전자금융 통합인증기술의 국내외 표준화 동향

정영곤, 김근옥, 심희원
금융보안연구원

요 약

오늘날 사람들은 PC, 테블릿, 스마트폰 등 다양한 모바일기기를 이용하여 시간과 공간의 제약 없이 인터넷에 접속하여 전자금융 서비스를 편리하게 이용하고 있다. 이렇게 전자금융 서비스를 편리하게 이용하고 있지만, 사용자의 금융정보도 온라인을 통해 전송되고 있어서 이를 노린 다양한 해킹위협에 노출되어 있다. 더욱이 금전적 이득을 노리고 불법적으로 금융정보를 탈취하는 등의 전자금융 이용자를 대상으로 하는 악의적인 목적의 다양한 해킹공격이 발생하고 있다. 이러한 해킹위협에 대응하기 위하여 OTP, 보안카드 등의 인증매체를 사용하고 있으나, 여러 서비스 제공자에 접속하기 위하여 다수의 인증매체를 발급해야 하는 불편이 뒤따르고 있어 통합인증기술에 대한 요구가 증가하고 있다. 국내외 표준화 기구에서 활발하게 추진하고 있는 전자금융 통합인증기술은 스마트환경에 적합한 다양한 인증기술을 통합하여, 사용자와 여러 서비스 제공자가 공동으로 이용할 수 있도록 하는 것을 목표로 한다. 통합인증기술은 크게 여러 사용자와 서비스 제공자를 통합하여 서비스를 제공할 수 있는 프레임워크와 사용자 인증 등에 필요한 OTP, BIO 등 다양한 요소 인증기술, 그리고 서비스 제공에 필요한 보안 요구사항으로 구분할 수 있다. 본 논문에서는 통합인증 프레임워크, 요소 인증기술, 보안 요구사항의 국내외 표준을 분석하고 표준화의 동향을 알아봄으로써 다양한 환경에서 안전하고 편리하게 사용할 수 있는 통합인증기술을 전망해본다.

Ⅰ. 서 론

2013년말 국내 인터넷뱅킹 서비스(모바일뱅킹 포함)의 등록 고객수는 9,549 만명으로 작년말 대비 10.5%가 증가하는 등 국내 전자금융거래는 모바일기기 등 다양한 환경을 이용하여 계속적으로 증가하는 추세를 보이고 있다[1]. 하지만 이와 함께 전세계적으로 2013년 3분기 인터넷뱅킹 거래의 악성프로그램이 20만건을 초과하여 전분기 대비 38%가 증가하는 등 금전적 이득을 노린 전자금융의 공격도 급속히 증가하는 추세를 보이고 있다[2].

전자금융에 대한 고도화되는 보안위협에 대응하기 위하여 최근에는 ID/PW 뿐만 아니라 보안카드, OTP 발생기, 휴대폰 SMS 인증 등이 사용되고 있으며, 중국, 싱가포르, 유럽 등에서는 거래서명기술을 적극 도입하여 고액이체 등 고위험의 거래에 활발히 사용하고 있다[3].

뿐만 아니라, 싱가포르, 스웨덴, 노르웨이 등에서는 다양한 사용자 인증매체를 통합적으로 이용·관리하고 보안위협을 효율적으로 관리하기 위한 통합인증서비스에 대한 연구가 꾸준히 진행되고 있다. 이와 관련하여 국내외에서는 차세대 인터넷 서비스기반 통합인증/응용의 표준화를 적극적으로 추진하고 있어, 본 논문에서는 해당 표준안을 중심으로 설명하고자 한다.

본 논문의 구성은 2장에서 전자금융 인증기술과 관련된 표준안을 통합인증 프레임워크와 요소 인증기술, 그리고 통합인증 서비스를 위한 보안요구사항으로 분류하여 주요 표준안의 내용을 살펴보고, 3장에서는 본 논문의 결론으로 전자금융 인증기술의 표준화 전망을 기술한다.

Ⅱ. 국내외 표준화 동향

1. 전자금융 인증기술 표준화의 분류

본 논문에서는 전자금융 인증기술의 표준화 대상을 〈그림 1〉과 같이 통합인증 프레임워크, 요소 인증기술, 보안 요구사항의 세가지 분류로 구분하였다. 첫째는 통합인증 프레임워크는 BIO, OTP, OOB 등 다양한 요소 인증기술을 수용하여 통합인증서비스의 제공이 가능하게 하는 프레임워크를 제공한다. 둘째는PC, 모바일기기 등 다양한 환경에 적합한 사용자 인증기술을 정의하여 표준화한다. 마지막으로 안전하게 서비스를 제공하기 위한 프레임워크와 인증기술의 보안 요구사항을 정의한다. 즉, 통합인증 서비스의 제공을 위해서 기본이 되는 큰 프레

