions): 인증서를 관리하고 안전하게 이용할 수 있도록 지원해주는 추가적인 정보이다. 버전3 에서 추가된 내용이다.
- 전자서명(signature): 인증서의 모든 필드에 대해서 인증기관의 개인키를 사용하여 암호화한 해쉬 코드를 나타낸다.

2.3.3 SPKI/SDSI

웹 환경에서 인증서비스를 제공해주는 기존의 X.509 공개키 기반구조는 권한이나 이름을 하나의 인증서에 나타내야 하므로 둘 중에 하나라도 변경 상황이 있을 경우 인증서를 새로 갱신해야하는 불완전성을 지니고 있다.

뿐만 아니라 루트에서 시작하는 계층적 구조의 전역이름을 이용하고 있어 사용자가 소속되어 있는 회사나 부서의 이동에 따른 전역이름의 변경이 자주 일어 날 수 있고, 루트가 어느 국가에 소속되어야하는가 등에 따른 국제적이 이해관계에 얽힐 수 있는 복잡성을 내재하고 있다. 이의 단점을 보완하고자 PKIX 작업그룹은 권한관리 기반구조(PMI: privilege management infrastructure)를 두어 속성-인증서를 정의해 사용자에 권한을 부여하고 있지만 여전히 전역적인 이름을 사용하고 있고, 구성 요소 또한 복잡하다.

이러한 문제점을 해결하기 위해 공개키 기반 구조를 단순화 시키고 유연하게 보안한 SPKI/SDSD가 연구되고 있다[13,17,22].

SPKI의 특징은 이름-인증서와 권한-인증서를 각각 구별하여 명세할 수 있는 융통성을 제공한다. 또한 주체의 구별을 이름이 아닌 공개키로 함으로써 수시로 바뀔 수 있는 전역이름을 주체의 구별대상으로 하는 X.509 v3인증서를 이용하는데 따른 문제점을 해결할 수 있다.

SDSI의 특징은 “지역이름공간”라는 개념을 도입해서 공개키의 소유자는 각각 그 공개키에 기반을 둔 지역이름공간을 생성할 수 있다. 즉, 누구든지 자신이 보유한 대상주체들의 공개키들을 자신의 공개키에 기반을 둔 지역이름으로 바인딩하는 이름-인증서를 발행 할 수 있다는 것이다. 또한 공개키 대신 이들 지역이름들을 이용하여 새로운 이름-인증서를 발행할 수도 있다.

이렇게 각각 연구되기 시작한 SPKI와 SDSI는 1998년에 SPKI/SDSI라는 명칭으로 통합되었다[22].

SPKI/SDSI는 두 개의 인증서인 이름-인증서와 권한-인증서를 명세하도록 허용하고, 전역이름 대신 계층적인 지역이름 공간을 이용하는 등 아주 단순하고 융통성 있는 정책모델을 제공하고 있다.

표 3은 PKI와 SPKI/SDSI를 비교한다.

표 3. PKI와 SPKI/SDSI 비교

	PKI	SPKI/SDSI
이름 공간	전역 이름	지역 이름
인증서 유형	이름-인증서	이름-인증서, 권한-인증서
이름-키 연결	단일 값 함수(한 개의 이름에 한 개의 키 연결)	다중 값 함수 (한 개의 이름에 한 개 이상의 키 연결)
인증기관 특징	전역적인 계층구조	평등적인 구조
신뢰 모델	계층적인 신뢰모델	검증자로부터 의뢰자에 이르는 권한-연결 검사
서명	발행자의 개인키로 서명	발행자의 개인키로 서명
인증서 폐기	인증서 폐기리스트 이용	짧은 생명주기의 인증서 옹호, 온라인 체크

2.4 접근제어(access control)

접근제어 서비스는 모든 사용자에게 유효성을 인식시켜 특정 사용자를 식별함으로써 오직 허용된 사용자만이 데이터에 접근할 할 수 있도록 하여 비인가자에 의한 불법적인 자원접근 및 파괴를 예방하고, 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용성 제공하는 보안 서비스이다[25].

2.4.1 RBAC(role-based access control)

Ravo S. Sandhu[19]에 의해 제안된 RBAC는 사용자의 역할에 기반을

둔 접근 통제 방법으로 조직 내의 사용자 허가 할당에 있어서 복잡성과 비용, 잠재적인 실수를 줄이기 위한 강력한 기법을 제공한다. 또한 조직 수준에서 보안 관리를 증진시키기 위해서 사용자 식별자 수준이 아닌 추상화 수준으로 제공하므로 권한 관리를 매우 단순화 시켜주고, 특정한 보안 정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다.

혼재된 자원의 환경 요소가 동적으로 변화하는 유비쿼터스 환경에서 다양한 자원의 보안 설정을 개별적으로 설정하고 관리하는 것은 복잡하고 많은 부담이 따른다. 따라서 RBAC 모델을 적용하면 권한 관리를 단순화 시켜주고 보안정책의 설정과 변경이 쉽고 변경된 보안 정책이 잘 반영 될 수 있는 유동적인 보안 관리 시스템을 제공 할 수 있다.

그림 4는 RBAC의 개념적인 모델인 RBAC1, RBAC2, RBAC3를 보여준다.

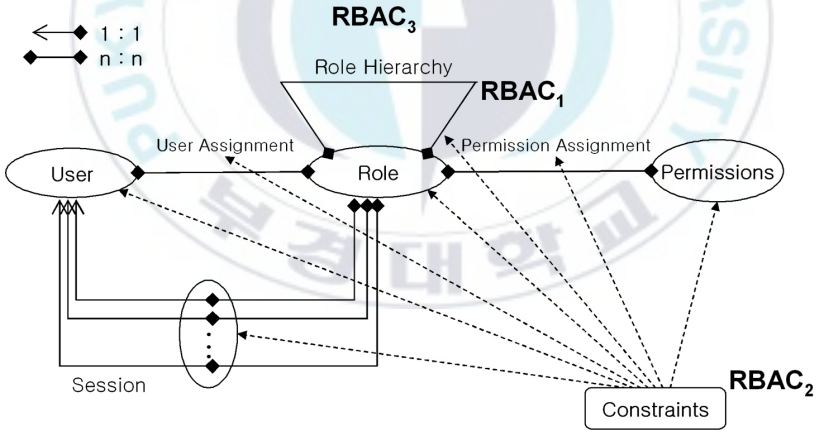

그림 4. RBAC 모델(출처:[19])

2.4.2 GRBAC(generalized role-based access control)

지금까지 보안은 정적인 것으로 인식되어서 접근 제어도 컨텍스트(context)에 따라 변경되지 않았으며 동적인 환경의 변화를 반영할 수 없었다. 이를 해결하기 위해서 상황 인식 컴퓨팅을 보안 서비스에 도입하여야 한다. 상황 인식 컴퓨팅을 위한 보안 서비스는 자연스럽고, 사용자의 개입을 최소로 하는 non-intrusive 형태의 것이어야 한다. 따라서 더 이상 보안을 위한 사용자 세션이 시간에 무관하게 동일한 인증 기법과 접근 기법을 사용한다고 가정 할 수 없다. 예를 들면, 상황 인식 인증 기법은 풍부한 정보로 이루어져 있는 디지털 홈(digital home, aware home)과 같은 환경에서는 굉장히 복잡하다. 인증 정책은 여러 요소에 의해서 제약을 받는데 사용자 종류와 사용자의 현재 위치 등의 정보에 따라서 많이 달라진다.

