모바일 RFID 서비스를 위한 QoS 및 보안 모델

정회원 김 말 희*, 이 용 준**

Mobile RFID Service QoS, Security Model

Marie Kim*, Yong Jun Lee* ***Reguler Members***

요 약

본 논문은 Diameter 프로토콜을 이용하여 모바일 RFID 서비스를 위한 구성 노드 간 보안 연관을 설정하여 노드 간 통신에 대한 보안을 제공하며, 모바일 RFID 서비스 사용자의 QoS 기반 권한 검증을 제공함으로써, 차별적인 서비스를 제공할 수 있도록 한다.

본 논문은 현재 우리나라에서 표준으로 제정중인 모바일 RFID 기술을 전제로 하며 따라서 900MHz 주파수 대역을 사용하는 RFID tag와 휴대폰에 장착되는 RFID 리더를 사용하는 환경을 가정한다. 또한 Diameter AAA 서버를 이용하여 망 접속 인증을 수행하는 환경을 가정한다. Diameter AAA 서버를 이용하여 망 접속 인증을 수행한 후, 사용자의 QoS와 서버의 정책에 따른 권한 검증을 수행하며, 모바일 RFID 서비스 노드 간 보안 정책을 동적으로 생성하여 분배한다. 보안 연관이 수립 가능한 구간은 RFID 태그와 RFID 리더간, RFID 리더(휴대폰)와 모바일 RFID 서비스 에이전트(Diameter AAA Client)간, 휴대폰과 응용 서버(OIS : Object Information Service) 간, 휴대폰과 이력정보제공서버(OTS : Object Traceability Service) 간 휴대폰과 과금/결재 서버 간으로 한다.

Key Words : Mobile, RFID, Diameter, Authorization, Qos

ABSTRACT

This paper extends Diameter AAA Protocol to provide secure communication channels between Mobile RFID Service Components and distinct service based on user's QoS level authorization. This paper supposes 900MHz, which is the target RF for Mobile RFID Forum and supposes RFID phone, which equitted with RFID reader. By using extended Diameter AAA server, user is authenticated, authorized and provided dynamic security associations between Mobile RFID Service components. The types of security associations are as followings:between RFID tag and RFID reader, between RFID reader(phone) and MobileRFID Service Agent, between phone and OIS, between phone and OTS and between phone and Accounting/Financial server.

Ⅰ. 서 론

RFID 기술은 Radio Frequency를 이용한 자동 식별 기술이다. RFID tag안에 tag에 대한 식별자를 기록하고, RFID 리더를 통해서 해당 tag에 기록되어 있는 식별자를 판독하게 된다[1]. RFID 리더는 식별된 tag 정보를 RFID 미들웨어에 전송하고, RFID 미들웨어는 정보를 요청한 호스트(응용, 서버)에 제공하여, 정보를 이용할 수 있도록 한다. 서버는 획득된 정보를 이용하여, tag와 관련된 정보들을 제공할 수 있는 데이터베이스를 구축할 수도 있으며, 이미 구축되어 있는 데이터베이스에 대한 검색 서비스를 제공할 수도 있다. 이러한 RFID 기술은 기존에 유통망 관리에 주로 이용되어 왔다.

* 한국전자통신연구원 텔레매틱스USN연구단 (mariekim@etri.re.kr),
** 한국전자통신연구원 RFID/ USN 미들웨어연구팀장 (yjl@etri.re.kr)
논문번호 : KICS2005-10-431, 접수일자 : 2005년 10월 24일, 최종논문접수일자 : 2006년 4월 17일

Diameter 프로토콜은 망 접속에 대한 인증, 권한 검증, 과금 서비스를 제공하는 프로토콜이다[2]. 망 접속 형태에 따라서 고정IP 주소를 이용하는 경우에는 Diameter Network Access Server application[3]을 이용하여 인증, 권한 검증을 수행하며, Mobile IPv4를 이용하는 경우에는 Diameter Mobile IPv4 Application[4]을 Mobile IPv6를 이용하는 경우에는 personal draft인 Diameter Mobile IPv6 Application[5]을 이용할 수 있다.