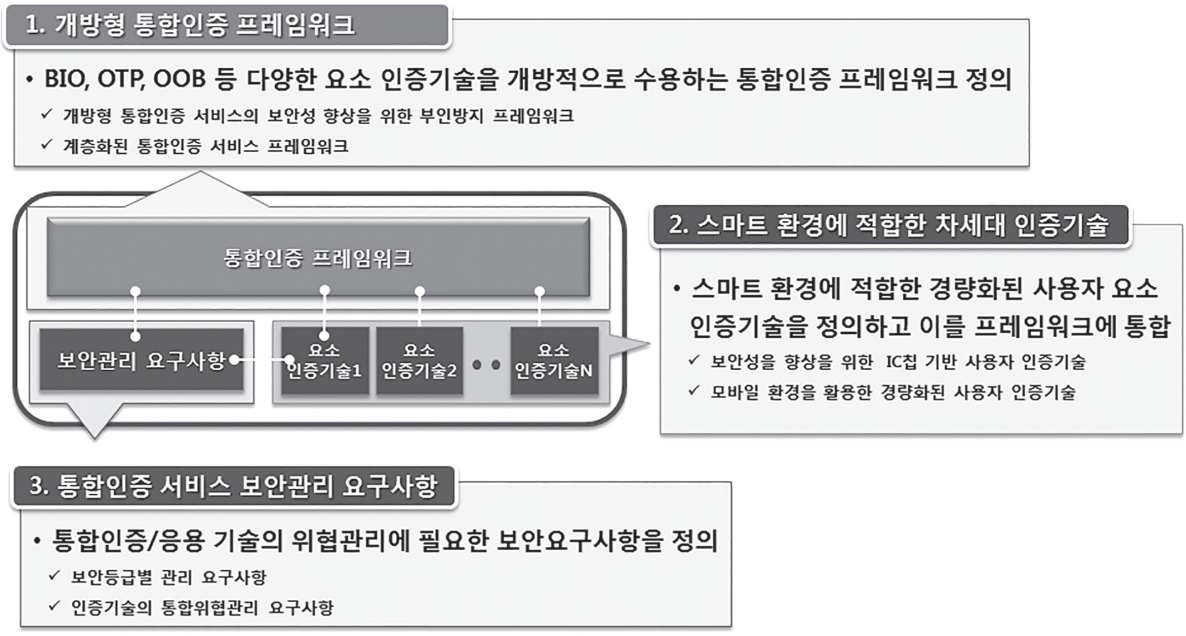

그림 1. 통합인증서비스 관련 표준화 분류

임을 만들어서 그 안에 요소기술로 수용될 수 있는 인증기술을 개발하고 안전하게 서비스 될 수 있도록 프레임워크과 인증기술의 보안 요구사항을 제시한다. 본 논문에서는 각각의 분류와 관련하여 제정되었거나 진행중에 있는 국내외 표준화의 동향을 알아본다.

2. 통합인증 프레임워크 표준화 동향

2.1 TTAK.KO-12.0192, IC칩 기반 보안 매체를 활용한 통합형 사용자 인증 서비스 프레임워크

본 표준[4]에서는 금융분야에서 OTP 발생기, 스마트 카드, 보안 토큰, BioHSM 등 IC칩 기반의 보안 매체를 활용한 사용자 인증기술의 통합을 정의하였다. 이 표준에서 정의하는 IC 칩은 칩 내에 메모리와 CPU를 포함하고 있어서 비밀정보를 안전하게 저장하고 관리할 수 있다. 통합형 사용자 인증 서비스는 IC 칩 기반 보안 매체를 활용하여 보안성을 높이고, 인증기술의 통합으로 사용자의 편의성은 향상시켜준다. 또한 서비스 제공자는 프레임워크에 적용된 인증기술을 사용자에게 별도로 보급하지 않고, 이미 배포된 인증매체 등을 공유하여 사용할 수 있어 인증기술의 적용성과 확장성을 높일 수 있다.

〈그림2〉는 IC칩 기반 통합형 사용자 인증 서비스 프레임워크 개념도이다. 사용자는 IC칩 기반의 보안 매체를 이용하여 인터넷 뱅킹, 전자 상거래 등의 서비스를 제공받기 위해 사용자 인증을 수행하며, 각각의 서비스 제공자는 통합 인증 센터를 통해 사용자 인증 서비스를 제공한다.

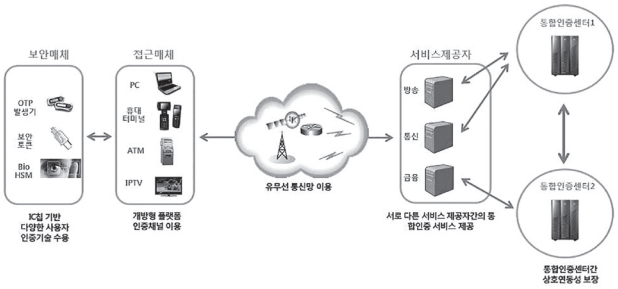

그림 2. 프레임워크 개념도

사용자 인증 서비스에 대한 통합은 서비스에 참여하는 개체간의 연동방식에 따라 구분되며, 세부적인 서비스 모델은 서비스 제공자와 통합 인증 센터를 통해 사용자 인증 서비스를 제공하는 단순모델, 여러 서비스 제공자 간 통합 인증이 가능한 모델, 민간, 공공 등 도메인 간 상호 운용이 가능한 모델로 구분된다.