기존의 RBAC는 역할에만 기반을 두고 상황 정보를 사용하지 못했기 때문에 다음과 같은 한계를 가지게 되었다[18,19,24].

- 개별 사용자들이 멤버로서 요구되는 역할에 근거하여 이루어짐.
- 접근 권한은 역할이름에 따라 그룹화 됨.
- 역할이 사용자 업무 책임과 권한에 따라 부과됨으로써 자원의 이용에 제약

이를 해결하기 위하여 GRBAC[15,16] 개념을 고려하게 되었는데, 이는 기존의 역할기반 접근 제어가 시간에 따른 접근제어 등과 같이 상황에 근거한 접근제어를 수행할 수 없었던 문제점을 해결하고 있다. GRBAC는 상황에 근거한 접근제어를 수행하기 위하여, 접근제어 결정에 사용자 역할(subject

role), 객체 역할(object role), 환경 역할(environment role)을 추가하여 기존 RBAC 모델을 확장하였다.

GRBAC 모델은 기존 RBAC 모델보다 상황 인식 애플리케이션의 접근 정책을 나타내는데 강력하고 융통성 있는 방법을 제공하고 있다[14]. 또한 디지털 홈 등을 실제 사용하게 될 사용자들은 컴퓨터나 보안 관련 초보자일 가능성이 크므로 여기에 사용될 애플리케이션에서 보안 정책을 쉽게 정의하고 사용할 수 있는 기능은 매우 중요하다. 이런 면에서 다양한 역할에 바탕을 둔 GRBAC 모델을 이용한 보안 서비스는 유비쿼터스 컴퓨팅 환경의 보안 서비스를 구현하는데 유용한 방법이 될 수 있다.

3. 엔터프라이즈 애플리케이션 프레임워크

이 장에서는 안전한 RFID 애플리케이션을 개발을 위한 엔터프라이즈 애플리케이션 프레임워크(EAF)를 살펴본다.

3.1 엔터프라이즈 애플리케이션 프레임워크 구조

엔터프라이즈 애플리케이션 프레임워크는 본 연구실에서 개발한 것으로서 개발자가 EPCglobal 네트워크를 기반으로 RFID 애플리케이션을 효율적으로 개발할 수 있도록 지원하는 프레임워크이며, 외부 시스템과 통신을 담당하는 데이터 계층, 시스템 및 네트워크 보안을 담당하는 보안 계층, RFID 관련 이벤트에 대한 요청 및 처리를 담당하는 비즈니스 이벤트 계층으로 구성되어 있다[11,26,27,28]. 그림 5는 엔터프라이즈 애플리케이션 프레임워크 계층 구조를 나타낸다.

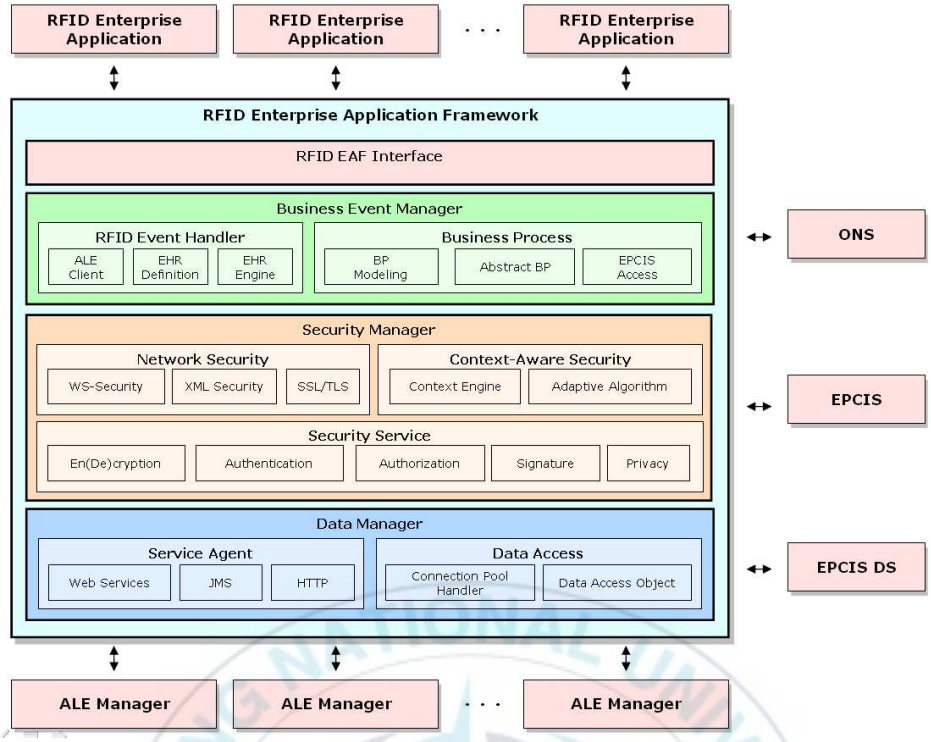

그림 5. 엔터프라이즈 애플리케이션 프레임워크(EAF)의 계층 구조

3.1.1 데이터 계층(data layer)

데이터 계층은 외부 시스템과의 통신을 담당하는 컴포넌트이다. 데이터베이스나 웹 서비스 등을 통해 외부시스템에 접근하는 기능을 제공한다. 이 계층에는 데이터베이스에 접근하여 데이터의 입출력 처리를 담당하는 데이터 엑세스(data access) 컴포넌트가 포함되며, 서비스 에이전트(service agent) 컴포넌트가 외부 시스템과의 상호작용을 전담하게 함으로써 외부 시스템의 변화에도 최대한 유연성을 갖도록 설계되었다.

EPCglobal 네트워크에서의 EPCIS, EPCIS DS, ONS 또는 다른 외부 시스템 및 데이터베이스에 접근하는 기능을 제공한다. 웹 서비스, JMS, HTTP 등의 다양한 통신 프로토콜을 지원한다.

3.1.2 보안 계층(security layer)

보안 계층은 분산 네트워크 환경을 위한 인증과 인터넷과 같은 개방형 네트워크를 통해 전송되는 데이터의 보호를 위해 전자서명, 데이터 암·복호화, 키 관리, 보안정보 교환, 권한부여 기술 등의 보안 서비스를 제공한다.

엔터프라이즈 애플리케이션 보안 모델은 위장과 같은 적극적인 공격에 대한 대처 방안으로 인증 서비스를 제공하고, 비인가자에 의한 불법적인 자원 접근 및 파괴를 예방하고자 권한 부여를 통해서 외부시스템(EPCIS)에 접근하고자 한다. 그리고 데이터 교환할 때 도청 및 메시지 위변조 공격을 대처하기 위해서 데이터 암 복호화 과정으로 기밀성, 무결성을 제공한다.

현재는 ID/패스워드 기반의 인증과 PKI 기반 인증, RBAC기반의 접근제어, 데이터 암·복호화 기능을 제공한다. 향후에는 최적화된 경량 PKI(SPKI/SDSI)기반 인증과 GRBAC 기반의 권현 부여를 통한 적응적 보안 서비스를 제공 할 예정이다.

3.1.3 비즈니스 이벤트 계층(business event layer)

비즈니스 이벤트 계층은 애플리케이션을 위한 RFID 관련 이벤트의 요청 및 처리 기능을 제공한다.