Mobile RFID 기술은 현재 국내 모바일 RFID 포럼을 통해서 표준화 작업 중이며, 여기에 아직 보안 모델에 관한 상세는 정의되어 있지 않은 상태이다. 현재까지는 상용화되어있는 서비스가 아니며, 유통되는 물품에 태그를 부착하여 단말부착리더를 통해서 태그 정보를 획득하여 인터넷을 통해서 태그와 관련된 정보를 사용자에게 제공하는 기술이다. 해당 물품에 관련된 정보는 보안상 중요하며, 특히 구매나 혹은 금융 서비스와 관련된 모바일 RFID 응용의 경우에는 사용자의 프라이버시 정보와 결합된 정보가 불법으로 유출될 수 있으므로 모바일 RFID 서비스에서의 보안은 매우 중요한 항목이다.

현재 제공되는 AAA 프로토콜은 이러한 모바일 RFID 기술에 대한 고려가 전혀 되어 있지 않은 상태이다. 단지 망 접속에 따른 인증, 권한 검증, 과금 서비스만을 제공하고 있다. 그러나 모바일 RFID 서비스가 신뢰성 있게 그리고 차별적으로 제공되기 위해서는 모바일 RFID 서비스 관련 노드 간 보안 연관이 수립되어 적용되어야 하며, 개인의 등급과 관련 정보 제공 서버의 정책에 따른 차별적인 권한 검증 서비스가 제공되어야 한다.

본 논문은 이러한 AAA 프로토콜의 한계를 극복하기 위해서 모바일 RFID 시스템에 대해서 권한 검증, 보안 연관 설정 서비스를 제공하도록 확장한다. 이러한 기능을 제공하기 위해서 본 논문은 Diameter 프로토콜을 확장하며, Diameter 클라이언트 역할과 모바일 RFID 서비스 에이전트 역할을 수행하는 노드를 정의하고, 사용자 QoS에 기반한 차별적인 서비스 제공과 안전한 모바일 RFID 서비스를 제공할 수 있도록 한다.

Ⅱ. 안전한 모바일 RFID 망 구조

다음 그림 1은 본 논문이 제안하는 안전한 모바일 RFID 서비스 망 구조를 나타낸다. 안전한 모바일 RFID 서비스를 위해서는 RFID 태그가 부착된

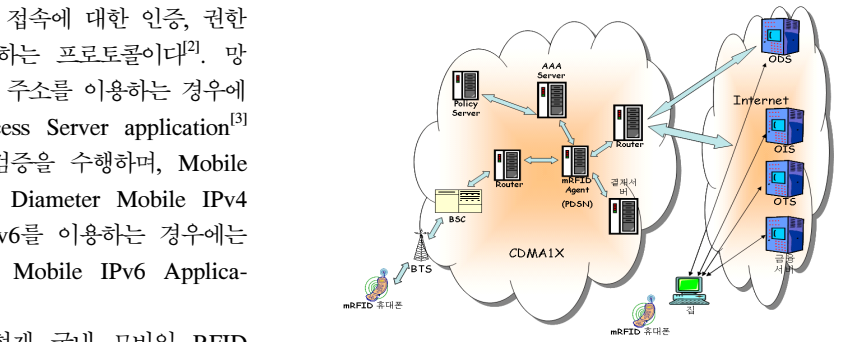

그림 1. 안전한 모바일 RFID 서비스 망 구조

물품, RFID 리더가 장착된 휴대폰, 모바일 RFID 서비스를 위한 모바일 RFID 에이전트와 망 접속 인증을 위한 AAA(Authentication, Authorization, Accounting) 서버, 정책 서버(Policy Server), 물품 정보를 보유하고 있는 OIS(Object Information) 서버, tag 부착 물품의 정보를 보유한 서버의 주소를 검색해주는 ODS(Object Directory Service), 그리고 선택적으로 OTS(Object Traceability) 서버와 금융 서버로 구성된다.

휴대폰으로 획득한 RFID 정보는 이동통신망을 통해서 인증이 수행된 후, ODS, OIS, OTS, 금융서버로 전송된다. 망 접속에 대한 인증은 망 접속 형태에 따라서 Diameter Network Access Server Application[3]이나, Diameter Mobile IPv4 Application [4]혹은 Diameter Mobile IPv6 Application[5]과 같은 응용을 이용해서 인증을 수행하며 필요한 권한 검증, 과금을 수행한다.

