금보원 2011-01

전자금융 新인증기술 연구보고서

2011. 3

금 융 보 안 연 구 원

* 본 연구보고서에서 검토한 연구내용은 '인증방법 평가위원회'의 평가기준과 무관하며, 순수 연구목적으로 작성되었습니다.
* 본 연구보고서의 내용 중 오류가 발견되었거나, 내용에 대한 의견이 있을 경우 금융보안연구원 인증기술팀(otp_apt@fsa.or.kr)으로 해당 내용을 보내주시기 바랍니다.

머 리 말

2010년 9월말 기준으로 우리나라 은행의 전자금융 이용자 수는 약 6,390만 명(17개 국내은행, 홍콩상하이은행 및 우체국 등록 기준)을 넘어섰으며, 거래 금액 또한 하루 평균 30조원에 육박하는 등 전자금융 이용은 매년 빠른 속도로 증가하고 있습니다. 특히 최근 정보기술의 발달에 힘입어 스마트폰을 비롯한 인터넷 TV 등에 기반을 둔 획기적인 전자금융서비스가 속속 개발됨에 따라 그 편리함으로 인하여 앞으로 전자금융 이용은 더욱 확대될 것으로 전망됩니다.

하지만 전자금융 확대에 따라 해킹공격도 점차 증가되고 공격기법 또한 날로 고도화되고 있어, 이를 대응하기 위해 보안이 강화된 새로운 보안기술의 요구가 증가되고 있습니다. 더욱이 지난 5월 "전자금융거래 인증방법의 안전성 가이드라인"이 확정·발표됨에 따라, 제도적으로도 금융회사가 다양한 인증방법을 자율적으로 선택 및 도입 할 수 있는 길이 열리게 되어, 국내 전자금융환경에 적용 가능하고 보안이 강화된 新인증기술 연구개발이 시급한 사안으로 인지되고 있습니다.

이에 금융보안연구원은 금융회사가 전자금융에 新인증기술을 도입시 검토되어야할 항목 및 방법을 제시한 『전자금융 新인증기술 연구보고서』를 개발하게 되었습니다. 아무쪼록 동 연구보고서가 금융회사의 요구에 부응할 수 있는 자료로 주요하게 활용될 수 있기를 바라며, 끝으로 연구보고서 작성에 직접 참여해 주신 전문가 여러분과 우리원 연구원들에게 깊은 감사를 드립니다.

2011년 3월

금융보안연구원장 곽 창 규

차례

전자금융 新인증기술 연구보고서

그림

표

전자금융 新인증기술 연구보고서

제1장 개 요

제 1 절 검토 배경

현재 인터넷은 일상생활의 일부분이 될 정도로 활성화 되어있으며, 이를 활용한 다양한 서비스가 존재한다. 이중 전자금융은 온라인으로 안전하고 신속하게 계좌이체를 하거나, 금융상품을 구입할 수 있어 많은 이용자에 편의를 제공하는 인터넷을 활용한 가장 대표적인 서비스라 할 수 있다.

인터넷 기반의 전자금융은 비대면 거래라는 특성으로 접속하는 이용자를 올바로 확인할 수 없다면 타인에 의한 부정거래를 막을 수 없게 되어 전자금융 사고에 직결될 수 있다. 또한, 전자금융 이용시 필수적으로 입력되는 개인정보 및 금융거래정보 등의 민감한 정보가 온라인으로 전송되기 때문에 타인에게 노출되지 않도록 올바른 이용자를 확인하는 전자금융 인증기술은 전자금융의 신뢰성을 확보하는 가장 중요한 수단이라 할 수 있다.

국내의 전자금융은 IT 선진기술과 더불어 매우 빠른 속도로 발전하였다. 최근 한국은행 자료[1]에 따르면 인터넷뱅킹 등록 이용자수는 63백만 명이며, 공인인증서도 무려 19백만 명이나 발급받아 사용하고 있다고 밝혔다. 이는 경제활동 인구의 대부분이 전자금융을 이용하고 있다는 것이다. 전자금융이 이렇게 활발하게 이용될 수 있었던 이면에는 이용자가 인터넷을 통한 거래도 안전하다고 믿게 하는 인증기술의 역할이 매우 컸다. 이 덕택에 1999년 말부터 국내에서는 공인인증서로 대표되는 인증기술이 큰 변화 없이 모든 전자거래에서 공통적으로 사용되게 되었다.

하지만, 2005년 최초의 인터넷뱅킹 해킹사고가 발생한 이후부터는 공인인증서와 보안카드 이외에도 추가적인 인증기술을 적용하여 전자금융의 안전성을 높여야 한다는 요구가 늘어나게 되었다. 정부에서는 이에 대한 대책으로 2008년 4월부터 고액의 이체에는 OTP(One Time Password)발생기, HSM(Hardware Security Module), 2채널인증(전화승인 등)의 3가지 기술 중 한 가지를 공인인증서와 함께 사용하도록 하였다[2].

한편, 최근의 전자금융은 2009년 초부터 스마트폰 열풍으로 대변되는 환경적인 변화에 적응하기 위한 역대 최대의 변혁기에 있다고 해도 과언이 아닐 것이다. 과거의 전자금융이 인터넷과 전화 채널에 한정되어 제공되었던 것과는 달리, 앞으로의 전자금융에서는 접근매체의 다양화와 함께 이를 지원하는 채널의 수도 더욱 많아질 것이다. 이에 따라, 차세대 전자금융 인증기술은 스마트폰, IPTV 등의 어떠한 채널에서도 공통적으로 사용이 가능하여야 하며, Active-X, 브라우저, 운영체제(OS) 등의 구현 기술에도 종속되지 않아 금융회사에서 쉽게 도입할 수 있는 적용성을 가져야 한다는 요구가 크게 증가하고 있다.

또한 2010년 5월말 방송통신위원회에서는 '전자금융거래 인증방법의 안전성 가이드라인'을 발표하였다. 이 가이드라인은 기존의 공인인증서의 의무사용 규제가 스마트폰 등 새로운 인터넷 환경에 적용되기 어렵고 사용절차도 복잡해, 다른 보안기술로 대체하여 사용할 수 있도록 규제 완화에 초점이 맞춰져 있다. 이는 한국의 대표적인 인증수단인 공인인증서의 사용을 스마트폰과 같은 새로운 환경에서 강제하지 않고, 다양한 시도를 할 수 있도록 허용한 것으로서 새로운 환경에 신속히 적응하고자 하는 것이다.

본 연구보고서는 전자금융의 관문에서 안전성을 책임지고 있는 인증기술이 새로운 IT 환경에 적응하기 위해 필요한 요건들을 면밀히 검토하고자 작성되었다. 본 연구보고서는 다음과 같이 구성된다. 제1장은 본장으로서 연구보고서의 작성 배경 및 목적을 설명하고 있으며, 제2장에서는 국내에 적용된 전자금융 인증기술의 현황을 분석하였다. 제3장은

스마트폰, IPTV 등 새로운 전자금융 환경에 적응하기 위한 新인증기술의 검토항목 및 검토방법을 제시하고 있으며, 이를 통해 제4장에서는 대표적으로 선정된 5가지 新인증기술에 대한 세부 검토결과를 기술하였다. 제5장은 결론으로 본 연구보고서의 결과를 요약하고 활용방법 등을 제시한다.

제 2 절 新인증기술 검토 목적 및 범위

본 연구보고서는 금융회사가 새로운 인증기술을 도입하고자 하는 경우, 활용 할 수 있는 검토항목 및 방법을 제시하는데 목적이 있다. 또한 대표적인 新인증기술을 선정하여 검토한 결과를 제공함으로서 금융회사에서 실제 해당 기술을 도입하는 경우 참고할 수 있도록 작성되었다.