RFID 이벤트 핸들러(event handler) 컴포넌트에서는 사용자가 원하는 EPC 이벤트를 정의하고, RFID 미들웨어(ALE Manager)로부터 받은 EPC 이벤트를 비즈니스 프로세스에서 처리하기 쉽도록 변환한다. 비즈니스 프로세스(business process) 컴포넌트에서는 사용자가 원하는 비즈니스 프로세스를 정의하고, 실행하여 사용자가 원하는 결과를 얻을 수 있다. 또한 RFID 관련된 다양한 비즈니스에 대한 추상 비즈니스 프로세스를 제공해줌으로써 개발자가 좀 더 편리하게 RFID 애플리케이션을 개발 할 수 있게 한다.

그림 6은 추상 비즈니스 프로세스 구성도를 나타낸다.

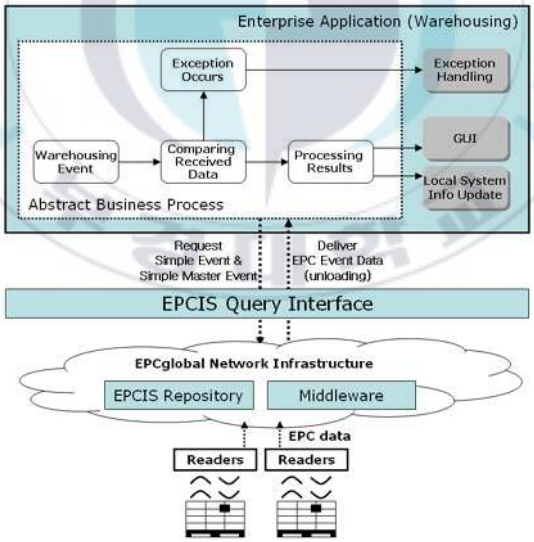

그림 6. 추상 비즈니스 프로세스 구성도

추상 비즈니스 프로세스는 SCM, WMS 등을 분석하여 많은 애플리케이션에서 공통적으로 사용되는 요소를 추출하여 추상화하였다. 이러한 추상 비즈니스 프로세스는 EPCglobal 네트워크를 통해 RFID 관련 데이터를 EPCIS에 요청하고 사용자가 필요로 하는 데이터를 반환하는 등의 공통적으로 사용되는 클래스를 정형화하여 재사용이 가능하도록 하고, 이를 사용하는 개발자는 이 API를 상속받아 기존의 비즈니스 프로세스 개발(BPM 등) 기술을 기반으로 각각의 도메인에 맞는 자신의 클래스를 구현하면 된다. 추상 비즈니스 프로세스는 다양한 산업에서 적용될 수 있는데 특히 물류 관련 산업에서 효율적으로 적용될 것이다.

3.2 엔터프라이즈 애플리케이션 프레임워크의 특징

EAF의 특징은 RFID 애플리케이션을 프레임워크의 특징인 일반적이고, 재사용, 확장 가능한 모듈을 통해서 적은 비용으로 쉽고, 빠르고, 효율적으로 개발할 수 있도록 하였다.

웹 서비스를 사용하여 상호운영성이 높은 서비스를 제공하며, 컴포넌트 기반이므로 특정산업에 무관하게 어떤 비즈니스에도 적용가능하며, 레거시 시스템뿐만 아니라 다른 웹 서비스와 통신이 가능해서 물류 IT 내의 이질적인 환경에 적합하도록 하였다. 뿐만 아니라 보안 서비스와 추상화된 비즈니스 프로세스를 제공하도록 설계하였다. RFID 애플리케이션을 개발하기 어려운 제조업 및 유통업의 중소기업에서 EAF를 사용하여 애플리케이션을 개발 할 경우 적은 비용으로 쉽게 개발 할 수 있다.

4. 엔터프라이즈 애플리케이션 프레임워크의 보안 모델

4.1 EAF의 보안 요구사항 분석

RFID 애플리케이션의 보안 요구 사항과 EAF에서 외부 시스템(EPCIS)과의 통신에서 각 트랜잭션별 데이터 흐름을 살펴본다.

4.1.1 RFID 애플리케이션의 보안 요구 사항

RFID 애플리케이션의 보안 요구 사항은 사물에 대한 태그 정보와 태그 관련 상세 정보를 가지고 있는 EPCglobal 네트워크 구성요소에 대해 보안 기술을 적용해야 한다. 또한 RFID 애플리케이션이 사용하는 네트워크상에서의 보안(SSL/TLS)도 고려하여야 한다. 이러한 보안 기술을 적용하지 않으면 공격자는 송수신 중인 데이터를 변형 할 수 있을 뿐만 아니라, EPCIS에 저장되어 있는 태그 관련 상세 데이터를 변경할 수 있다.

<보안 요구사항 1: 기밀성 및 무결성>

- RFID 애플리케이션과 외부시스템(EPCIS) 사이의 통신에서 주고받는 데이터 교환할 때 도청 및 메시지 위변조 공격을 대처하기 위해서 데이터 암 복호화 과정으로 기밀성, 무결성이 요구된다.

<보안 요구사항 2: 인증>

w 위장, 중간자 공격 또는 서비스 거부 공격과 같은 적극적인 공격에 대한 대처 방안으로 인증 서비스가 요구된다.

<보안 요구사항 3: 접근제어(권한부여)>

w 비인가자에 의한 불법적인 자원 접근 및 파괴 취약점을 해결하고, 프라이버시 침해 취약점 해결하기 위하여 권한 부여를 통해서 외부시스템(EPCIS)과의 접근제어 서비스가 요구된다.

RFID 애플리케이션에 보안 요구사항 및 보안 기술과 보안 기술이 적용되어야 할 RFID 환경 요소는 표 4와 같다.

표 4. RFID 애플리케이션 보안 요구사항 및 보안 기술

보안 요구사항	보안 기술	*RFID* 환경 요소
기밀성	En(De)cryption	ALE, EPCIS
무결성	WS-Security	RFID Application, ALE, EPCIS
인증	ID/패스워드 & PKI	RFID Application, EPCIS
접근제어	RBAC & GRBAC	RFID Application

RFID 애플리케이션, 외부시스템(ALE, EPCIS)과의 통신에서는 데이터 암복화를 통해서 기밀성, 무결성이 요구되고, 외부시스템과의 인증 서비스를 위해서는 ID/패스워드, PKI 기반 인증이 요구된다. RFID 애플리케이션의 권한부여를 하기 위해서 RBAC, GRABC 기반의 접근제어 서비스가 요구된다.

4.1.2 EAF의 데이터 흐름

EAF를 사용하여 개발한 엔터프라이즈 애플리케이션은 EPCIS Repository에 Query Operation을 사용하여 EPCIS Repository에 데이터 처리를 요청하고, XML 형태의 응답 메시지를 받는다.

엔터프라이즈 애플리케이션과 ALE Manager간에는 ECSpec 형태로 Reader에서 읽힌 정보를 요청하고, ECReport 형태의 응답 메시지를 받는다.

그림 7은 EAF의 데이터 흐름도를 나타내고, 데이터 흐름의 각 단계별 설명은 다음과 같다.