Ⅲ. 모바일 RFID 응용 서비스 예제

본 논문 동작의 이해를 돕기 위해서 다음과 같은 두 가지 응용 예를 정의한다.

3.1 보석 제품 정보 제공 및 구매, 이력 조회 서비스

모바일 RFID 리더가 장착된 휴대폰을 이용하는 사용자는 매장에서 RFID tag가 부착된 사파이어 반지를 구매하려고 한다. 휴대폰 사용자는 반지에 휴대폰을 가까이한다. 휴대폰은 RFID tag로부터 객체식별정보(UII: Unique Item Identifier)를 획득한다. 획득된 객체식별정보는 ODS query로 생성되어 ODS로 전송된다. ODS는 반지에 대한 상세정보를 제공하는 응용서버의 주소(URL:Uniform Resource Locator) 및 기타 정보를 휴대폰으로 전송한다. 휴

대폰은 해당 응용서버로 접속하여 반지에 대한 상세정보를 사용자에게 제공한다. {반지식별자, 사피어어순도, 사파이어산지, 반지제조사, 가격, 반지관련동영상, etc}. 사용자는 해당 정보를 확인한 후, 구매를 결정하고 구매절차를 수행한다. 구매는 모바일 결재서비스를 이용한다. 결재 완료된 후, 사용자는 구매한 반지를 가지고 집으로 돌아온다. 집에 돌아온 사용자는 휴대폰을 PC에 연결해서 휴대폰에 저장되어 있는 정보들을 이용해서 응용서버(OIS)와 이력제공서버(OTS), 금융서버에 직접 접속하여 구매 관련 정보, 물품관련 정보, 물품의 이력 정보 등을 조회한다.

3.2 전자금융서비스

모바일 RFID 리더가 장착된 휴대폰을 이용하는 사용자는 RFID tag가 부착된 통장이나 카드에 휴대폰을 가까이한다. 휴대폰은 RFID tag로부터 객체식별정보(UII: Unique Item Identifier)를 획득한다. 획득된 객체식별정보는 ODS query로 생성되어 ODS로 전송된다. ODS는 해당 RFID tag 부착 금융서버의 URL을 제공한다. 사용자는 휴대폰을 통해서 금융서버에 접속하여 계좌조회 혹은 통장 정리, 계좌이체 등의 서비스를 제공받는다.

이러한 두 가지 유형의 응용 서비스를 위해서 본 발명은 다음과 같은 권한 검증과 보안 연관 설정 및 분배 기능을 제공한다. 첫번째 응용의 경우에는 사용자의 QoS에 따른 권한 검증이 중요한 응용이며, 두번째 응용의 경우에는 노드간 보안 연관이 매우 민감한 응용이다.

본 논문은 망 접속 유형을 Mobile IPv6를 사용하는 환경으로 가정한다. 모바일 RFID 서비스의 특성상 컨텐츠의 지속적인 수신 및 서비스 세션의 유지, 이동성 보장이 요구되므로 Mobile IP 서비스를 사용하도록 한다. 따라서 본 논문은 망 접속 인증을 Diameter Mobile IPv6 Application[5]을 이용하도록 한다.

Ⅳ. 구성노드

본 발명의 구성 노드들은 다음과 같다.