본 연구보고서의 대상이 되는 인증기술은 다양한 인증기술들 중 전자금융에 적용 가능한 인증기술로 한정한다. 또한, 해외 전자금융에서는 사용되고 있으나 국내에서는 사용되지 않는 인증기술이거나, 차세대 전자금융에 적합하도록 새롭게 개발된 신기술만을 대상으로 한다. 따라서, 본 연구보고서의 전자금융 新인증기술의 범위는 국내에 도입되지 않은 새로운 전자금융 인증기술로 한정한다.

본 연구보고서는 스마트폰, IPTV 등 새로운 전자금융 환경에서 사용될 수 있는 新인증기술에 대한 일반적인 소개 및 사전에 반드시 검토되어야 할 최소한의 검토항목을 제공하고 있다. 하지만, 이러한 新인증기술이 실제 전자금융에 적용되기 위한 법·제도적 요건은 '인증방법 평가위원회'[3]에서 검토되어야 할 사항으로, 본 연구보고서의 검토 범위에서는 제외하도록 한다.

따라서, 금융회사는 새로운 인증기술의 도입시 본 연구보고서에서 제시된 검토항목 및 검토방법으로 해당 기술을 사전에 검토할 수 있으며, 실제 도입시에는 해당 기술의 보안성에 대한 추가적인 평가를 받기 위해 '인증방법 평가위원회'의 심의를 거쳐 전자금융에 적용할 수 있다.

제 3 절 용어정의

- 구동모듈 : 모바일OTP 소프트웨어의 구성 중 OTP 생성과 직접적인 관계가 없는 사용자 인터페이스 프로그램을 의미
- 서비스 도메인키 : Service Domain Key, USIM에 비밀정보 혹은 애플릿을 설치 및 제거를 위해 사용되는 접근제어용 비밀키
- 인증모듈 : 모바일OTP 소프트웨어의 구성 중 OTP가 관리하는 비밀키, 부가정보, PIN 정보 등의 비밀정보에 직접 접근하여 OTP를 생성하는 모듈로서 USIM에서 구동되는 애플릿
- 2채널인증 : 인터넷뱅킹 이용시, 인터넷 망 이외에 다른 채널을 이용하여 거래 인증을 수해하는 기술
- CAP : Chip Authentication Program, EMV에서 제정한 규격을 만족하는 IC Card를 이용하여 인증 및 전자금융에 이용하기 위한 기술규격
- EMV : IC카드 칩의 표준 규격 등을 공동으로 제안한 Europay社, MasterCard社, Visa社를 통틀어 일컫는 말
- HSM : Hardware Security Module, 전자 서명 생성 키 등 비밀정보를 안전하게 저장, 보관할 수 있고 기기 내부에 암호 연산 장치가 있어 전자서명 키 생성 및 서명 생성 등이 가능한 하드웨어 장치
- MAC : Message Authentication Code, 컴퓨터 보안에서 메시지의 내용, 작성자, 발신처 등 속성의 정당성을 검증하기 위하여 메시지와 함께 전송되는 값

- MITM공격 : Man-in-the-middle Attack, 중간자공격이라고 표현됨, 공격자가 통신하는 두 사람 사이에서 몰래 끼어들어 주고받는 메시지를 읽고, 삽입 및 수정을 통해 공격 하는 방법
- OTA : Over The Air, 무선 통신 시스템에서 시스템 등록에 관한 정보를 송수신하기 위한 표준. 휴대전화의 사소한 고장이나 프로그램의 업그레이드를 위함
- OTP : One Time Password, 로그인 또는 통신마다 매번 변경되어 단 한번만 사용 가능한 비밀번호이다. 일반적인 고정 비밀번호는 수집에 의한 재사용 공격에 취약한 반면, OTP는 매번 비밀번호가 변경되어 수집한 비밀번호를 사용할 수 없게 되므로 보안성이 높음
- OTP발생기 : OTP Generator, 일회용 비빌번호를 생성하는 전용 하드웨어 장치 또는 휴대폰 등에 설치되는 소프트웨어 모듈을 의미
- PKI : Public Key Infrastructure, 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 보안 시스템 구조, PKI는 인터넷뱅킹 및 전자상거래와 같이 광범위한 지역에 분산된 사용자의 인증 및 전자서명에 이용됨
- USIM : Universal Subscriber Identity Module, 스마트폰의 소유자를 인증할 목적으로 사용되었으나,. USIM에 다양한 응용 애플릿을 구현 가능하기 때문에 전자상거래, 신용카드, 금융결제 등에 인증수단으로 사용이 가능할 것으로 예상됨

제2장 인증기술 현황

제 1 절 인증기술 정의

인증기술은 원격지에 있는 사용자의 신원확인 기능과 송수신자간 전송되는 거래내역의 무결성을 보장하는 거래인증 기능의 2가지 의미를 모두 내포한다. 특히, 전자금융에서 인증기술은 주로 거래내역의 무결성을 보장하여 부정거래를 방지하기 위해 사용되기도 한다. 부가적으로 사용자 또는 전자금융서버의 전자금융 이용사실에 대한 부인방지기능을 제공하여 전자금융의 신뢰성을 보장하는 기능을 포함할 수 있다.

이러한 인증기술의 특성으로, 現 국내 전자금융에 새로운 인증기술을 도입하기 위한 기술적 요건으로 사용자인증, 전자금융서버의 인증, 거래내역에 대한 무결성 기능, 전자금융 이용사실에 대해 부인방지기능을 제공하여야 하며, 추가적으로 전송구간의 암호화 기능이 제공되어야 한다.

전자금융은 재화의 이동 수단으로 사용되므로, 특히 신뢰성이 최우선시 되어야 한다. 이러한 전자금융의 관문을 지키는 인증기술이야말로 전자금융의 신뢰성을 보장하기 위한 가장 중요한 기술이므로, 금융회사에서는 반드시 높은 중요도로 인증기술의 안전성을 검토하여야 할 것이다.

제 2 절 인증기술 분류

전자금융에 사용할 수 있는 인증기술을 인증팩터(Authentication factor) 관점으로 분류한다면, <표 1>와 같이 '지식 기반'(What you know), '소지 기반' (What you have), '특징 기반(What you are)으로 분류하는 것이 일반적이다.

이밖에도 개인 간의 비밀번호 입력패턴 차이, 전자적인 서명필체 등을 이용하는 인증팩터를 '행동 기반'(What you do)으로 분류하기도 하며, 사용자의 전자금융 이용패턴, 이용위치 등 사용자의 알려진 사실에 기반한 인증팩터를 '알려진 사실 기반'(What known about you)[4]으로 세분화하여 분류하기도 하지만 아직까지는 일부에서만 적용하여 분류하고 있다.

표 1 인증팩터 분류

분 류	내 용	예 시
지식 기반 (What you know)	사용자가 알고 있는 지식 기반	ID/PASSWORD, 사전 등록된 질의응답방식 등
소지 기반 (What you have)	사용자가 소지 하고 있는 인증매체 기반	OTP발생기, HSM, 보안카드, 스마트카드 등
특징 기반 (What you are)	바이오정보를 이용	지문, 홍채, 정맥 등

'지식 기반' 인증팩터를 사용하는 인증기술은 사용자의 기억 능력 제약 및 습관 등으로 인해 안전한 비밀번호 생성 및 변경 등에 어려움이 있어 보안성이 낮지만, 인증기술을 도입하는 기관에서는 관리의 편리성과 구축이 용이하여 널리 사용되고 있고, 더불어 '지식 기반' 인증팩터를 사용한 인증기술의 취약점을 보완하고 보안성을 높이는 방법으로 사람만이 인식 가능한 이미지를 이용하거나 사전에 등록된 질의응답 방식으로 변화하고 있다.

전자금융에서 사용하고 있는 대부분의 인증기술은 '소지 기반' 인증팩터를 이용한 것으로 보안카드, 공인인증서, OTP발생기, HSM은 모두 '소지 기반'의 인증팩터로 분류된다. 특히 하드웨어 장치기반의 OTP발생기 및 HSM은 휴대의 불편한 점이 존재하지만 높은 보안성으로 향후 활용도가 높은 인증팩터 중에 하나이다.