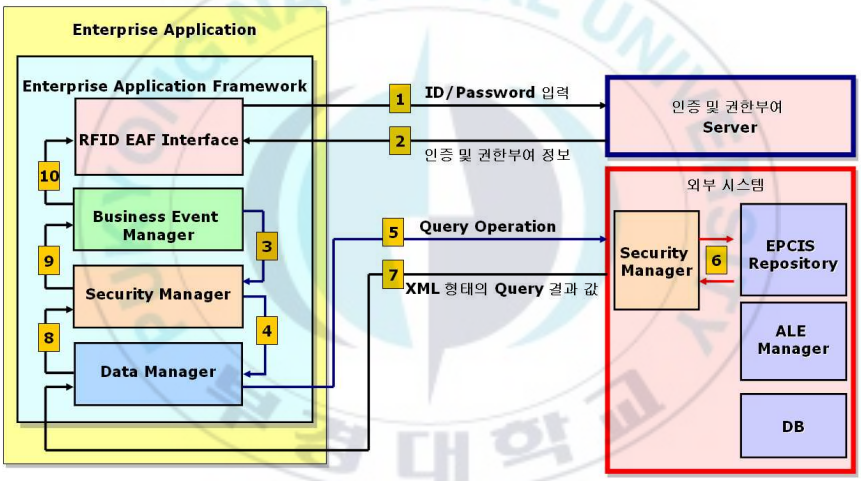

그림 7. EAF의 데이터 흐름도

① 사용자는 EAF 인터페이스(Interface)를 통해서 ID와 패스워드를 입력하고 인증 및 권한부여(접근제어) 서버로 전달한다.

② 인증 및 권한 부여 서버에서 ID와 패스워드의 유효성 검사를 하고, ID

에 따라 미리 정의되어 있는 외부시스템 접근 권한 정보를 EAF에게 응답메시지 형태로 전달한다.

③ 비즈니스 이벤트 매니저(Business Event Manager)에서 접근 권한이 있는 EPCIS Repository에 정보를 요청하기 위한 Query Operation을 생성한다.

④ Query Operation을 보안 매니저(Security Manager)에서 보안(데이터 암호화) 서비스를 적용한다.

⑤ 데이터 매니저(Data Manager)에서 EPCIS Repository와 통신을 담당하고 Query Operation을 전송한다.

⑥ EPCIS Repository 내부에 있는 보안 매니저를 사용하여 보안(데이터 복호화) 서비스를 적용하고, 응답메시지를 보안 매니저를 사용하여 보안(데이터 암호화) 서비스를 적용한다.

⑦ EPCIS Repository에서 보안서비스 적용된 XML 형태의 Query 결과를 전송한다.

⑧ 받은 XML 형태의 질의 결과를 보안 매니저에서 보안(데이터 복호화) 서비스를 적용한다.

⑨ XML 형태의 질의 결과를 비즈니스 이벤트 매니저에서 정의되어 있는 Business Rule에 따라 처리한다.

⑩ 비즈니스 이벤트 매니저에서 처리된 결과를 EAF 인터페이스(Interface)를 사용하여 사용자에게 전달한다.

4.2 EAF의 인증 및 권한부여 프로토콜

EAF의 인증은 보안 강도 보다는 빠른 처리 속도가 요구 될 경우에는 ID/패스워드 기반인증 서비스를 제공하고, 처리 속도 보다는 보안 강도가 중요시 되는 경우 PKI 기반 인증 서비스를 제공한다. 접근제어는 RBAC 기반으로 한다. ID/패스워드 기반 인증 및 권한 부여 프로토콜은 표 5와 같다[10].

표 5. ID/패스워드 기반 인증 및 권한 부여 프로토콜

Protocol	
(1) U → AS : IDu || PWu (2) AS → U : IDu || PWu || Ekas[M] || Lkas (3) U → AS : IDu || Ekas[M] || Lkas (4) AS → U : IDu || R	
Notations	
IDu	User Identification
PWu	User password
Kas	Secret Key of the AS System
Ekas[M]	Encrypted Message M Using Kas
Lkas	The span of life of the Message M
R	Authority Information to use Service

(1) 사용자 인증 요청(U → AS)

w IDu || PWu

w 사용자가 특정 서비스를 이용하고자 할 때는 먼저 인증 서비스로부터 인증을 받아야 한다. 사용자는 자신의 ID와 패스워드를 인증 서비스에 전송한다.

(2) 사용자 인증 처리(AS → U)

w IDu || PWu || Ekas[M] || Lkas

w 인증 서비스는 사용자의 인증이 완료되면, 권한 부여를 위한 비밀 메시지와 메시지 수명에 관한 정보를 사용자에게 전송한다. 권한 부여를 위한 비밀 메시지와 수명 정보는 사용자 인증 후 사용자가 서비스에 대한 권한 정보를 요청할 때 인증된 사용자인지를 한 번 더 확인하기 위한 방법이다.

(3) 서비스 권한 요청(U → AS)

w IDu || Ekas[M] || Lkas

w 서비스 권한 요청이 필요할 때, 사용자는 인증 서비스로부터 받은 비밀 메시지와 수명에 대한 정보를 전송한다.

(4) 서비스 권한 정보 전송(AS → U)

w IDu || R

w 비밀 메시지와 수명에 대한 정보를 받은 인증 서비스는 자신의 비밀키로 비밀 메시지를 복호화하여 자신이 전송한 데이터가 맞는지를 판단하고, 수명이 다한 메시지가 아닌지를 판단한 후에 두 가지 과정 모두 참이면 사용자에게 권한에 대한 정보를 전송한다.

PKI를 이용하여 RFID Application(App)에서 CA로부터 인증서를 발급받고, EPCIS와 비밀통신을 하는 과정은 그림 8과 같다.

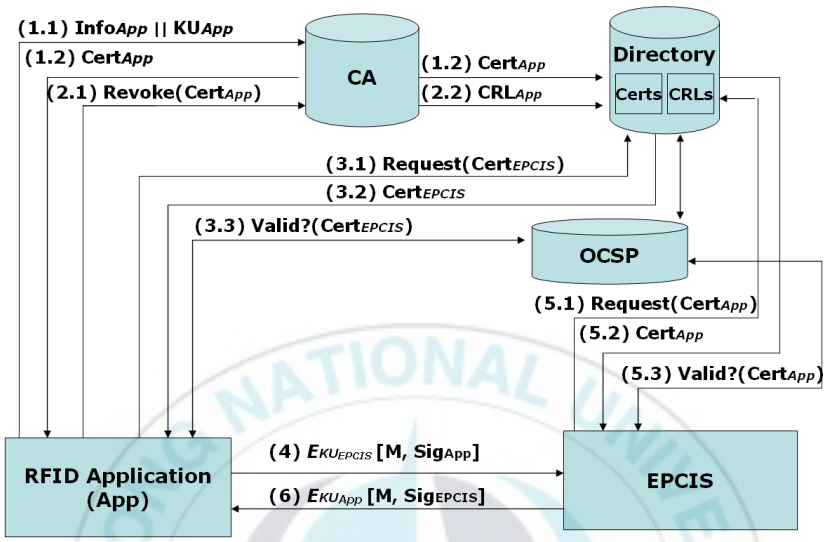

그림 8. PKI 기반 인증 과정(RFID Application 관점)

(1.1) 인증서 발급 요청 단계(App → CA)

w Info*App* || KU*App*

w App의 사용자 정보와 App의 공개키를 CA에 전송하고, 인증서 발급을 요청한다.

w App의 사용자 정보 예

CN = "RFID Application" // common name

OU = "CS&AI LAB" // organizational unit

O = "LIT" // organization

L = "Busan" //location

C = "KR" //country

(1.2) 인증서 발급 단계(CA → App, CA → Directory Server)

w Cert*App*

w CA에서 인증서가 생성되면 App에게 인증서를 발급해주고, EPCIS등 다른 PKI Client에서 App 인증서 요청을 대비하여 Directory Server에 인증서를 저장한다.