- 모바일 RFID Agent: 모바일 RFID 서비스를 위한 에이전트 역할과 함께, AAA 클라이언트의 역할을 수행하는 노드
- AAA 서버: 모바일 RFID 서비스에 대한 권한 검증, 과금, 보안 관련 정보 생성 및 분배 등의 기능을 제공하는 서버
- 정책 서버(Policy Server): 각 사용자에게 어느 정도의 서비스를 제공할 것이며, 보안 관련해서는 각 노드 간 어떠한 정책을 적용할 것인지에 대한 정책을 수립 관리하는 서버. 정책 서버와 AAA 서버는 논리적 개념이며 물리적으로 동일할 수도 있음
- ODS(Object Directory Service): 객체검색서버로 RFID 코드 관련 정보 제공 서버의 URL(Uniform Resource Locator)을 검색
- OIS(Object Information Service): 응용서버로 RFID tag 부착 객체에 대한 상세 정보를 제공하는 서버로, 정보는 text, 이미지, multimedia등의 형식. 사용자의 등급(QoS level)에 따른 정보 제공
- OTS(Object Traceability Service): 이력제공서버로 RFID tag 부착 객체의 이력정보를 제공하는 서버. 사용자의 QoS level에 따른 정보를 제공
- 금융서버/결재서버: 휴대폰과 연결된 특정 은행의 서버이거나 혹은 태그가 부착된 통장 혹은 카드가 등록되어 있는 은행의 서버로, RFID tag에 연결하여 해당 사용자의 결재 관련, 혹은 은행 거래 내역 조회 등의 서비스를 제공
- 휴대폰: RFID reader가 장착된 휴대폰
- 객체(태그부착): 태그가 부착된 특정 객체로 사용자에 의한 구매 대상이거나 혹은 태그가 부착된 통장 혹은 카드

Ⅴ. 모바일 RFID 보안 개요

본 논문의 권한 검증은 다음과 같이 수행된다. 모바일 RFID 서비스를 위한 권한 검증을 하기 위해서 다음과 같은 사전 설정작업이 수행되어져야한다.

- 사용자 등급(QoS level)이 사전에 정해진다. 등급 설정 및 할당은 각 서비스별, 서비스 제공사별로 다를 수 있다.
- ODS, OIS, OTS, 금융서버 등은 각 사용자 등급에 따른 차별적인 컨텐츠를 제공하도록 구축되며, 해당 정책은 정책 서버에 등록된다. (예: QoS 레벨 0의 사용자에게는 text기반 정보만 제공, QoS 레벨 1의 사용자에게는 text+이미지 정보 제공, QoS 레벨 2의 사용자에게는 동영상 제공, QoS 레벨 3의 사용자에게는 동영상 정보와 함께 관련 물품과 매치 상품정보까지 제공)

모바일 RFID 서비스를 위한 권한 검증은 망 접속에 대한 AAA 서버에서의 인증 절차가 성공적으로 수행된 이후에 처리된다. 망 접속에 대한 AAA 서버에서의 인증은 망 접속 형태에 따라서 적당한 Diameter 응용을 이용하게 되며, 휴대폰(사용자)과 AAA 서버 간에 수행된다. 본 논문은 Mobile IPv6 서비스를 위한 망 접속 인증을 이용한다. AAA 서버는 해당 휴대폰 사용자에 대한 인증을 위해서 정책 서버에 접속할 수도 있다. 휴대폰을 통해서 요청된 망 접속 요청은 모바일 RFID 에이전트에 의해서 Diameter 메시지로 생성되어 AAA 서버로 전달되며, AAA 서버는 해당 휴대폰(사용자)에 대한 인증 완료시 결과를 모바일 RFID 에이전트로 전송하고, 모바일 RFID 에이전트에 의해서 ODS를 접속, 사용자가 필요로하는 정보제공 서버의 정보를 획득하여 이를 휴대폰으로 전송한다. 사용자는 휴대폰을 이용하여 해당 정보제공서버에 접속하여 원하는 contents를 획득한다.

그림 2는 이와 같은 인증 처리 절차를 각 노드간 메시지흐름을 통해서 나타낸다.

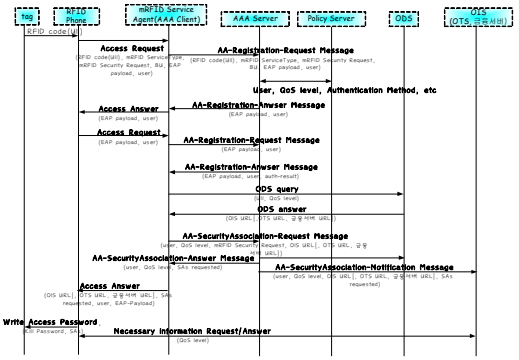

그림 2. 인증 처리 및 권한검증, 보안연관 설정 절차

그림 3은 노드간 정보의 흐름을 도시한다. RFID 리더를 통해서 획득된 RFID code(UII)는 이동통신망을 타고 인증을 받는다. 인증 완료 후, ODS 질의 처리를 하고, 질의 처리 후 획득된 OIS, OTS, 금융서버등과의 보안연관설정 작업이 동적으로 수행된 후, 설정된 보안 연관 정보를 각 노드(휴대폰, OIS, OTS, 금융서버)로 전달한다. 이후 전달된 보안 연관을 이용하여 노드간 통신이 안전하게 처리된다.