'특징 기반'의 인증팩터는 복제가 어렵고 별도 장비를 휴대할 필요가 없어 향후에 각광받을 인증팩터로 여겨진다. 개인의 바이오 정보를 기반으로 유일성의 특징을 가지고 있지만, 유일한 바이오정보의 노출에 대한 사용자의 부정적 인식과 상대적으로 높은 적용비용 등의 문제로 아직은 많이 활용되고 있지 않다.

단일팩터(Single-Factor)가 가지는 취약성을 보완하고 보안성을 높이기 위해서 다수의 인증팩터를 결합한 멀티팩터(Multi-Factor) 인증기술을 사용하기도 한다. PIN으로 활성화되거나 비밀번호 등과 동시에 사용되는 OTP발생기와 HSM은 '지식 기반' 과 '소지 기반의 인증팩터를 이용한 멀티팩터 인증기술의 대표적인 사례이다.

제 3 절 국내 전자금융 인증기술 적용 현황

국내 전자금융 현황을 살펴보면 2008년 4월 발표된 보안등급별 이체한도 차등화 정책에 따라 전자금융거래의 안전성 강화를 위하여 인터넷뱅킹이나 텔레뱅킹 이용 시 거래수단별로 보안등급을 부여하고, 부여된 보안등급에 따라 이체한도를 적용하고 있다.

보안등급은 <표 2>와 같이 총 3개의 등급으로 분류되며 공인인증서와 일회용 비밀번호(보안카드 포함)를 사용해야 하며, 조합되는 인증수단에 따라 등급을 구분하고 있다. 보안 1등급으로 OTP발생기, HSM, 2채널 인증이 사용되고, 2등급으로는 휴대폰 SMS(거래내역통보), 그리고 보안카드는 3등급으로 분류된다.

표 2 등급별 보안매체수단

거래이용수단	보안등급
OTP발생기 + 공인인증서	1 등 급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 공인인증서 + 2 channel 인증	
보안카드 + 공인인증서 + 휴대폰 SMS(거래내역통보)	2 등 급
보안카드 + 공인인증서	3 등 급

만약 공인인증서와 보안카드만 사용할 경우는 <표 3>과 같이 1등급에 비해 1회 이체한도가 1억에서 1,000만원으로, 1일 이체한도는 5억에서 5,000만원으로 줄어드는 등 1등급 보안매체를 이용하지 않으면 인터넷

뱅킹의 이체한도는 최대 1/10까지 줄어들게 된다.

기업, 법인의 경우에는 1등급 보안매체를 사용해야 하는 대상으로 분류되어 반드시 OTP 등을 사용해야 한다. 개인은 보안 2·3등급의 보안매체를 사용해도 되지만 이체한도와 보안성이 떨어지게 된다.

표 3 보안등급별 이체한도 (단위 : 억원)

구 분			보안등급		
			1등급	2등급	3등급
텔레뱅킹	개인	1회	0.5	0.2	0.1
		1일	2.5	1	0.5
	법인	1회	1	0.2	0.1
		1일	5	1	0.5
인터넷뱅킹	**개인**	**1회**	**1**	**0.5**	**0.1**
		1일	**5**	**2.5**	**0.5**
	법인	**1회**	**10**		
		1일	**50**		

1. 공인인증서

공인인증서는 전자금융 거래시 거래 당사자인 사용자의 신원확인 기능, 거래 내역에 대한 위·변조 방지, 거래사실의 부인 방지 등의 목적으로 신뢰된 공인인증기관이 발행하는 전자적 정보로서, 일종의 전자금융

거래용 인감증명서이다.

전자금융감독규정 제3장 7조에 따라 모든 전자금융거래에 있어서 공인인증서의 사용은 필수적이다. 공인인증서는 가입자의 개인키의 사용용도, 전자서명 검증키, 일련번호, 소유자이름, 유효기간 등의 내용을 포함하고, 공인인증기관에서 포함된 내용을 보증하는 전자서명 값으로 구성된다. 이로써 사용자가 자신의 개인키로 서명한 값은 해당 사용자의 공인인증서를 통해 검증이 가능하며, 전자서명 생성자의 신원 확인 및 거래에 대한 인증을 제공한다.

전자금융거래법 등으로 전자금융에 의무적으로 사용되고 있는 공인인증서의 사용자 수는 국내 경제활동 인구의 90%이상이며, 2010년 말 2,371만 건의 인증서가 발급되어 사용 중에 있다. 전자금융뿐만 아니라 사회 전반에 걸쳐 공인인증서가 사용될 만큼 국가차원의 공인인증 인프라를 구축한 사례는 전세계적으로 우리나라가 유일하다. 하지만 공인인증서는 웹호환성 부족 및 개인 키 관리 문제 등 해결해야 할 문제점도 안고 있어 개선이 필요하다.[5]

국내 전자금융에서 공인인증서의 적용현황은 굳이 조사할 필요가 없을 정도로, 모든 금융회사에서 사용할 만큼 일반화되어 있다.

2. OTP발생기

OTP는 인터넷, 휴대폰, 전화 등을 다양한 매체를 이용하여 은행, 증권, 선물사의 전자금융 거래 시에 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 비밀번호이다.

보안카드의 경우 35개 이내의 비밀번호가 반복적으로 사용되므로 재사용

할 수 있지만, OTP는 일회용비밀번호로써 재사용이 불가능하고 생성된 OTP를 통해서 사용자의 비밀정보를 유추할 수 없다. OTP의 경우 <그림 1>에서 보는바와 같이 생성되는 값은 의미 없는 숫자로 구성되며, 생성되는 숫자 패턴 또한 100만개 이상의 임의 숫자를 조합하여 생성하는 특성이 있어서 다음에 생성할 OTP를 유추하는 것은 수학적으로 불가능하고, 오프라인 추측공격 및 사전공격에도 안전하다.

그림 1 OTP발생기

국내 전자금융의 OTP 적용현황 조사결과, 2010년 12월 기준 총 450만개의 OTP발생기가 발급되어 사용되고 있으며, 전자금융을 제공하고 있는 19개 은행, 37개 증권회사에서 모두 OTP를 사용하고 있다. 또한, 상호저축은행, 신용협동조합, 새마을 금고, 산림조합, 금호종합금융, 외환선물의 6개 기타 금융회사에서도 OTP를 사용하고 있다. 다만, 카드사 및 보험사에서는 아직까지 OTP를 사용하고 있지 않은 것으로 조사되었다.

3. 보안카드

보안카드는 35개 이내의 난수가 적혀진 카드로, 전자금융 거래시 사용자가 카드에 인쇄된 번호를 직접 입력하고, 응답번호와 일치여부를 판단하여 전자금융거래를 수행한다.

현재 모든 은행과 대부분의 증권사가 전자금융거래를 위해 사용하고

있으며 인증을 위해 사용된다는 점은 같지만 안전카드, 시크릿카드 등 명칭이 각기 다르다.

그림 2 보안카드 사용 예

현재 보안카드는 <그림 2>와 같이 비밀번호 2자리씩 분할하여 입력하는 방식으로 사용되고 있으며, 비밀번호개수는 약 35개로 금융회사에 따라 다르다. 각 금융회사에서 정하는 일정횟수 이상(3~10회) 오류 시 사용제한이 되므로 해당금융회사를 방문하여 사용제한 해제를 해야 한다.

국내 전자금융의 보안카드 적용현황 조사결과, 국내 모든 은행에서 사용하고 있으며, 대부분의 증권사 및 일부 보험회사에서도 보안카드를 사용하고 있는 것으로 조사되었다. 현 전자금융감독규정에 의해 계좌이체의 경우 일회용비밀번호(보안카드 포함)가 필수적으로 사용되어야 하지만, 지정 계좌(본인명의)로의 이체에는 보안카드를 사용하지 않아도 되므로, 지점수가 부족하고 온라인 업무를 위주로 하는 증권사 등에서는 보안카드를 사용하지 않는 것으로 조사되었다.