- 단순모델 : 다양한 서비스 제공자에게 기존에 발급받은 보안 매체를 이용해서 사용자 인증을 요청하면, 서비스 제공자는 통합 인증 센터를 통해 사용자 인증을 수행하는 가장 단순한 모델
- 서비스 제공자 통합형 : 각각의 서비스 제공자가 IC칩 기반 사용자 인증 서비스를 구축하고, 추가적으로 통합 인증 센터와 연계하여 사용자 인증서비스를 제공
- 도메인 간 상호 운용 모델 : 다른 도메인 간 통합 인증 센터를 연계하여 사용자 인증 서비스를 제공할 수 있는 모델로 서로 다른 도메인간 사용자 인증 서비스 정책을 정의하고 인증 정책을 통해 서로 사용자 인증 서비스를 공유

2.2 ITU-T X.1156, An One time password based non-repudiation framework

기존 전자금융 환경에서 금융거래에 대한 부인방지 기능을 제공할 수 있는 기술로는 공개키 기반의 전자서명인 공인인증서가 유일하였다. 본 표준[6]에서는 대칭키 기반의 OTP로 부인방지 기능을 제공할 수 있는 기술을 제시한다.

부인방지는 사용자가 메시지를 송신하고도 이를 시행하지 않았다고 주장하는 송신자의 부인을 막는 송신 부인방지(NRO, non-repudiation of origin)와 수신자측에서 메시지가 전달된 사실을 송달되지 않았다고 주장하는 수신자의 부인을 막는 수신 부인방지(NRD, non-repudiation of delivery)로 구분된다. 부인방지토큰은 크게 송신부인방지토큰(NROT, Non-Repudiation of Origin Token)과 수신부인방지토큰(Non-Repudiation of Delivery Token)으로 구분한다. 송신부인방지토큰은 서비스 제공자가 보관하고 수신부인방지토큰은 사용자가 보관하여 분쟁이 발생할 경우 각각의 토큰으로 송수신행위를 증명할 수 있다.

OTP기반의 부인방지는 각각의 객체가 금융거래정보를 포함하여 OTP를 기반으로 부인방지 토큰 메시지를 생성하여 신뢰기관에 부인방지 토큰을 요청하면 신뢰기관은 요청 메시지를 검증하여 부인방지토큰을 생성하여 전달한다. 신뢰기관은 객체의 부인방지토큰에 대한 검증 요청에 대해서도 요청메시지를 검증하여 결과를 전달하는 역할도 한다.

OTP기반의 부인방지 서비스 모델은 제3의 신뢰기관(TTP)과 사용자와 각 객체 사이에서 부인방지 토큰을 전달하는 통신방법에 따라 4가지로 분류하고 있다.

〈그림 3〉는 NROT 통신방법을 나타내며 서비스 제공자가 TTP로부터 송신부인방지토큰을 직접 전달받는 방식과 사용자를 통하여 전달받는 방식에 따라 두 가지로 구분되며 후자의 경우 송신부인방지토큰에 대한 별도의 토큰검증 절차가 필요하다.

〈그림 4〉는 NROD 통신방법을 나타내며 사용자가 서비스 TTP로부터 수신부인방지토큰을 직접 전달받는 방식과 서비스 제공자를 통하여 전달받는 방식에 따라 두 가지로 구분되며 후자의 경우 수신부인방지토큰에 대한 별도의 토큰검증 절차가 필요하다.

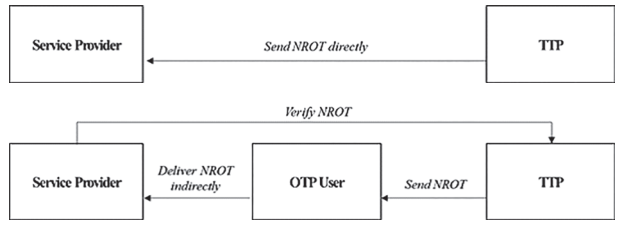

그림 3. NROT 통신방법

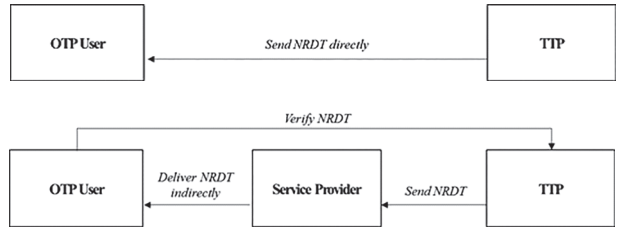

그림 4. NROD 통신방법

2.3 TTAK.KO-12.0194, 통합인증 기반 부인방지 서비스 프레임워크

본 표준[5]은 전자거래에서 사용되는 여러 가지 인증기술을 신뢰된 제3의 기관 (TTP, Trusted Third Party)에서 수용하여 사용자의 통합인증 서비스를 제공하고 이를 통하여 인증 받은 사용자에게 부인방지 기능을 제공하기 위한 프레임워크를 정의하고 있다.