본 논문은 Mobile IPv6 응용을 이용하는 것으로 한다. 또한 본 논문은 휴대폰으로부터의 traffic을 최소화하기 위해서 망 접속요청 메시지(ARR : AA-Registration-Request)에 휴대폰에 장착된 RFID

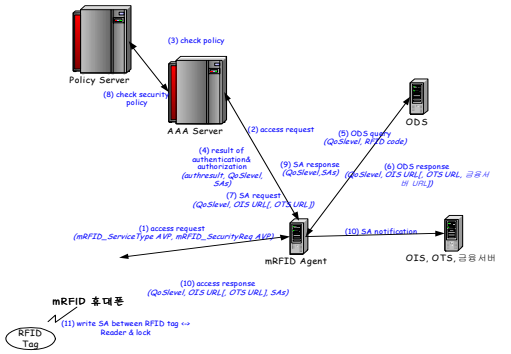

그림 3. 정보 처리 흐름도

reader가 획득한 RFID code 정보와 휴대폰으로부터의 보안연관 설정 요청(mRFID Security Request) 및 기타 요구 사항(mRFID ServiceType)을 모두 포함하여 인증이 완료된 후, 모바일 RFID 에이전트에 의해서 ODS 서버로부터 OIS, OTS, 금융 서버 등의 정보를 모두 획득하고 관련 보안 연관정보 등을 모두 획득하여 인증 결과와 함께 획득된 정보를 휴대폰 및 관련 노드에 전달되도록 한다.

Ⅵ. 모바일 RFID 보안 처리 절차

처리 절차를 상세히 정의하면 다음과 같다.

1) 휴대폰을 이용해서 RFID tag정보를 획득한 후, 이동통신망을 이용해서 인터넷을 사용할 수 있는지 network access control이 수행되어져야한다. 본 논문은 Diameter Mobile IPv6 Application을 이용한다. 휴대폰은 access request에 사용자가 접속하고자하는 서버의 유형(OIS, OTS, 금융서버)을 명시하고, 보안을 위해서 다음과 같은 정보를 요청한다.
   - RFID tag와 휴대폰(RFID reader)간에 이용할 인증 정보와 선택적으로 encryption 정보 요청
   - 휴대폰과 mRFID 서비스 에이전트(AAA Client)간 사용할 사용자 인증 정보와 암호화 정보 요청
   - 사용자가 PC/phone을 통해서 응용 서버에 접속할 때 필요한 사용자 인증 정보와 암호화 정보 요청
   - 사용자가 PC/phone을 통해서 이력제공서버에 접속할 때 필요한 사용자 인증 정보와 암호화 정보 요청
   - 사용자가 PC/phone을 통해서 금융서버에 접속할 때 필요한 사용자 인증 정보와 암호화

정보 요청

이러한 정보를 요청하기 위해서 AVP(Attribute Value Pair)를 추가적으로 정의하며, 새로 정의된 AVP는 Diameter Mobile IPv6 Application의 인증 요청 메시지인 ARR에 추가적으로 포함된다.

mRFID_ServiceType AVP : 단일 혹은조합도 가능함.
0 : OIS 이용
1 : OTS 이용
2 : 금융서버 이용
mRFID_SecurityReq AVP :
0 : RFID tag와 Reader간 보안 정책 요청
1 : 휴대폰과 mRFID 에이전트(AAA Client)간 보안 정책 요청
2 : 휴대폰과 OIS 간 보안 정책 요청
4 : 휴대폰과 OTS 간 보안 정책 요청
8 : 휴대폰과 금융 서버 간 보안 정책 요청