4. HSM(Hardware Security Module)

HSM은 전자서명 생성키 등 비밀정보를 안전하게 저장·보관 및 키 생성, 전자서명 생성 등이 기기 내부에서 처리되도록 구현된 스마트 칩

을 내장한 하드웨어 모듈로 휴대가 가능한 인증서 보안기술이다.

HSM은 <그림 3>과 같이 일반 USB 메모리스틱처럼 PC의 USB슬롯에 연결하여 사용한다. 연산장치와 메모리 등이 포함된 스마트카드 칩을 탑재해 전자서명과 암호화 등 모든 프로세스가 매체 내부에서 이루어지기 때문에 PC에 설치된 해킹 프로그램이나 악성코드를 통해서 HSM 내부에 저장된 비밀정보에 접근할 수 없다. HSM 내부에서 생성되어 안전한 메모리 공간에 저장된 전자서명키는 다른 매체로의 복사나 이동이 금지되어 있어, 전자서명키의 외부 유출을 원칙적으로 차단한다.

그림 3 HSM 예

국내 전자금융의 HSM 적용현황 조사결과, 현재 우리은행 외 5개의 은행에서 HSM을 발급하여 사용하고 있는 것으로 조사되었다. HSM은 OTP와 같은 1등급 보안매체이지만 OTP에 비해 도입된 금융회사 수가 적으며, 사용빈도가 낮다. 해당 조사에서는 1등급 매체로 사용되는 HSM만을 대상으로 하였으며, 이미 PC 등에 발급된 공인인증서를 단순히 저장하여 사용하는 경우는 1등급 매체로 인정되지 않아 조사에서 제외하였다.

5. 2채널인증

OTP발생기, HSM방식 공인인증서와 같이 1등급 보안매체로 분류되는 2채널인증은 전자금융거래 채널 이외에 거래승인을 위한 채널을 분리하여 이용하는 기술이다.

2채널인증의 대표적인 서비스인 전화승인서비스의 경우, 인터넷뱅킹을 통한 자금이체 시 사전에 등록된 전화번호로 사용자가 이체여부를 최종 승인한다.

그림 4 전화승인 서비스 과정

2채널인증의 사용절차는 <그림 4>와 같이 전자금융이용자가 인터넷뱅킹화면에서 ① 금융회사에 거래를 수행하고 ② 금융회사가 인증서버에 전화승인을 요청하면 인증서버는 사용자가 지정한 전화번호로 ③ 전화승인 ARS를 통해 사용자와 연결을 시도한다.

이용자는 연결된 별도매체(휴대폰, 전화, FAX 등)에 ④ 이체승인 번호를 입력하게 되면 ⑤ 이체승인번호 검증 여부에 따라 ⑥ 이체완료/보류/취소 등의 거래를 처리한다. 마지막으로 사용자는 이체결과조회화면에서 전화승인 및 이체결과를 확인하고 서비스절차를 마친다.

국내 전자금융의 2채널인증 적용현황 조사결과, 현재 3개의 은행에서 전화승인서비스를 제공하고 있는 것으로 조사되었다.

6. 휴대폰 SMS(거래내역통보)

휴대폰 SMS는 인터넷뱅킹, 텔레뱅킹 등의 전자금융 서비스를 이용한

자금이체내역을 휴대폰으로 통지하는 서비스로 전자금융보안 2등급 거래 이용수단이다. 사용자의 주요거래 또는 중요통지사항을 사후에 실시간으로 알려주는 방식이다.

<그림 5>와 같이 전자금융이용자가 ① 금융거래 승인 요청을 하고 ② 거래가 승인이 되어 완료되면 즉시 거래 결과가 사용자가 사전에 등록한 휴대폰으로 ③ 거래내역이 통지된다.

그림5 휴대폰 SMS(거래내역통지) 과정

국내 전자금융의 휴대폰 SMS 적용현황 조사결과, 21개의 금융회사에서 휴대폰 SMS 서비스를 제공하고 있으며 이용자 수는 많지 않은 것으로 조사되었다. 휴대폰 SMS는 전자금융감독규정의 2등급 매체로 인정된다. 하지만 일부 금융회사에서는 2등급 이체한도를 운영하지 않고, 2등급에 해당하는 이체한도는 1등급 매체를 통해서만 이체할 수 있도록 한다는 의미로 해석된다.

7. 바이오인증

바이오정보 인증과 관련해 가장 쉽게 접할 수 있는 것은 지문인식기술이다. 지문인식기술은 인터넷뱅킹 접속 시 또는 자금 이체 시 지문정보를 이용하여 인증을 수행하며, 복제 및 해킹 위험이 적다.

우리은행에서 도입한 지문인식기술은 지문정보 분석 알고리즘에 의해 사용자의 고유한 지문정보 템플릿을 생성한다. 지문정보는 복제가 불가능하기 때문에 타인이 지문을 복사해 사용할 수 없으며, 사용자 본인의 지문을 입력함으로서 안전한 사용자 인증을 수행한다. 특히 인터넷뱅킹 접속시 ID와 비밀번호, 자금이체시 필요한 보안카드나 인증서 비밀번호 대신 사용자의 지문정보를 입력하는 것으로 인터넷뱅킹을 이용할 수 있다. 바이오인증은 바이오 인식기기의 보급 및 사용자의 인식 등의 문제로 거의 사용되고 있지 않다.

국내 전자금융의 바이오인증 적용현황 조사결과, 우리은행이 바이오인증을 유일하게 적용하고 있는 것으로 조사되었다.

8. 기타 보안기술

현재 전자금융에 급증하는 위협들 중 하나는 MITM 공격이다. MITM 공격에 대응하기 위해서는 금융서버에 대한 인증이 제공되어야만 한다. 이를 지원하기위한 보안기술로는 서버인증서를 통한 SSL기술이 있다. 하지만 기존 SSL기술에는 몇 가지 단점이 있어, 이를 보완하고 기능을 확장한 EV-SSL기술이 등장하였다. EV-SSL기술의 가장 큰 특징은 접속된 웹사이트가 보안인증이 되어있는 사실을 한눈에 알아볼 수 있도록 사용자 인터페이스가 강화되었다는 것이다.

현재 HSBC은행의 인터넷뱅킹과 우리은행, 국민은행의 오픈뱅킹 서비스에서 EV-SSL 기술을 사용하고 있으며, EV-SSL 기술이 적용되어있는 사이트에 접속하게 되면 웹브라우저의 주소창이 초록색으로 바뀌고 주소창 옆에 접속한 금융회사의 이름과 인증기관이 나타난다.

<그림 6>과 같이 ① 녹색 주소창을 통해 접속한 금융회사임을 확인할 수 있고, ② 우측 자물쇠로 SSL 암호화통신을 한다는 사실을 확인할 수 있다.

그림 6 EV-SSL 인증서를 이용한 서버인증 화면

우측 자물쇠를 클릭하면 <그림 7>과 같이 사이트를 운영하는 회사명, 주소 등을 ③ EV-SSL의 인증서를 통하여 사용자들이 접속한 사이트의 정보를 확인할 수 있어, 쉽게 진위여부를 확인할 수 있다.