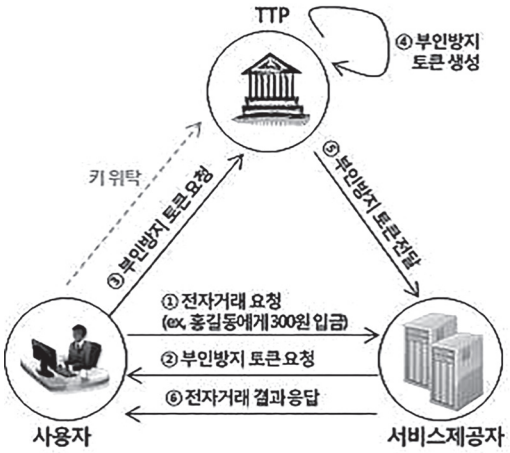

그림 5. 완전 위탁 부인방지 서비스 개념도

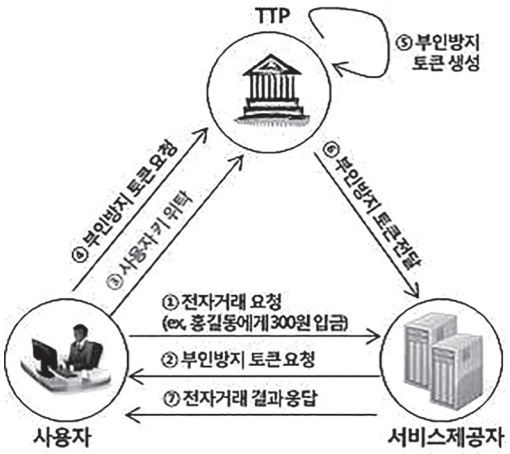

그림 6. 실시간 위탁 부인방지 서비스 개념도

통합인증 기반 부인방지 서비스 프레임워크는 사용자, 서비스 제공자, 신뢰된 제3자(TTP)의 객체로 분류되며, 서비스 모델은 크게 완전 위탁 부인방지와 실시간 위탁 부인방지가 있다. 완전 위탁 부인방지 서비스 모델은 사용자가 부인방지 토큰의 생성에 필요한 비밀키를 TTP에게 미리 위탁하고, 이 비밀 키를 이용해서 TTP가 사용자를 대신해서 부인방지 토큰을 생성 및 관리하는 모델로 〈그림 5〉에서 서비스 개념도를 보여준다. 실시간 위탁 부인방지 서비스 모델은 미리 사용자의 키를 등록하지 않고, 사용자가 자신의 키를 저장하고 있다가 필요시 키를 TTP에 위탁하여 부인방지 서비스를 제공받는 모델로 〈그림 6〉에서 서비스 개념도를 보여준다.

본 표준에서 제시한 키 위탁 부인방지 서비스는 기존에 국제 표준으로 정의되어 있는 부인방지 메커니즘 'ISO/IEC 13888-1', 'ISO/IEC 13888-3'을 준용하여, 해당 메커니즘을 확장한 모델을 정의한다.

2.4 ITU-T X.sap-9, Delegated non-repudiation architecture based on ITU-T X.813

본 표준[9]은 2012년 8월 ITU-T SG17에서 신규아이템을 제안하여 현재 계속 개발중에 있으며 3번째 수정제안서까지 승인되어 2014년 10월 최종 표준채택을 할 계획이다. ITU-T X.813을 기반으로 하여 서명권한만을 위임하는 모델과 서명권한과 서명키를 함께 위임하는 모델로 2가지 모델 아키텍쳐를 정의한다. 본 표준의 위임부인방지 모델은 키의 분실·도난 등에 대응 가능하며 전자금융 환경에서 신뢰기관을 통하여 보다 안전하고 편리하게 부인방지 서비스를 제공할 수 있는 것을 특징으로 한다.

〈그림 7〉는 위임부인방지 아키텍쳐의 콘셉트를 보여준다. 아키텍쳐의 객체는 서명권한을 위임하고 부인방지 서비스를 요청하는 사용자, 서명권한을 위임받아 사용자를 대신하여 부인방지정보를 생성·관리하는 신뢰기관, 인증서비스를 제공하는 별도의 인증정보 제공자, 사용자에게 서비스를 제공하는 서비스 제공자로 구성된다. 위임부인방지 아키텍쳐는 서명권한만을 위임하거나 서명권한과 서명키를 함께 위임하는 경우로 나눌 수 있다. 서명권한만을 위임하는 모델은 사용자가 처음 등록한 당시에 서명권한을 위임했음을 증빙하면, 이후에 신뢰기관이 자신의 키로 부인방지 증빙을 생성하는 대칭키 기반의 부인방지 서비스 모델이다. 서명권한과 서명키를 함께 위임하는 모델은 사용자가 등록과정에서 서명권한과 서명키를 위임하면 해당키를 활용하여 신뢰기관이 부인방지 증빙을 생성하는 비대칭키 기반의 부인방지 서비스 모델이다.