(2.1) 인증서 폐기 요청 단계(App → CA)

w Revoke(Cert*App*)

w App에서 비밀키 손상 및 유출이 될 경우 인증서 폐기 요청을 CA로 하면 CA에서는 인증서를 폐기 하고 CRL을 생성한다.

w 인증서 폐기 목록 예

일련번호: 03 15 ea cf

해지날짜: 2007년 01월 01일 월요일 오후 12:34:00

CRL 원인 코드: 키 손상(1)

(2.2) 인증서 폐기 단계(CA → Directory Server)

w CRL*App*

w CA에서 발급된 CRL을 Directory Server에 저장한다.

(3.1) EPCIS 인증서 요청 단계(App → Directory Server)

w Request(Cert$_{EPCIS}$)

w App가 EPCIS와 비밀통신을 하기위해서는, EPCIS의 공개키가 필요하다. EPCIS의 인증서를 Directory Service에 요청한다.

(3.2) EPCIS 인증서 획득 단계(Directory Server → App)

w Cert$_{EPCIS}$

w CA로부터 받은 EPCIS의 인증서를 획득한 후, 인증서에서 EPCIS의 공개키를 추출한다.

(3.3) 인증서 검증 요청 및 검증 결과 획득 단계(App ⇄ OCSP Server)

w Valid?(Cert$_{EPCIS}$)

w App에서 가지고 있는 EPCIS의 인증서가 유효한지 OCSP Server에서 CRL을 확인한 후 인증서 검증을 수행한다.

w 인증서 검증 결과를 App로 전달한다.

w OCSP Server은 Directory Server로부터 CRL을 다운로드 받아서 보유하고 있다.

(4) App에서 EPCIS에 메시지 전송 단계(App → EPCIS)

w $\boldsymbol{E}$KU$_{EPCIS}$ [M, Sig$_{App}$]

w App는 EPCIS의 인증서에서 추출한 공개키로, 메시지(EPCIS Query)와 App의 전자서명을 함께 암호화해서 EPCIS에 전달한다. EPCIS는 자신의 개인키를 사용하여 메시지를 복호화한다.

w App의 전자서명을 첨부함으로써, 부인봉쇄를 보장한다.

w 데이터 암복화를 통해서, 기밀성, 무결성을 보장한다.

(5.1) App 인증서 요청 단계(EPCIS → CA)

w Request(Cert$_{App}$)

w App의 인증서를 Directory Server에 요청한다.

(5.2) App 인증서 획득 단계(CA → EPCIS)

w Cert$_{App}$

w 요청한 App의 인증서를 Directory Server에서 획득한다.

w App의 인증서에서 공개키를 추출해서, App로부터 전달받은 암호화된 메시지에 포함된 App의 전자서명을 검증하는 역할을 하고, EPCIS에서 App에 전송할 데이터를 암호화하는데 사용된다.

(5.3) 인증서 검증 요청 및 검증 결과 획득 단계(EPCIS⇄ OCSP Server)

w Valid?(Cert$_{App}$)

w EPCIS에서 가지고 있는 App의 인증서가 유효한지 OCSP Server에서 CRL을 확인한 후 인증서 검증을 수행한다.

w 인증서 검증 결과를 EPCIS로 전달한다.

w OCSP Server은 Directory Server로부터 CRL을 다운로드 받아서 보유하고 있다.

(6) EPCIS에서 App에 메시지 전송 단계(EPCIS → App)

w $\boldsymbol{E}$KU$_{App}$ [M, Sig$_{EPCIS}$]

w EPCIS는 App의 인증서에서 추출한 공개키로, 메시지(EPCIS query 결과)와 EPCIS의 전자서명을 함께 암호화해서 App에 전달한다. App는 자신의 개인키를 사용하여 메시지를 복호화한다.

w EPCIS 전자서명을 첨부함으로써, 부인봉쇄를 보장한다.

w 데이터 암복화를 통해서, 기밀성, 무결성을 보장한다.

PKI를 이용하여 EPCIS에서 CA로부터 인증서를 발급받고, RFID Application(App)과 비밀통신을 하는 과정은 그림 9와 같다. 그림 8은 RFID Application 관점에서 인증서를 발급받아서, 비밀통신을 하는 것을 나타내고, 그림 9는 EPCIS 관점에서 인증서를 발급받아서, 비밀통신을 과정을 나타낸다. 설명은 그림 8과 동일하다.

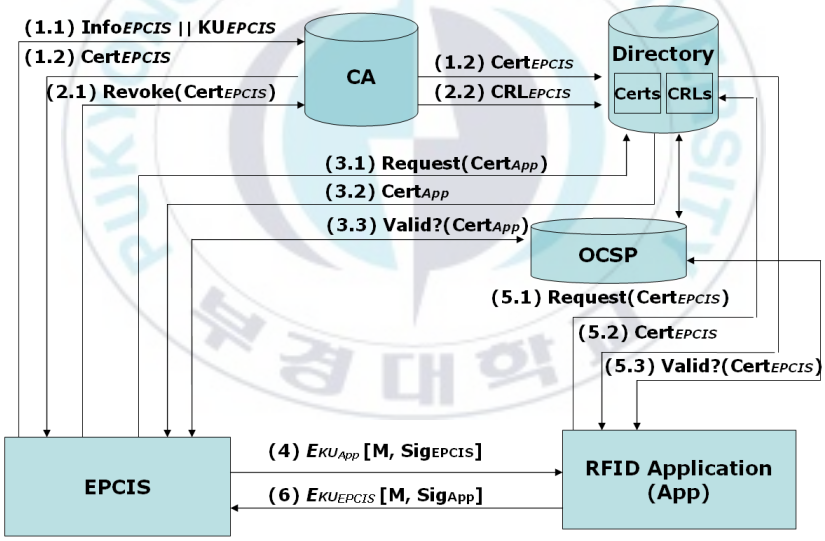

그림 9. PKI 기반 인증 과정(EPCIS 관점)

4.3 EAF의 보안 모델

4.3.1 사용자 인증 및 권한 부여

그림 10은 ID/패스워드 기반 인증 및 권한부여를 위한 유저케이스 다이어그램을 나타낸다.

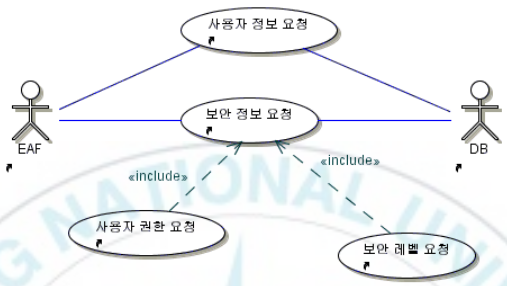

그림 10. ID/패스워드 기반 인증 및
권한부여 유저케이스 다이어그램

EAF 애플리케이션을 사용하는 사용자는 EAF에 있는 Member클래스와 MemberManager클래스를 이용하여 사용자 인증을 하게 된다.

EAF 애플리케이션은 사용자가 입력한 ID/패스워드를 이용하여 사용자 정보와 보안 정보(권한 및 보안 레벨)를 가지고 있는 데이터베이스에 접근하여 사용자가 EAF 애플리케이션을 어느 정도 사용 할 수 있는지를 판단한다. ID/패스워드 기반의 인증과 RBAC 기반의 권한 부여를 위하여 데이터베이스를 사용하며, 그 테이블 구성은 그림 11과 같다.