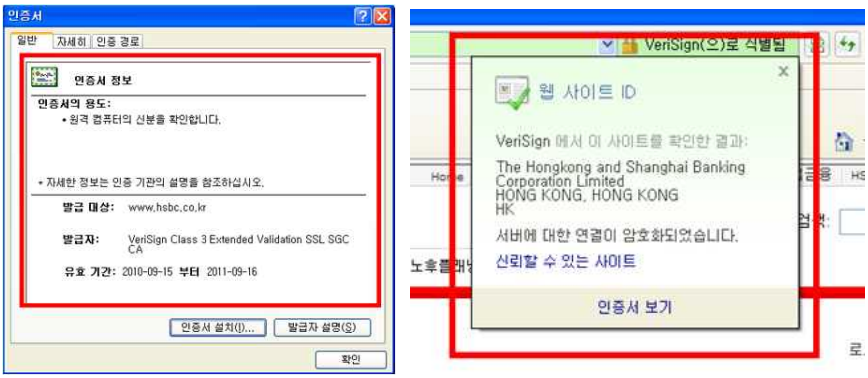

그림 7 서버 인증서 정보 확인 화면

제3장 新인증기술 검토

제 1 절 新인증기술 검토항목 및 대상

본 연구보고서에서 검토되는 新인증기술은 전자금융에 적용되기 위해 필수적으로 검토되어야 할 다음의 3가지 항목으로 검토된다.

첫째, 검토대상이 되는 인증기술이 스마트폰, IPTV 등 새로운 전자금융환경에 적합한 인증기술인지 여부를 검토한다. 즉, 전자금융 환경이 인터넷에 국한되어 있어, PC 등에서만 한정되어 사용되는 인증기술 보다는 스마트폰, 스마트패드, IPTV, VoIP, ATM, 개인금융 단말기 등의 다양한 채널에서 공통적으로 사용될 수 있는 적용성을 가져야 한다. 특히, 적용성은 iPhone, Android 기반 스마트폰 등 모바일 사용자의 증가 및 Mac, Linux 등의 다양한 운영체제와 플랫폼을 이용하는 사용자가 점점 증가하는 현 시점에서, 해당 사용자들이 전자금융을 이용할 수 있는 통로를 제공하기 위한 중요한 요건이 된다.

둘째, 검토되는 인증기술이 휴대 및 이용이 간편하고, 언제 어디서든지 이용할 수 있는 인증기술인지 여부를 검토한다. 편의성으로 대표되는 이러한 특성은 전자금융 인증기술을 이용하는 사용자의 가장 중요한 선택항목이 된다. 분명 전자금융 인증기술은 해킹사고를 방지하기위한 목적으로 도입되지만, 사용자가 이용상의 불편으로 해당 기술의 사용을 꺼려한다면 도입의 효과가 크게 감소될 것이다.

셋째, 검토되는 인증기술이 지속적으로 발전하는 해킹기술에 대응하여 부정거래를 방지하는데 효과적인지 검토되어야 한다. 인증기술의 보안성을 검토하는 방법은 매우 다양하지만 인증, 무결성, 암호화, 부인방지 등의 보안기능들이 제공되는지 확인하는 방법이 일반적이다. ‘인증방법

평가위원회'에서 새로운 인증기술의 보안성을 평가하는 기술적 요건 역시, 이용자 인증, 정보처리시스템 인증, 통신채널 암호화, 거래내역의 무결성, 거래사실의 부인방지의 5가지를 평가하는 방법을 적용하고 있다. 본 연구보고서에서는 보안성을 검토하는 방법으로 기술적 요건을 검토하기보다는, 실제 해킹에 사용되는 공격기술에 대응하여 부정거래 방지에 효과적인지에 대한 검토를 한다.

금융보안연구원에서 운영하는 '新인증기술 전문가 그룹'에서는 다양한 인증기술 중 이러한 3가지 검토항목으로 검토될 대표적인 5가지 新인증기술을 선정하여, 해당 전문가 그룹에서 협의된 검토방법에 의해 세부사항을 검토하기로 하였다. 선정된 5가지 新인증기술은 국내에 도입되지 않은 새로운 전자금융 인증기술로서 첫째, 새로운 전자금융 환경에 적용 가능한 적용성과 둘째, 휴대 및 이용이 간편한 편의성, 셋째, 부정거래 방지에 효과적인 보안성의 3가지 검토항목을 만족할 수 있는 대상 중에 선정되었다.

아래의 선정된 5가지 新인증기술은 제2절에서 설명되는 新인증기술 검토방법에 따라 제4장에서 세부 검토결과를 제시한다.

- **USIM 기반 모바일 OTP**: USIM에 OTP생성키 등을 보관하여, 휴대폰, 스마트폰 등을 이용하여 안전하게 OTP를 생성하는 기술
- **거래연동 인증기술**: 계좌번호, 이체금액 등의 거래정보와 직접 연동된 인증정보를 이용하여 안전하게 인증하는 기술
- **이상거래 탐지기술** : 사용자의 정상적인 전자금융 이용 패턴을 분석하여 이상거래 여부를 탐지하는 기술
- **PKI 서명센터** : 공인인증서, 개인키 등을 중앙 센터에 안전하게 보관하고, 사용자가 2팩터 인증을 통해, 서명 요청시 서명 값만을 제공하는 부인방지 기술
- **바이오정보 인증기술** : 지문, 홍채, 정맥 등의 바이오정보를 이용하여 사용자를 인증하는 기술

제 2 절 新인증기술 검토방법

1. 공통적인 검토방법

본 연구보고서에서는 新인증기술을 세부적으로 검토하기 위한 방법에 대해 설명하기 위해, 적용성, 편의성, 보안성의 3가지 검토항목에 따라 검토방법에 대한 세부사항, 검토 우선순위, 검토결과를 각각 제공한다.

검토방법의 세부사항은 검토방법을 세부적으로 설명하는 예시로 활용할 수 있다.

검토방법의 검토 우선순위는 금융회사의 담당자가 해당 기술을 전자금융에 도입하기 위해 세부사항을 검토하는 경우 반드시 검토되어야 할지의 여부를 판단하는 지표로 사용할 수 있다.

검토 우선순위가 높은 경우에는 반드시 검토 세부사항을 만족하는 경우에만 도입 여부를 검토하도록 한다. 검토 우선순위가 보통의 경우에는 검토 세부사항을 만족하는 것을 원칙으로 하되, 해당 금융회사에서 특정한 검토 사유가 있는 경우에는 만족하지 않아도 도입 여부를 검토할 수 있다. 낮은 검토 우선순위의 경우에는 금융회사의 담당자에 의해 선택적으로 세부사항을 검토할 수 있도록 한다. 반드시 검토되어야 하는 높은 검토 우선순위의 세부사항부터 선택적으로 검토되어도 되는 낮은 검토 우선순위의 세부사항까지 모두 만족하는 경우에는 최적의 인증기술로 분류될 수 있어 도입효과가 큰 인증기술로 분석된다.

도입하고자 하는 新인증기술의 각 항목별 검토결과는 검토 세부사항과 검토 우선순위를 고려하여 결정한다. 즉, 검토 우선순위에 대해 차례로

비중을 두고(예, 높음3, 보통2, 낮음1), 세부사항의 만족여부를 산정(예, 우수3, 보통2, 미흡1)하여 평균 검토수치가 1~1.6은 미흡, 1.7~2.4는 보통, 2.5~3은 우수로 종합검토 할 수 있다.

2. 적용성 검토방법

新인증기술의 적용성을 검토하기 위해서 다음 <표 5>와 같은 4가지 검토방법을 제시한다.

표 5 적용성 검토방법

검토방법	세부사항	검토 우선순위
적용 가능성	멀티 OS, 멀티 플랫폼 지원 여부	높음
적용 비용	도입시 소요되는 비용 및 시간	보통
기술 중립성	표준 기술의 사용	보통
기존 인프라 활용성	기존 도입된 시설 및 장비를 활용하여 변경 최소화	낮음

첫째, 적용 가능성은 새로운 전자금융 환경에 적용이 용이한지를 검토한다. 스마트폰, IPTV 등 새로운 전자금융 환경에 적용이 가능하기 위해서는 멀티 OS, 멀티 플랫폼에서 유연하게 동작하여야 하며, 향후 전자금융 환경이 어떻게 변화하더라도 적용될 수 있어야 한다. 따라서 적용 가능성은 높은 검토 우선순위를 가지고 검토되어야 하며, 적용 가능성이 낮은 경우에는 금융회사의 도입 여부에 대해 신중히 검토하여야 할 것이다.