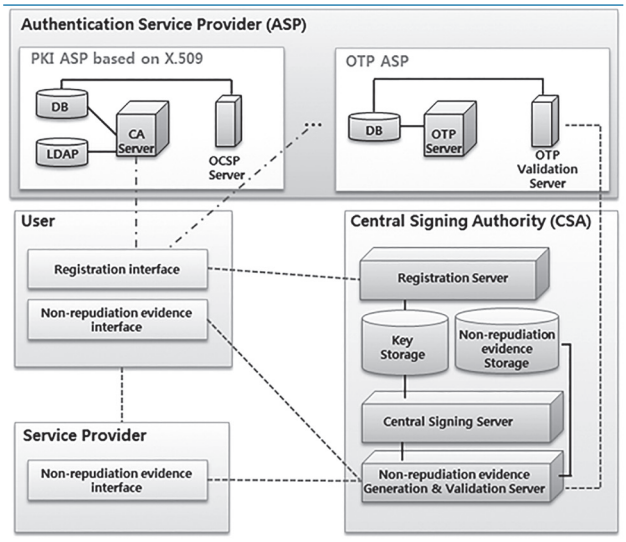

그림 7. 위임 부인방지 아키텍쳐 콘셉트

3. 요소 인증기술 표준화 동향

3.1 TTAK.KO-12.0218, 모바일 기기에 적합한 IC칩 기반 인증모듈용 API

본 표준[7]은 USIM, 스마트카드 등 IC칩에 중요 비밀정보를 저장하여, IC칩의 복제 및 위변조에 대응할 수 있는 IC칩 기반의 인증 모듈을 소개하고, 다양한 응용 프로그램에서 인증모듈을 사용할 수 있도록 관련 API의 규격을 정의하고 있다. IC칩 기반 인증모듈에서 사용하는 IC칩은 칩내에 메모리와 CPU를 포함하고 있어 중요정보를 안정하게 저장 및 관리하고 CPU를 통해 인증정보 생성에 필요한 연산을 하고 그 결과만은 칩 외부로 출력한다. 또한 IC칩의 보안성을 위한 TRM(Tamper Resistant Module) 기능을 제공해야 하며, 통신기능을 위한 접촉식(ISO 7816), 비접촉식(ISO 14443), NFC 기능 등을 제공해야 한다.

IC칩 기반 인증모듈은 크게 비밀정보, 인증 모듈, 구동 모듈로 구성되며, 인증 모듈과 구동 모듈 간에 인터페이스를 하는 인증 모듈용 API가 있다. IC내에는 비밀정보와 인증 모듈이 있으며, 비밀정보는 인증정보를 생성하기 위한 중요정보가 안전하게 저장되어 외부로 노출되지 말아야 하고, 인증 모듈은 IC칩 내에 저장된 비밀정보에 접근하여 인증정보를 생성하고 인증결과만을 IC칩 외부로 전달하는 역할을 한다. 구동 모듈은 모바일기기에 설치하고 인증 모듈로부터 받은 인증정보를 출력하는 등의 기능을 수행한다. 인증모듈에서 인증정보를 생성하고 입출력 등의 기능을 하는 인증모듈과 구동모듈 간에 인터페이스는 상호 호환성을 보장하기 위해 인증 모듈용 API를 이용한다.

위의 〈그림 8〉은 IC 칩 기반 인증 모듈용 API구조이다. 인증모듈은 인증모듈의 정보를 관리하는 모듈, 비밀정보를 관리하

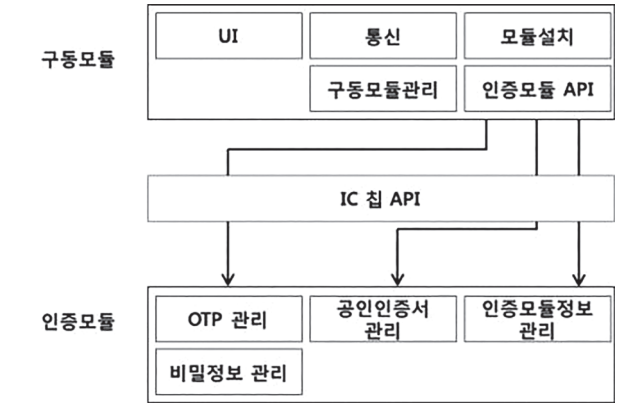

그림 8. 인증 모듈 API 구조

는 모듈, OTP(일회용 비밀번호)를 관리하는 모듈, 공인인증서를 관리하는 모듈로 구성되어 있다. 이렇게 구성된 IC칩 기반 인증 모듈은 인증기술의 확장을 용이하게 하기 위해 IC칩을 관리하는 인증모듈 정보관리와 각각의 인증기술을 하나의 모듈로 구성한 것이 특징이다.