2) 휴대폰으로부터의 인증 요청은 모바일 RFID 에이전트(ex.PDSN)로 전송되고, 모바일 RFID 에이전트는 해당 정보를 Diameter 메시지로 생성하여, AAA 서버로 전송한다.
3) 휴대폰과 이동통신망이 관리하는 AAA 서버에 의해서 인증이 수행된다. EAP 인증을 사용할 경우에는 인증 노드와 인증 서버 간 multi-roundtrip이 발생 가능하다. 성공적으로 처리된 경우 AAA 서버는 정책서버로부터 수신한 해당 사용자의 QoS level과 사용자가 휴대폰을 통해서 요청한 mRFID_ServiceType AVP, mRFID_SecurityReq AVP 내용을 비교해서 권한 검증을 수행한다. 권한 검증이 성공적인 경우, AAA 서버는 모바일 RFID 에이전트로 인증 결과를 전송한다. 사용자의 QoS level이 포함된 ARA(AA-Registration-Answer) 메시지를 이용한다. 홈 에이전트에 대한 Mobile IPv6 처리는 HAR/HAA(Home-Agent-MIPv6-Request/Home-Agent-MIPv6-Answer) 메시지를 이용하며, 해당 처리가 완료된 후 이후 모바일 RFID 에이전트에 의한 처리가 진행되나 본 논문에서는 생략하도록 한다. 모바일 RFID 에이전트는 수신한 인증 응답의 결과가 성공인 경우, 해당 RFID 코드를 ODS로 전송한다. 이때 사용자의 QoS level을 함께 보낸다. QoS 레벨은 다음과 같은 내용을 포함한다.

mRFID_QoSLevel_AVP :
- 사용자가 OIS만을 사용할 것인지, OTS까지 이용할 수 있는지
- OIS를 사용할 경우, OIS에서 제공하는 정보를 어디까지 제공할 수 있는지, 예를 들자면 text기반 정보만 제공하거나, 혹은 multimedia정보를 제공하거나, 혹은 특별한 보안장치없이 보여줄수있는 정보만을 보여주거나, 보안장치가 함께 제공된 경우 보여줄수있는 모든 정보를 보여주거나
- OTS를 이용하는 경우, OTS의 정보 어디까지를 제공할 것인지. OIS의 경우와 마찬가지로 다양한 경우의 level을 정의할 수 있다.

4) ODS는 QoS level에 따라서 관련 물품에 대한 응용 서버의 URL, 이력제공서버의 URL을 검색하여 모바일 RFID 에이전트로 전송한다. RFID tag이 통장이나 신용카드에 부착된 경우 혹은 휴대폰에 금융서버가 연결된 경우, 관련 금융서버의 URL이 포함된다.
5) 모바일 RFID 에이전트는 사용자가 요청한 경우, 태그와 리더(휴대폰) 간, 휴대폰과 mRFID 서비스 에이전트 간, 휴대폰과 획득된 응용 서버 간, 휴대폰과 이력 제공서버 간 그리고, 휴대폰과 금융서버 URL에 대한 보안 연관(SA) 설정요청을 AAA 서버로 전송한다. 이때 사용할 Diameter 메시지를 추가 정의한다. 추가 정의되는 메시지는 AA-SecurityAssociation-Request/Answer와 AA_SecurityAssociation-Notification이다. 각 메시지는 다음과 같은 정보들을 포함한다.

AA-SecurityAssocation-Request: user, QoS level, OIS URL, OTS URL, 금융서버 URL, mRFID Security-Request
AA-SecurityAssocation-Answer: user, QoS level, SAs requested
AA-SecurityAssocation-Notification: user, QoS level, SAs requested

6) AAA 서버는 요청받은 보안 관련 정보들과 각 서버들의 정책에 기반하여 정보를 설정하여 모바일 RFID 에이전트로 전송한다. AA-Security Association-Answer, AA-SecurityAssociation-Answer 메시지를 이용한다.
7) 모바일 RFID 에이전트는 ODS로부터의 응답과 AAA 서버로부터의 응답을 포함하는 응답 메시지를 휴대폰으로 전송한다. OIS, OTS, 금융서버에 관련 보안 연관정보를 전달한다.
8) 휴대폰은 응답 메시지에 RFID tag간 보안 정보(EPC C1G2의 경우, access password, kill password, encryption정보등)를 태그에 기록하고, lock을 건다. 패스워드 기록 시 반드시 encryption 하여 기록하도록 한다. Encryption의 경우에는 휴대폰과 AAA 서버간 공유하는 AAA key를 이용하여 shared secret을 생성하고 AAA 서버가 선택한 알고리즘을 이용하도록 한다. 다른 노드와의 보안 연관 정보는 휴대폰에 저장하며 각 노드와의 접속 시 이용할 수 있도록 한다.
9) 사용자는 해당 응용 서버(OIS)로 접속하여 물품의 상세 정보를 획득하여 사용자에게 보여준다. 이때 사용자의 QoS를 반드시 포함하도록 한다. 만약 보안이 필요한 경우 해당 정보 요청 메시