둘째, 적용 비용은 금융회사에서 해당 新인증기술의 도입시 소요되는 비용 및 시간이 수용 가능한지 여부를 검토하는 것이다. 적용 비용이 높은 경우에는 도입을 결정하는 금융회사에 많은 부담이 발생하게 된다. 단, 높은 적용 비용에도 불구하고 제도적, 정책적 결정 또는 다른 부가적인

효과 등에 의해 도입 여부가 검토될 수 있으므로 검토 우선순위는 보통 수준이다.

셋째, 기술 중립성은 도입하고자 하는 新인증기술이 표준 기술을 사용하고 있는지 여부를 판단하는 것이다. 기술 중립성이 낮은 경우에는 도입 이후에, 점차적으로 사용되지 않아 소멸될 가능성이 있으며, 타 기술과 호환되지 않아 상호 운용성이 떨어지게 된다. 따라서 가급적 기술 중립성을 만족하여야 하지만, 새롭게 개발된 기술로서 관련 표준이 없거나 특허 등에 의해 보호되는 기술의 경우에는 예외적로 할 수 있으므로 검토 우선순위는 보통으로 한다.

넷째, 기존 인프라의 활용성은 기존에 이미 도입된 시설, 장비, 인력 등을 그대로 활용하여 변경을 최소화할 수 있는지 여부를 판단하는 것이다. 기존 인프라를 그대로 활용하는 경우에는 도입에 소요되는 시간 및 비용을 획기적으로 줄일 수 있을 뿐 아니라, 기존에 안정적으로 운용되는 인프라에 부담을 주지 않아 적용에 따른 부작용이 최소화 될 수 있어 가용성(Availability)을 유지할 수 있다. 다만, 新인증기술은 대부분 새로운 환경에 적합하도록 새롭게 개발된 기술이므로, 기존 인프라의 활용성을 유지하는 것이 어려울 수 있어 검토 우선순위는 낮음으로 한다.

3. 편의성 검토방법

사용자의 대표적인 선택항목이 되는 新인증기술의 편의성을 검토하기 위해서 다음 <표 6>와 같은 5가지 검토방법을 제시한다. 편의성의 경우에는 보안성과 상충관계(Trade-off)로써 보안성을 높이면 편의성이 저하될 수 있다. 금융회사에서는 전자금융에 인증기술 도입시 이점을 고려하여야 하며, 특히 관리 및 교육 편의성의 경우에는 보안사고와 직결되어 문제 발생시 위험도가 매우 높기 때문에 주의를 요한다.

표 6 편의성 검토방법

검토방법	세부사항	검토 우선순위
소지 편의성	인증매체의 휴대성, 소지 가능여부	높음
사용 편의성	사용 및 입력이 직관적인지 여부	보통
발급 편의성	발급, 등록, 교체 등이 편리한지 여부	낮음
관리 편의성	도난, 노출 등에 대응 가능여부	보통
교육 편의성	교육이 부족한 경우 사고 개연성 등	낮음

첫째, 소지 편의성은 전자금융 인증기술을 사용하기 위해 별도의 인증매체가 필요한 경우, 해당 인증매체의 휴대성 및 소지 가능여부를 판단하는 것이다. 최근의 新인증기술이 대부분 멀티팩터 기반의 인증을 제공하므로, '지식 기반'(What you know) 보다는 '소지 기반'(What you have) 또는 '특성 기반'(What you are)의 특징을 가지는 경우가 많다. 따라서 인증매체가 특정 장소에 고정되어 소지할 수 없거나, 휴대하기 불편한 경우에는 이동성이 떨어지게 되므로 새로운 전자금융 환경에 적합하지 않다. 따라서 높은 검토 우선순위로써 반드시 검토해야 한다.

둘째, 사용 편의성은 전자금융의 인증시에 사용자가 수행해야 하는 방법 또는 입력하는 절차 등이 복잡한지 여부를 판단하는 것이다. 新인증기술은 직관적으로 사용방법을 알 수 있어 별도의 교육 또는 설명서 없이 편리하게 사용되어야 하며, 과다한 정보의 입력 등을 요구하지 않아야 한다. 사용 편의성이 떨어지는 인증수단은 대부분 이용자의 외면을 받게 되지만, 높은 보안성이 제공되는 인증기술의 경우에는 사용의 불편함을 감수하더라도 높은 금액의 이체시 등에 한정하여 사용될 수 있으므로 검토 우선순위가 보통 수준이다.

셋째, 관리 편의성은 해당 인증기술의 주요정보 또는 인증매체가 도난되거나, 타인에게 노출되었을 경우 신속하게 대응이 가능한지 여부를 판단하는 것이다. 특정 인증기술의 경우에는 일단 인증정보가 노출된 경우에는

영구적으로 복구가 불가능할 수 있으며, 노출된 인증정보가 쉽게 복제되는 경우에는 해당 인증정보의 위치가 여러 곳에 위치하여 관리가 어려울 수 있다. 新인증기술은 가급적 관리가 쉬워야 하지만, 관리상의 문제를 보완하는 수단이 있는 경우에는 도입이 가능할 것으로 판단되어 검토 우선순위는 보통 수준이다.

넷째, 발급 편의성은 해당 인증기술을 설치하거나, 발급, 등록, 교체 등의 필요한 경우 편리하게 수행할 수 있는지 판단하는 것이다. 발급 편의성은 사용 편의성과 유사하지만, 인증기술의 초기 사용 시에만 수행된다는 차별성이 있다. 더욱이 보안성을 위해 대면발급 등을 기본으로 수행해야 하는 금융회사의 경우, 발급 편의성을 유지하기는 어려운 것이 사실이다. 따라서, 발급 편의성을 향상시키기 위한 보완수단 또는 기술의 융통성이 있는 지 검토하여야 하며, 낮음의 검토 우선순위이다.

다섯째, 교육 편의성은 해당 인증기술을 이용하는 사용자에 대해 별도의 보안교육을 수행하지 않는 경우 보안사고의 개연성이 높아지는지 판단하는 것이다. 예를 들어, TLS/SSL의 경우에는 사용자가 브라우저에서 직접 접속한 서버의 URL을 확인해야만 안전하다는 제약이 있다. 즉, 사용자의 부주의를 미연에 방지하여, 교육이 되지 않은 경우라도 안전하다는 신뢰성을 줄 수 있어야 한다. 그러나, 사용자의 인식(User Awareness)의 개선은 대부분의 인증기술이 가지는 제약으로 낮음의 검토 우선순위이다.

4. 보안성 검토방법

인증기술의 보안성을 검토하는 방법론은 수년간 고전적인 Dolev- Yao 위험모델[6]이 사용되어져 왔다. 해당 방법론은 인증기술들이 클라이언트와 서버 사이의 통신 채널 사이에 대한 충분한 안전성을 제공할 수 있도록 하는 이론적 근거를 제공하고 있다. 그러나, 해킹기술이 발전함에 따라 해커들은 수학적으로 안전성이 보장된 클라이언트와 서버 사이의 통신채널에 침입하기 보다는 채널의 마지막 부분(end-point)에 관심을 가지게 된다.

즉, 서버와 클라이언트에 직접 침입하여 채널을 변조하지 않고도 해킹이 가능한 하는 서버와 클라이언트의 취약성을 직접 이용하게 되었다. 하지만, 금융회사가 관리하는 전자금융 서버는 해커가 침입하는 것이 거의 불가능하도록 안전하게 관리되고 있으므로, 전자금융 서버에 침입하기 보다는 사용자의 PC 또는 단말기를 공격하는 해킹기술이 발전하게 되었다. 이에 따라, 현재의 전자금융 해킹사고에는 악성코드, 키보드 해킹, 피싱(Phishing) 등이 사용자 채널을 직접 공격하는 방법이 이용되고 있다. 이러한 공격기법은 대부분 고전적인 검토 방법론으로는 검토될 수 없어, 본 연구보고서 에서는 새로운 방법론으로 新인증기술의 보안성을 검토하고자 한다.