3.2 TTAK.KO-12.0221, 모바일 기기를 이용한 다중 요소 인증 메커니즘

본 표준[10]은 모바일 기기를 이용한 다중 요소 인증 메커니즘을 정의하고, 각각의 단일 요소(Single-factor) 인증기술을 결합한 다중 요소(Multifactor) 인증 메커니즘을 설명한다.

서비스를 받는 사용자가 적법한지 여부를 판별하기 위해 사용되는 요소를 인증요소라 하며 〈표 1〉과 같이 세가지 형태로 분류할 수 있다.

표 1. 인증 요소의 종류

인증 요소	설 명	예시
소지기반	사용자가 소유하고 있는 인증요소	OTP 발생기, 보안토큰 등
지식기반	사용자만이 알고 있는 인증요소	비밀번호, PIN 등
특성기반	사용자의 특성 정보 인증요소	홍채, 지문, 목소리, 얼굴 등

다중요소 인증이란 인증요소를 결합하여 두가지 이상의 인증요소를 사용하여 인증을 하는 것을 의미한다. 금융에서 사용되는 다중요소 인증으로 OTP, SMS, ARS 등을 비밀번호 외에 추가로 이용하는 것을 예로 들 수 있다. 이것은 하나의 인증 요소가 해킹에 의해 노출 또는 탈취되더라도 이와 독립된 다른 인증요소에 의해 보안위협에 대응할 수 있어 단일 요소 인증에 비하여 보안성이 높다.

다중요소 인증의 메커니즘을 크게 네가지의 모델로 정의하였고, 사용자, 매체(접속 매체, 인증 매체), 서비스 제공자로 구분하여 설명한다.

〈그림 9〉는 4가지의 서비스 모델을 비교하여 볼 수 있다. 첫번째 모델의 대표 서비스로는 전화 승인으로 사용자가 소유한 매체에서 생성한 소지기반 인증정보와 사용자의 인증정보를 서로 다른 채널을 이용하여 인증한다. 두번째 모델의 대표 서비스로는 휴대폰 문자 인증으로 사용자가 매체를 통하여 서비스 제공자로부터 전달받은 인증정보와 사용자의 인증정보를 다시 서비스 제공자에게 전달하여 인증한다. 세번째 모델의 대표 서비스로는 모바일 전자서명이 있으며 사용자의 인증정보를 매체를 통하여 인증받고 매체와 연결된 보안요소에서 생성된 인증정보를 서비스 제공자에게 각각 전달하여 인증한다. 네번째 모델의 대표 서비스로는 모바일 OTP로 매체를 통하여 보안요소에서 생성된 인증정보를 전달받아 사용자의 인증정보와 함께 서비스 제공자에게 전달하여 인증한다.

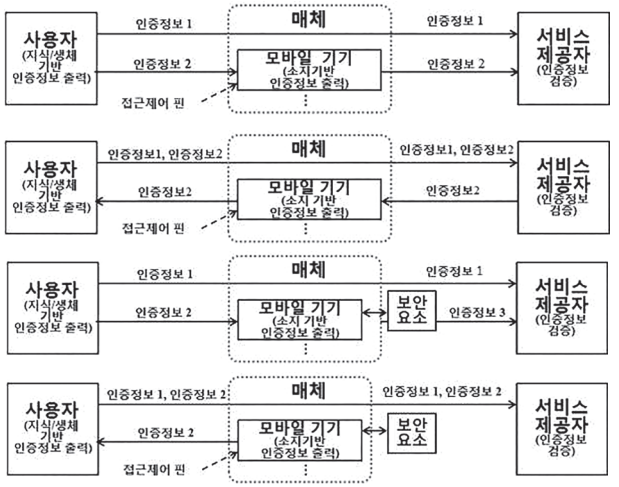

그림 9. 4가지 서비스 모델

표준문서에는 다중요소 인증 메커니즘에 필요한 보안 요구사항을 모바일기기, 보안요소, 서비스 제공자로 구분되어 정의하고 있고 각각의 모델에 대한 프로토콜을 정의하였다.

3.3 ITU-T X.sap-8, Multi-factor authentication mechanisms based on mobile devices

본 표준[9]은 2012년 8월 ITU-T SG17에서 신규아이템을 제안하여 현재 계속 개발중에 있으며 3번째 수정제안서까지 승인되어 2014년 10월 최종 표준채택을 할 계획이다. 위에서 분석한 국내표준인 '모바일 기기를 이용한 다중 요소 인증 메커니즘(TTAK.KO-12.0221)'과 범위와 내용은 비슷하지만 국외 전자금융 환경을 고려하고 여러 국가의 의견을 반영하여 표준화를

진행하고 있다.