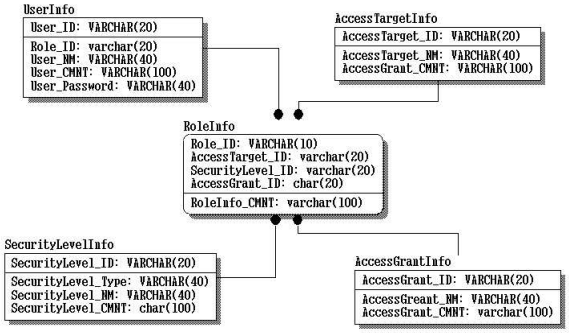

그림 11. ID/패스워드 기반 인증 및
권한부여를 위한 DB 테이블

그림 12는 PKI 기반 인증을 위한 유저케이스 다이어그램을 나타낸다.

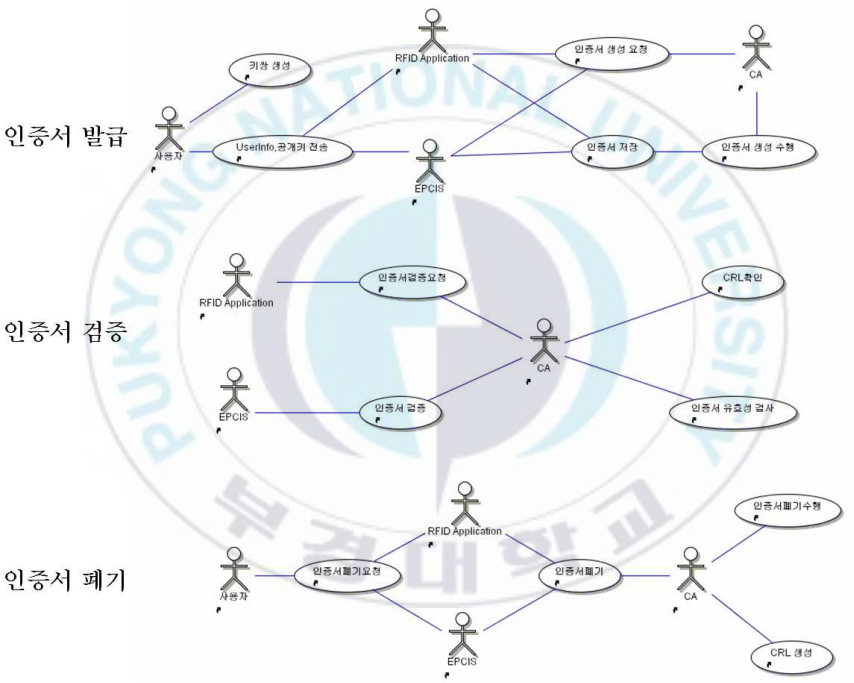

그림 12. PKI 기반 인증 유저케이스 다이어그램

4.3.2 데이터 보안

EAF와 개체간의 데이터를 안전하게 송수신하기 위해서는 데이터에 대한 암·복호화가 이루어져야 한다.

암호화 방법에는 대칭키, 비대칭키 방법이 있다. 대칭키는 비밀키를 상호간에 유지하기 어렵다는 단점이 있고 비대칭키는 시간이 많이 걸린다는 단점이 있다. 이로 인해 암호화는 대칭키, 대칭키를 만들거나 교환하기 위한 문서에는 비대칭키를 이용하여 많이 사용하고 있다. 그러므로 EAF에도 효율적인 암호화를 위해 Diffie Hellman을 바탕으로 하는 키 일치를 기본 암호화 방법으로 사용한다. 또한 개발자가 다른 암호화 방법을 사용하고자 하면 다른 암호화 방법을 적용할 수 있는 형태의 디자인을 제공한다.

그림 13은 데이터 보안을 위한 유저케이스 다이어그램을 나타낸다.

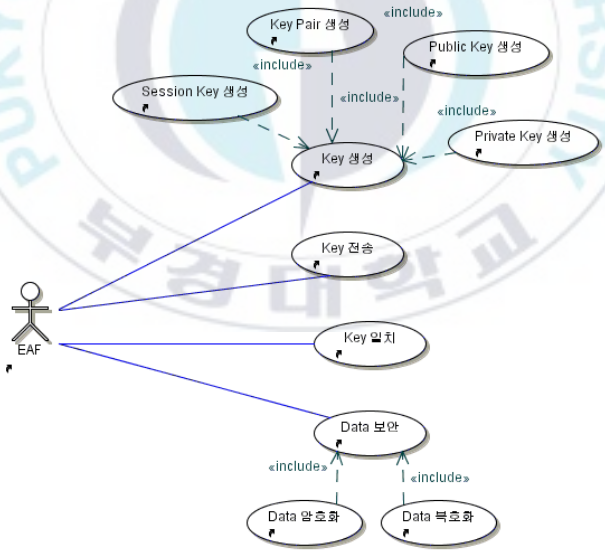

그림 13. 데이터 보안 유저케이스 다이어그램

EAF의 ID/패스워드 기반 인증 및 권한 부여 프로토콜은 7단계로 이루어져 있으며, 각 단계별 프로토콜의 전송 내용과 처리방법은 그림 14와 같이 진행된다.

사용자 인증 과정을 거친 후 RFID 애플리케이션과 외부시스템(EPCIS)사이의 키 일치를 통해서 데이터 암 복화를 통해서 안전한 데이터 송수신을 한다.

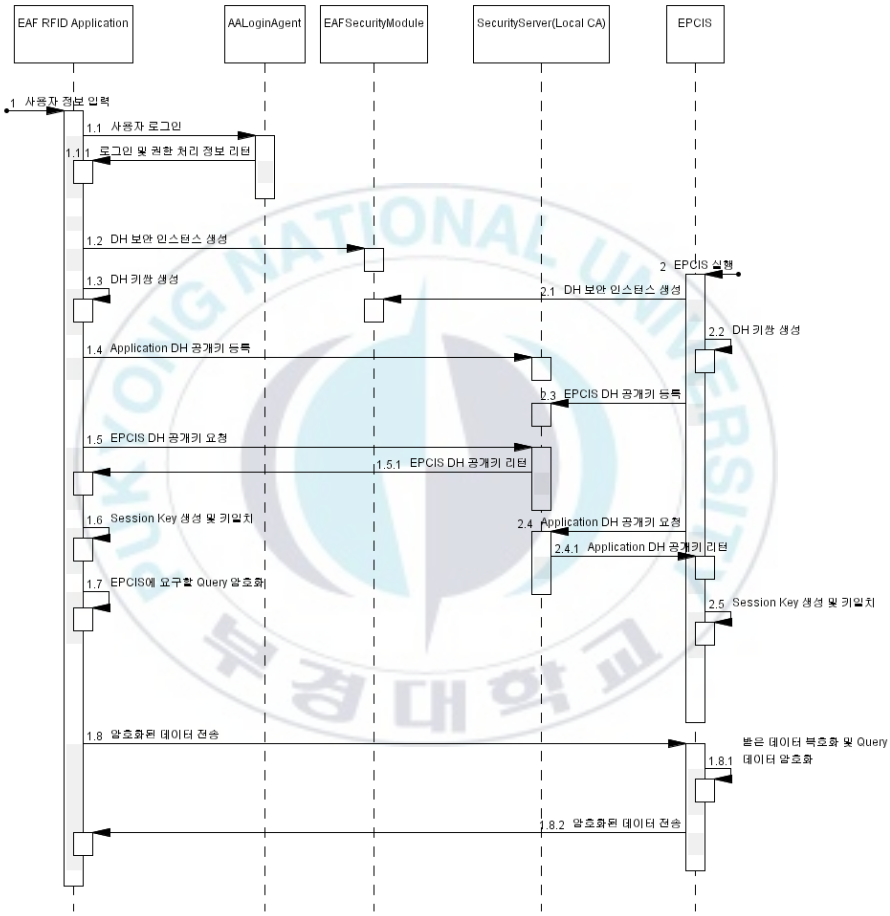

그림 14. EAF의 보안 모델의 시퀀스 다이어그램

① 사용자는 EAF를 이용하여 개발된 애플리케이션에 로그인을 한다. 로그인을 통해 애플리케이션은 사용자의 애플리케이션 권한을 설정 할 수 있다.