新인증기술의 보안성을 검토하기 위해서는 전자금융에 발생할 수 있는 공격에 대한 분류가 선행되어야 한다. 2006년 IEEE에서는 전자금융에 적합한 새로운 위험모델을 발표하였다[7]. 이 논문에 따르면 최신의 전자금융 공격기술은 다음과 같이 3가지 종류로 분류될 수 있다.

- **오프라인 공격**(Offline credential stealing attacks): 악성코드를 이용하여 사용자의 PC를 공격하거나, 사용자를 속여 비밀정보를 훔치고, 이를 해커의 PC로 수집하여 추후 공격하는 기법 (예: 키보드 해킹, Phishing, Parming)
- **온라인 공격**(Online channel-breaking attacks): 악성코드(proxy, Web washer 등)를 이용하여 사용자와 서버의 통신채널 사이에 침입하여 온라인으로 거래정보를 변조하는 기법 (예: MITM)
- **거래조작 공격**(Contents manipulation attacks): 사용자 PC를 완벽히 장악하여, 인증정보를 해커가 원하는 값으로 생성하는 공격기법 (예: MITB, 메모리 해킹)

이러한 배경으로 본 연구보고서에서는 新인증기술이 새로운 환경에서 발생 가능한 공격에 실제로 대응하여 부정거래를 차단할 수 있는지 검토하고자 한다. 이에 따라, 新인증기술의 보안성을 검토하기 위해서 다음 <표 7>과 같은 3가지 검토방법을 제시한다.

다만 보안성의 경우에는 해킹공격으로 인해 시스템에 문제 발생시 상당히 치명적이기 때문에 보안성의 검토방법에 대한 검토 우선순위를 가름하기 어려워 검토 우선순위를 설정하지 않았다.

표 7 보안성 검토방법

검토방법	세부사항	검토 우선순위
오프라인 공격대응	Phishing, Pharming 등 대응가능	-
온라인 공격대응	MITM 등 대응가능	-
거래조작 공격대응	MITB, 메모리 조작공격 등 대응가능	-

첫째, 해당 인증기술이 오프라인 공격에 대응 가능한지 여부를 검토한다. 악성코드를 이용한 오프라인 공격은 최근 가장 빈번하게 발생하는 대표적인 전자금융 공격기법이다. 오프라인 공격을 막기 위해서는 新인증기술이 OTP발생기, HSM 등과 같은 소지 기반 인증기술과 함께 사용될 수 있어야 하며, 지원되는 보안 프로토콜에서는 한번 사용된 인증정보가 재사용되지 않도록 하여야 한다. 새로운 환경의 전자금융은 시간과 장소에 제약 없이 사용될 수 있으므로 해킹으로 인한 인증정보의 수집은 반드시 방지되어야 한다.

둘째, 해당 인증기술이 온라인 공격에 대응할 수 있는지 여부를 검토한다. 대표적인 온라인 공격인 MITM(Man In The Middle) 공격은 사용자가 전자금융서버를 가장한 해킹사이트에 접속하여 거래정보를 입력하는 경우, 해커가 이를 이용하여 전자금융서버에 온라인으로 접속하고 거래를 중계하는 기법이다. 국내에서는 아직 생소하지만, 해외의 경우에는 Phishing, Pharming 등과 혼합된 공격기법이 많이 알려져 있다. MITM 공격에 대한 대응기술은 사용자 인증기술 보다는 서버 인증기술로 방어하는 것이 일반적이며, NIST에서는 MITM 공격에 대응 가능한 기술로 2팩터 인증을 제공하는 OTP발생기 또는 HSM 중 하나를 SSL/TLS와 동시에 사용하도록 권고하고 있다[8]. 최근 해외에서는 MITM 공격이 점점 증가하는 추세이므로 新인증기술은 온라인 공격에 대응이 가능하여야 할 것이다.

하지만, 온라인 공격을 실현하기 위해서는 높은 수준의 해킹기술이 구현되어야 하며, Phishing 등의 다양한 해킹기술과 복합적으로 동원되어야 가능하다.

셋째, 해당 인증기술이 거래조작 공격에 대응할 수 있는지 여부를 검토한다. 거래조작 공격은 앞서 설명된 2가지 공격기법 보다 한 차원 높은 공격기술로 고도의 해킹 기술을 이용해야 하며, 구현기술이 매우 어렵지만 일단, 전자금융 해킹사고에 적용되는 경우 가장 위험한 해킹기술로 분류될 수 있다. 그 이유는 해킹이 이루어지는 동안에도 이용자는 전자금융 거래가 정상적으로 처리되는 것으로 보여 해킹 사실을 전혀 인지할 수 없기 때문이다. 거래조작 공격에 대응하는 기술로는 EMV 표준인 CAP 기술[9]과 IBM의 zTIC[10]이 대표적이다. 新인증기술은 앞으로 발생 가능한 모든 종류의 부정거래를 원천적으로 차단하도록 충분한 보안성을 제공하여야 한다.

제4장 新인증기술 검토결과

제 1 절 USIM OTP 인증기술

1. 기술소개

가. 배경

USIM이 탑재된 스마트폰을 이용하는 사용자 수가 급속하게 증가하고 있고 앞으로도 증가가 예상되고 있어 향후 스마트폰은 현대인의 필수품으로 자리 잡을 것이다. 또한 스마트폰에 탑재되는 USIM은 IC칩과 동일한 물리적 보안성을 제공할 수 있고 다양한 응용 애플릿을 탑재가 가능하여, 다양한 인증기술을 USIM에 구현이 가능하다. 이를 활용하여 기존 인증매체를 대신하여 USIM을 활용하려는 시도가 증가하고 있다. USIM OTP 인증기술도 USIM 내에서 안전하게 OTP를 생성하여 인증에 이용하는 기술로 USIM을 활용한 인증기술이라 할 수 있다.

나. 기술 개요

H/W OTP와 동등한 수준의 보안성을 제공하고 OTP발생기 휴대에 따른 불편함을 해소하여 사용자 편의성을 높인 USIM OTP 인증기술은 OTP를 생성하는 인증모듈과 OTP 사용자 인터페이스로 이루어진 구동모듈로 구성된다.

이 중 인증모듈은 높은 보안성을 제공하기 위해 USIM 내부에서 구동

되어 OTP를 생성한다. USIM OTP 인증기술은 S/W 방식으로 발급 및 인증 시에 모듈을 다운로드 받아 설치되는 특징을 갖는다.

본 연구보고서에서는 OTP생성키, OTP 인증모듈 등의 주요 정보를 USIM에 저장하기 위해 사용되는 서비스 도메인키(Service Domain Key)의 효율적이고 안전한 관리를 위해 OTP 통합인증센터 기반의 서비스 모델을 대상으로 기술한다.

□ USIM OTP 발급

USIM OTP 발급 모델은 USIM에 설치되는 인증모듈은 인증모듈과 구동모듈을 설치하는 1차 발급과, OTP생성키 등의 주요 정보를 USIM내에 저장하는 2차 발급으로 구성된다. 1차 발급은 이동통신사를 통해 OTA방식으로 발급하며, 2차 발급은 대면확인 후 발급이 가능하다.