표 2. 멀티팩터 인증의 결합

	결합	예시
Two factor 인증	지식기반+소지기반	패스워드+OTP
	지식기반+특징기반	패스워드+지문
	소지기반+특징기반	OTP+지문
Three factor 인증	지식기반+소지기반+특징기반	패스워드+OTP +지문

단일 인증요소로는 지식기반, 소유기반, 특성기반으로 구분하였고, 위치기반 인증요소를 추가로 설명하였다. 위치기반의 예로 재택근무를 할 경우에는 회사의 서버에 접속하는 컴퓨터는 미리 등록한 집의 위치를 확인하여 추가 인증요소로 사용하는 것을 들 수 있다. 아래의 〈표 2〉는 멀티팩터 인증의 결합 방법을 보여준다.

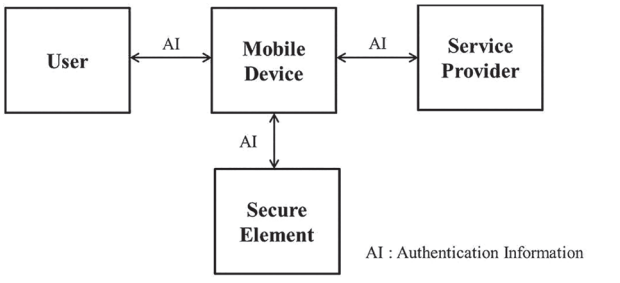

그림 10. Overview

〈그림 10〉은 멀티팩터 인증 메커니즘의 개념도를 보여준다. 사용자, 서비스제공자, 보안 요소가 모바일기기를 통하여 인증정보를 교환한다.

4. 보안 요구사항 표준화 동향

4.1 TTAK.KO-12.0219, IC칩 기반 인증 모듈 보안 요구사항

본 표준[8]은 요소 인증기술 표준인 '모바일 기기에 적합한 IC칩 기반 인증모듈용 API'에서 정의한 인증 모듈의 구성과 인증 모듈 API의 구조에 따라 발생 가능한 보안 위협을 분석하고 이에 대한 보안 요구사항을 정의하고 있다.

IC칩 기반의 인증 모듈에 대한 보안 취약성을 인증정보 생성, 인증 모듈의 발급 등을 포함하여 인증 시스템을 구성하는 모든 주체(인증 모듈 개발자, 인증 모듈 발급자 등)에서 공격이 발생할 가능성을 예상하여 표준에서는 크게 인증 모듈과 구동 모듈 간의 데이터 통신 공격, 인증 모듈과 구동 모듈의 위변조, 인증 모듈과 구동 모듈의 이용 환경 취약점으로 분류하여 설명한다.

위의 〈그림 11〉는 IC기반 인증 모듈의 보안 요구사항을 3가지 영역으로 구분됨을 보여준다. 인증모듈 영역, 구동모듈 영역,

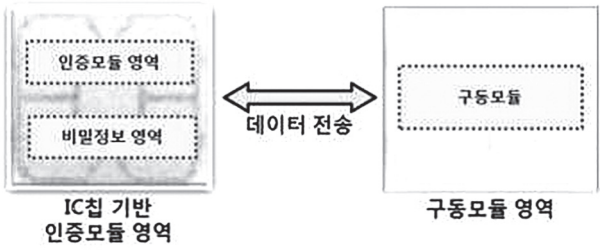

그림 11. 보안 요구사항 영역

일반 영역으로 구분하였고, 구분된 각각의 영역에서 요구되는 보안 요구사항을 체크한다.

4.2 TTA 2014-014, 전자거래 인증방법의 보증수준별 요구사항

2014년 2월에 신규표준과제로 채택되어 2014년 12월 표준제정을 목표로 현재 개발중에 있는 국내표준이다[11]. 전자거래에서 OTP, 보안카드, SMS 등 다양한 인증방법으로 본인임을 증명하고 있다. 국내 전자거래에서 사용되는 인증방법의 보안등급을 분류하여 스마트폰, IPTV 등 다양한 환경에 안전한 인증수단을 선택하여 사용할 수 있도록 한다. 인증수단의 발급, 인증, 관리의 단계에서 발생하는 다양한 보안 위협을 분석하여 보증레벨을 구분한다. 최종적으로는 인증방법의 보증수준별로 요구되는 사항들을 정의하여 보안위험의 수준에 따라 적합한 인증방법을 선택할 수 있도록 하는데 그 목적을 두고 표준개발을 한다. NIST와 ITU-T X.1252, ISO/IEC 29115 등의 관련 국외 표준문서를 분석하여 국내 전자금융 환경에 적용할 수 있도록 한다.