② 사용자는 EPCIS와 안전한 통신을 하기 위해서 Diffie Hellman 키 쌍을 생성한다.

③ 사용자는 생성한 공개키를 SecurityServer에 등록하고 통신하려는 EPCIS의 공개키를 받는다. Security Server는 지역 CA로 사용한다.

④ 사용자는 자신의 비밀키와 EPCIS의 공개키를 이용하여 세션키를 생성하고 이를 이용하여 암호화를 위한 TripleDES 비밀키를 생성한다.

⑤ 사용자는 EPCIS에 질의할 Query를 ④에서 생성한 비밀키를 이용하여 암호화 하고 EPCIS에 전송한다.

⑥ EPCIS는 전송된 데이터를 복호화 하고 Query에 대한 응답을 다시 암호화 하여 사용자에게 전송한다.

⑦ 사용자는 받은 데이터를 복호화하여 활용한다.

4.4 EAF 보안 모델 평가

EAF는 개발자들이 기존의 Java 보안 기술들을 사용하기 쉽도록 보안(security) API를 제공해 줌으로 보안서비스가 적용된 안전한 RFID 애플리케이션 개발 시간 및 유지보수 시간을 단축 할 수 있다.

EAF는 대칭키, 비대칭키 암 복호화 및 키 관리방식을 제공함으로써 데이터 기밀성, 무결성을 보장하고, 인증 서비스와 RBAC 기반의 접근제어(권한

부여)를 제공한다. 인증은 높은 보안 강도 보다는 빠른 처리 속도가 요구될 경우에는 ID/패스워드 기반인증 서비스를 제공하고, 처리 속도 보다는 높은 보안 강도가 중요시 되는 경우 PKI 기반 인증 서비스를 제공한다.

EAF가 제공하는 보안서비스는 표 6과 같다.

표 6. EAF의 보안 서비스

보안서비스	현재	향후
인증	ID/패스워드 기반 or PKI 기반	경량화 PKI (SPKI/SDSI)기반
접근제어(권한부여)	RBAC 기반	GRBAC 기반
기밀성, 무결성	비밀키, 공개키 기반 암 복호화	비밀키, 공개키 기반 암 복호화
부인봉쇄	전자서명	전자서명

EAF의 보안 모델은 다음의 보안 요구사항을 만족한다.

- w RFID 애플리케이션과 외부시스템(EPCIS) 사이의 통신에서 주고받는 데이터 교환할 때 도청 및 메시지 위변조 공격을 대처하기 위해서 JCA(Java Cryptography Architecture), JCE(Java Cryptography Extension)를 사용하여 데이터 암 복호화하며, 웹서비스 보안 서비스인 WS-Security를 사용하여 네트워크 보안에서 기밀성, 무결성을 제공한다.
- w 위장과 같은 적극적인 공격에 대한 대처 방안으로 ID/패스워드 인증 및 PKI 기반 인증 서비스를 제공하고 향후 경량 PKI(SPKI/SDSI) 인증 서비스를 제공한다.
- w 비인가자에 의한 불법적인 자원 접근 및 파괴를 예방하고자 RBAC를 사용하여 외부시스템(EPCIS)에 접근제어 서비스 제공하고, 향후 GRBAC를 사용한 접근제어 서비스를 제공한다.

5. RFID 애플리케이션 구현 사례

5.1 창고관리 시스템(WMS) 구성 및 구현 환경

RFID 기술 및 엔터프라이즈 애플리케이션 프레임워크를 이용하여 창고관리 및 물품의 현재 상황 및 입출고 내역을 좀 더 효율적으로 관리할 수 있는 안전한 시스템을 구현한다.

그림 15는 창고관리 시스템 구성 환경을 나타낸다.

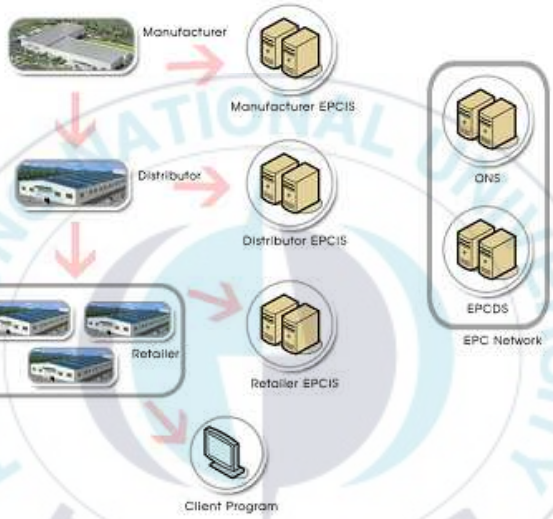

그림 15. 창고관리 시스템 구성 환경

• 공장(Manufacturer)에서 RFID를 활용하여 배송될 Containment를 구성하고, 이에 대한 정보를 제공한다.

• 도매상(Distributor)에서는 공장에서 출고된 제품이 어느 Retailer로 가는지를 결정해주며, 도매상이 Containment에 대한 정보를 알고 있지 않아도

EPCIS에 접근해서 Containment가 구성하고 있는 제품들의 정보를 제공한다.

• 소매상(Retailer)에서는 RFID를 이용하여 제품의 입출고 및 도난의 상태를 알 수 있고, 실시간으로 재고량 파악이 가능하다. 그림 5는 보안서비스가 적용된 창고관리 시스템을 나타낸다.

RFID 애플리케이션 개발 환경은 표 7과 같다.

표 7. RFID 애플리케이션 개발 환경

Platform/Tools/Spec	Version	Description
MS Windows OS	2003 Server	Platform
J2SDK 1.5	1.5	Java Development Kit
JWSDP	1.6	Web Service 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-96		EPC tag

5.2 창고관리 시스템 시나리오

그림 16은 보안 서비스가 적용된 창고관리 시스템(WMS)을 나타내고 있다.

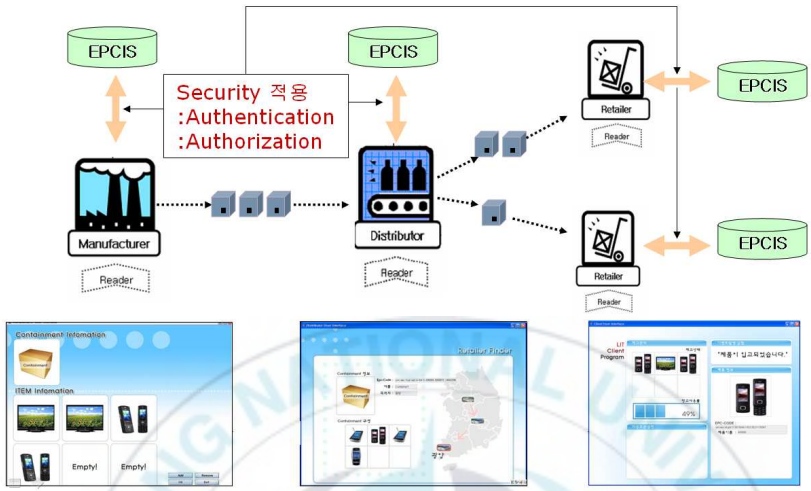

그림 16. 보안 서비스가 적용된 창고관리 시스템

가) RFID 애플리케이션과 EPCIS는 CA에게 사용자정보와 공개키를 전송하고, CA는 인증서를 생성하여 디렉토리 서버에 인증서를 보관하고, 인증서 요청자에게 발급한다.