지는 AAA 서버에 의해서 생성된 보안 정책에 의해서 보호되도록 한다.

10) 선택적으로 사용자는 해당 OTS로 접속하여 물품의 이력 정보를 획득하여 사용자에게 보여준다. 이때 사용자의 QoS를 반드시 포함하도록 한다. 만약 보안이 필요한 경우 해당 정보 요청 메시지는 AAA 서버에 의해서 생성된 보안 정책에 의해서 보호되도록 한다.
11) 선택적으로 사용자는 해당 금융서버로 접속하여 관련 금융정보를 획득하여 사용자에게 보여준다. 이때 사용자의 QoS를 반드시 포함하도록 한다. 만약 보안이 필요한 경우 해당 정보 요청 메시지는 AAA 서버에 의해서 생성된 보안 정책에 의해서 보호되도록 한다.

선택적으로 휴대폰 사용자가 집에서 PC를 이용해서 OIS, OTS, 금융서버로 접속하여 정보를 보고자하는 경우, 휴대폰에 저장된 보안연관 정보와 각 서버의 URL정보를 이용하여 접속한다.

Ⅶ. 결 론

세계적으로 RFID 기술은 큰 관심을 가지고 개발되고 있으나, 반면 그 보안 위협으로 인해서 반감도 만만치 않은 상황이다. 더구나 모바일 RFID 서비스는 그 위협이 더욱 크다. RFID 리더가 이동성을 갖게 되므로 언제 어디에서 정보가 유출되어 악용될 수 있다.

본 논문은 이러한 상황에서 사용자에게 안전한 서비스를 제공할 수 있도록 보안 채널을 제공하며, 이러한 서비스를 사용자 등급별로 차별적으로 제공할 수 있도록 함으로써 모바일 RFID 서비스 업체에게 수익성을 제공하여 보다 빠르고 적극적인 서비스 활성화에 기여할 것으로 기대된다. 특히, 각 태그와 관련된 정보가 좀 더 세분화되어 다양한 형태로 제공될 수 있다면 사용자 등급에 따른 권한 검증과 보안 채널 제공은 모바일 RFID 서비스 사업을 하려는 업체에게 매력적인 기술이 될 수 있을 것이다.

참 고 문 헌

〔1〕 Auto-ID Savant Specification v1.0, 2003.9.
〔2〕 Diameter Base Protocol, RFC3588, 2003.9.
〔3〕 Diameter Network Access Server Application, RFC 4005, 2005.8.
〔4〕 Diameter Mobile IPv4 Application, RFC 4004, 2005.8.
〔5〕 Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-03.txt, April 2003.

김 말 희 (Marie Kim) 정회원

1996년 1월 서강대학교 전자계산학과 학사
1998년 1월 서강대학교 전자계산학과 석사
1998년 1월~2000년 11월 삼성전자 통신연구소 근무
2000년 11월~2005년 2월 한국전자통신연구원 정보보호연구단 AAA정보보호연구팀
2005년 3월~2006년 현재 한국전자통신연구원 RFID/USN 미들웨어연구팀 근무
<관심분야> 이동통신, 정보보호

이 용 준 (Yong Jun Lee) 정회원

1987년 연세대학교 전산학 석사
1993년 정보처리기술사(전자계산조직응용)
2001년 충북대학교 전산학 박사
1984년~현재 한국전자통신연구원 책임연구원
현재 한국전자통신연구원 RFID/USN 미들웨어연구팀장
<관심분야> 스트림 데이터마이닝, 센서 DB, DB 보안, 워크플로우