4.3 TTA 2014-016, 통합인증서비스를 위한 신뢰기관의 보안 요구사항

2014년 2월에 신규표준과제로 채택되어 2014년 12월 표준제정을 목표로 현재 개발중에 있는 국내표준이다[12]. 신뢰기관(TTP, Trusted Third Party)은 통합인증 프레임워크에 사용자와 서비스 제공자 사이에서 신뢰를 바탕으로 통합인증 서비스를 제공한다. 이렇게 여러 사용자와 서비스 제공자가 제3의 신뢰기관을 통하여 인증서비스를 제공받기 때문에 투자, 관리 등의 비용절감 및 통합 보안관리가 가능하다. 하지만 통합에 따른 서비스 집중으로 인하여 서비스 가용성 및 인증정보 보안성에 단일장애점(single point of failure)이 발생하는 등의 위협이 존재할 수 있다. 이에 본 표준에서는 전자금융환경에서 통합인증서비스에 따른 보안 위협을 분석하여, 식별 가능한 보안 위협에 대응이 가능한 보안 요구사항을 정의하는 것을 목표로 표준화가 진행될 예정이다.

Ⅲ. 결 론

본 논문에서는 전자금융 통합인증기술의 국내외 표준을 분석하였고 표준화의 동향을 살펴보았다.

국내외 표준화기구에서 통합인증기술의 표준화가 활발하게 진행되어 프레임워크, 요소 인증기술, 보안 요구사항이 각각 국내외 표준으로 제정되었고 일부는 개발중에 있는 상황이다. 신뢰기관을 활용한 부인방지기술로 통합인증체계를 정립하고, 모바일기기를 활용한 다중요소 인증기술의 표준화로 편리성과 보안성을 향상시킬 것으로 보인다. 또한, 통합인증서비스 프레임워크의 요소기술인 IC칩 기반 인증기술은 전자금융 환경의 보안성을 강화하기 위한 범용 인증기술로 활용할 수 있을 것으로 기대된다. 현재 국내 전자금융에서 사용되고 있는 고유의 OTP 통합인증 기술이 ITU-T 국제표준으로 제정되어 있으며, 이를 기반으로 하는 통합인증 프레임워크의 국내외 표준화를 통해 국제적으로 기술선점이 가능할 것이다.

통합인증기술과 관련한 프레임워크, 요소 인증기술, 보안 요구사항 등의 기술은 국내외에서 활발히 표준화가 이루어지고 있으며, 이러한 표준기술을 통해 인터넷서비스의 보안성을 효과적으로 향상시킬 수 있고, 이를 통해 산업 전반에 대한 활성화의 기반을 마련하였다.

Acknowledgement

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음.

참 고 문 헌

[1] 한국은행, '2013년중 국내 인터넷뱅킹서비스 이용현황', 공보2014-2-2호, 2013년 2월 10일
[2] 트랜드마이크로, '2013년 제3분기 정보보안 보고서', 2013년 11월
[3] 금융보안연구원, '해외 전자금융거래 이용환경 분석 및 시사점 - 인터넷뱅킹 중심-', Vol.2014-01, 2014년 1월
[4] 한국정보통신기술협회, 'IC칩 기반 보안 매체를 활용한 통합형 사용자 인증 서비스 프레임워크', TTAK.KO-12.0192, 2012년 12월
[5] 한국정보통신기술협회, '통합 인증 기반 부인방지 서비스 프레임워크', TTAK.KO-12.0194, 2012년 12월
[6] ITU-T, 'An One time password based non-repudiation framework', ITU-T X.1156, June 2013
[7] 한국정보통신기술협회, '모바일 기기에 적합한 IC칩 기반 인증모듈용 API', TTAK.KO-12.0218, 2013년 12월
[8] 한국정보통신기술협회, 'IC칩 기반 인증 모듈 보안 요구 사항', TTAK.KO-12.0219, 2013년 12월
[9] ITU-T, 'Multi-factor authentication mechanisms based on mobile devices', ITU-T X.sap-8, Jan. 2014.
[10] 한국정보통신기술협회, '모바일 기기를 이용한 다중 요소 인증 메커니즘', TTAK.KO-12.0221, 2013년 12월
[11] 한국정보통신기술협회, '전자거래 인증방법의 보증수준별 요구사항', TTA 2014-014, 2014년 3월
[12] 한국정보통신기술협회, '통합인증서비스를 위한 신뢰기관의 보안 요구사항', TTA 2014-016, 2014년 3월

약 력

정 영 곤

2010년 순천향대학교 정보보호학과 학사
2012년 순천향대학교 정보보호학과 석사
2012년~현재 금융보안연구원 인증기술팀 주임연구원
관심분야: OTP, PKI, 정보보호

김 근 옥

2004년 성균관대학교 전자전기 컴퓨터공학과 석사
2011년~현재 성균관대학교 전자전기 컴퓨터공학과 박사과정
2001년~현재 금융보안연구원 인증기술팀 선임연구원
관심분야: OTP, 암호이론, 정보보호

심 희 원

2000년 홍익대학교 전자계산기학과 석사
2011년 전남대학교 정보보호학과 박사
2006년~현재 금융보안연구원 인증기술팀 팀장
관심분야: PKI, OTP, 네트워크 보안, 암호이론