나) 애플리케이션과 EPCIS는 서로 상대방의 인증서를 디렉토리 서버에 요청하고, 인증서를 받는다.

다) 받은 인증서를 OCSP서버를 통해 인증서 검증을 한 후, 이상이 없을 경우에 애플리케이션과 EPCIS은 비밀통신을 한다.

라) 비밀통신은 상대방의 공개키로 메시지와 자신의 전자서명을 암호화하여 전달함으로써, 기밀성, 무결성, 부인봉쇄 서비스를 제공한다.

6. 결론 및 향후 연구

본 논문에서는 보안서비스가 적용된 안전한 RFID 애플리케이션을 개발자들이 효율적으로 개발할 수 있도록 개발한 엔터프라이즈 애플리케이션 프레임워크(EAF)와 EAF의 보안 모델을 소개하고 이를 이용하여 구현한 보안서비스가 적용된 안전한 창고관리 시스템을 제시하였다.

EAF를 이용한 RFID 애플리케이션 개발은 생산성, 품질, 운영 및 유지보수 향상을 통하여 제조업, 유통분야와 등과 같은 다양한 분야에 활용될 수 있다. 그리고 EAF의 보안모델을 제공함으로써 보안전문 지식이 없는 개발자들도 기존의 Java 보안 기술들을 사용하기 쉽도록 보안(security) API를 제공해 줌으로 보안서비스가 적용된 안전한 RFID 애플리케이션 개발 시간 및 유지보수 시간을 단축 할 수 있다.

RFID 애플리케이션과 외부시스템(EPCIS) 사이의 통신에서 주고받는 데이터 교환할 때 도청 및 메시지 위변조 공격을 대처하기 위해서 JCA(Java Cryptography Architecture), JCE(Java Cryptography Extension)를 사용하여 데이터 암 복호화하며, 웹서비스 보안 서비스인 WS-Security를 사용하여 네트워크 보안에서 기밀성, 무결성을 제공하며, 위장과 같은 적극적인 공격에 대한 대처 방안으로 ID/패스워드 인증과 PKI 기반 인증 서비스를 제공한다. 그리고 비인가자에 의한 불법적인 자원 접근 및 파괴를 예방하고자 RBAC를 사용하여 외부시스템(EPCIS)에 접근제어 서비스 제공한다.

하지만 사용자 인증에서 ID/패스워드 기반 인증 방식은 처리 속도는 빠르지만 보안 강도가 약하다는 단점이 있고, PKI는 현재 많이 사용하고 있는

인증 방법이지만, 처리 속도가 느리고 인증서 유형에 의한 불안정성, 이름공간에 의한 복잡성의 단점이 있다. 향후 연구 방향은 엔터프라이즈 애플리케이션 프레임워크의 보안모델을 기존 PKI보다 빠른 경량 PKI 인증(SPKI/SDSI) 서비스로 확장하고 context-aware 서비스를 도입하여 상황에 맞는 GRBAC 기반 접근제어 서비스를 중점적으로 연구할 예정이다.

참고문헌

[1] Auto-ID Center, "EPC Information Service," White Paper, 2004.

[2] Auto-ID Labs, http://www.autoidlabs.org.

[3] Auto-ID Center, "EPC Information Service," White Paper, 2004.

[4] David Hook, Beginning Cryptography with Java, Wiley Publishing, INC. Wrox, 2005.

[5] EPCglobal, http://www.epcglobalinc.org.

[6] EPCglobal, "EPC Information Service(EPCIS), version1.0, Specification, 2006

[7] EPCglobal, "Object Name Service(ONS) 1.0," working Draft Version, April 15, 2004

[8] EPCglobal, "The Application Level Events (ALE) Specification, Version 1.0," Specification, February 8, 2005.

[9] EPCglobal, "EPCglobal Certificate Profile", Ratified Specification 1.0, March 8, 2006.

[10] Hyundong Lee and Kiyeal Lee, and Mokdong Chung "*Enterprise Application Framework for Constructing Secure RFID Application*," Proc. of The 2006 International Conference on Hybrid Information Technology, CHEJU ISLAND, KOREA, Nov. 2006.

[11] Hyundong Lee, Mokdong Chung, "*RFID-based ALE Application Framework using Hierarchical Architecture,*" Proc. of IASTED Int'l Conf. on Advances in Computer Science and Technology, Puerto

Vallarta, Jan. 2006, pp.26-31.

[12] Matjaz Juric, *PROFESSIONAL J2EE EAI,* WROX PRESS, 2002.

[13] Michelle S. Wangham, et al. *"Security Mechanisms for mobile Agent Platforms Based on SPKI/SDSI Chains of Trust,"* SELMAS 2003, LNCS 2940, 2004, pp. 207-224

[14] M.J.Covington, et al., *"A Context-Aware Security Architecture for Emerging Applications,"* In Proc. of the 18th Annual Computer Security Applications Conferences (ACSAC'02), 2002., pp. 249-258.

[15] M.J.Convington, et al., *"Generalized Role-Based Access Control for Securing Future Applications,"* In Proc of 23rd National Information Systems Security Conference(NISSC), Baltimore, Oct.2000, pp.115-125.

[16] M.J. Moyer and M.Ahamad, *"Generalized Role-Based Access Control,"* In proc of IEEE Int'l Conf. on Distributed Computing Systems(ICDSC2001), Mesa, April 2001, pp.391-398.

[17] Moon-Sang Kwak, Young-Sik Hong, *"Design and Implementation of Message Security Protocol suing SPKI/SDSI,"* KCC, Vol. 33, No. 1, 2006, pp.322-324.

[18] NIST, http://csrc.nist.gov/rbac.

[19] 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.

[20] Verisign, http://www.verisign.com.

[21] W3C, http://www.w3.org.

[22] Yong-lok Lee, et al., *"SPKI/SDSI HTTP Secure Server to support Role-based Access Control & Confidential Communication,"* KISS, Vol.12, No. 6, 2002, pp.29-46.

[23] 김유정, "RFID 시범사업 현황 및 추진방향", TTA저널 제 95호, pp. 55~63, 2004.

[24] 남승좌, 박석, *"유비쿼터스 컴퓨팅 환경의 역할기반 접근제어에서 발생하는 상황충돌,"* 정보보호학회논문지, 15권 2호, 2005, pp.37-52.

[25] 여호영, 박근용, *Digital Network security,* 운정미디어, 2006

[26] 이현동, 권중규, 안규희, 정목동, *"RFID기반 엔터프라이즈 애플리케이션 프레임워크를 이용한 ebXML 애플리케이션 설계 및 구현,"* 한국지능정보시스템학회 춘계학술대회, 2005, pp.159-165.

[27] 이현동, 안규희, 권중규, 정목동, *"RFID 애플리케이션 개발을 위한 Context-Aware ALE 애플리케이션 프레임워크,"* 한국정보처리학회 춘계학술대회, 제13권 제1호, 2006, pp.1121-1124.

[28] 이현동, 이기열, 정목동, *"안전한 RFID 애플리케이션 개발을 위한 엔터프라이즈 애플리케이션 프레임워크,"* 한국정보처리학회 추계학술대회, 제13권 제2호, 2006, pp.1657-1660.

[29] 한국과학기술정보연구원, RFID 기술, 한국과학기술정보연구원, 2003.