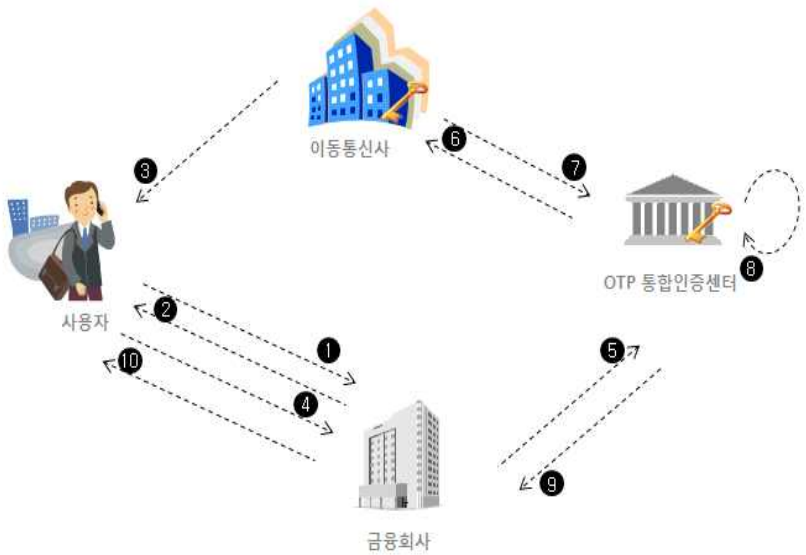

그림 8 USIM OTP 발급과정

<적용 예시>

① 사용자가 금융회사에 USIM OTP 발급 신청
② 금융회사는 사용자 대면확인 후 발급에 필요한 정보를 사용자에게 전달
③ 사용자는 발급에 필요한 정보를 이용해서 1차 발급 요청을 하고 이동통신사는 사용자에게 1차 발급 수행
④ 사용자는 금융회사에 2차 발급 요청
⑤ 금융회사는 사용자 정보와 함께 OTP 통합인증센터에 USIM OTP 2차 발급 요청
⑥ ⑦ 이동통신사와 OTP 통합인증센터는 사용자의 서비스 신청여부 확인
⑧ 통합인증센터는 사용자의 OTP생성키등 주요정보 생성
⑨ 통합인증센터는 관련 정보를 금융회사에 전달
⑩ 통합인증센터는 관련 정보를 이용해서 사용자에게 USIM OTP 2차 발급 수행

□ USIM OTP 인증

USIM OTP 인증과정은 H/W 기반의 OTP와 동일하며 <그림 9>은 USIM OTP 인증과정을 도식화하고 있다.

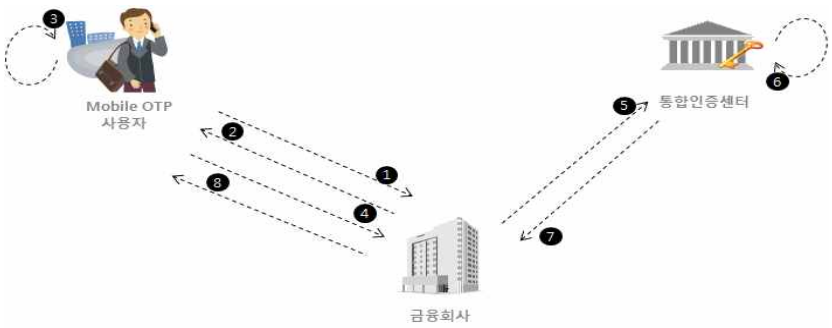

그림 9 USIM OTP 인증과정

<적용 예시>

① 사용자는 금융회사에 인증 요청
② 금융회사는 사용자에게 OTP 요청
③ 사용자는 USIM OTP를 이용해서 OTP 생성
④ 생성한 OTP를 금융회사에 전달
⑤ 금융회사는 사용자 정보와 전달받은 OTP를 OTP 통합인증센터에 전달하여 OTP 인증 요청
⑥ OTP 통합인증센터는 사용자 정보를 이용해서 OTP 인증
⑦ OTP 통합인증센터는 인증한 결과를 금융회사에 전달
⑧ 금융회사는 전달받은 정보를 이용해서 사용자 인증결과를 사용자에게 전달

2. 특징

가. USIM 기반 인증기술

기존 H/W 기반의 OTP는 별도의 H/W 장치 소지에 따른 사용자 불편함이 있었지만, USIM OTP 인증기술은 USIM을 지원하는 사용자의 휴대폰을 이용해서 OTP를 생성하기 때문에 별도의 장치를 소지하지 않아도 된다. 사용자는 인증이 필요한 경우 자신의 휴대폰에 저장된 USIM OTP 모듈을 이용해서 OTP를 생성하고 그 값을 입력함으로써 기존의 H/W 기반의 OTP와 동일하게 인증을 수행할 수 있다. 또한 스마트 폰의 키패드와 디스플레이를 이용하여 거래연동 인증기술과 같은 보안이 강화된 인증기술을 USIM에 구현이 가능하기 때문에 높은 보안을 요구하는 서비스에도 활용이 가능하다.

나. H/W 기반의 OTP와 동등한 수준의 보안성

USIM OTP 인증기술은 S/W 기반으로 구현되지만, 기본적으로 OTP 생성키, 인증모듈과 같은 중요 정보를 안전한 USIM내에 저장함으로써, H/W 기반의 OTP와 동등한 수준의 안전성을 제공한다. 이로 인해 비밀정보의 외부유출 방지 및 비밀정보 추측공격, 사전 공격 등 오프라인 공격에 대응이 가능하다.

다. 서비스 적용시 고려사항

USIM OTP 인증기술은 사용자 비밀정보, 인증모듈 등은 USIM에 저장되기 때문에 이를 위한 USIM 저장용량이 필요하지만, 현재 USIM의 저장용량에 제약이 있어, 다수의 비밀정보 및 인증모듈을 저장하기보다는 단일 비밀정보 및 인증모듈을 공유하여 용량제약을 해결해야 할 것이다. 또한 사용자 비밀정보 및 인증모듈을 USIM에 설치를 위해 서비스 도메인키가 필요하여 이 키의 안전한 관리가 필요하고, USIM 사용을 위해 이동통신사의 협력이 필요하다.

3. 기술적 근거 및 적용사례

가. 적용사례

현재 USIM을 이용한 OTP 인증기술을 상용화하여 적용된 사례를 찾아보기가 어렵고, 다만 기존 모바일 폰에 탑재된 SIM을 이용한 OTP 인증기술은 유럽의 일부나라에서 도입된 사례가 있다.

그 예로서 독일의 UniverSIM OTP를 들 수 있으며 구성은 <그림 10>과 같다. UniverSIM OTP 서비스를 이용하기 위해서는 SMS를 통해서

사용자의 비밀정보를 SIM에 다운로드한 후, OTP를 SIM에서 생성하여 인증에 이용한다.[11]

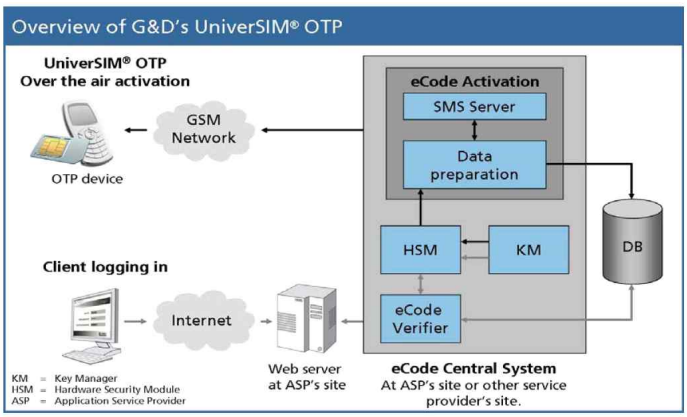

그림 10 독일 Giesecke & Devrient社의 SIM-OTP

<그림 11>은 네덜란드의 Gemalto社의 SIM-OTP을 이용한 인증절차를 나타낸다. 사용자는 ①원하는 은행(계좌)을 선택하고 OTP생성을 요청하고 ② SIM에 접근하기 위한 PIN을 입력 후, ③ 생성된 OTP를 웹브라우저에 입력하여 전자금융을 이용하는 방식이다.[12]

그림 11 Gemalto社의 SIM-OTP

4. 항목별 검토결과

가. 적용성

검토항목	검토 우선순위	검토내용
적용 가능성	높음	• USIM OTP를 도입하기 위해서는 이동통신사와 기술적, 업무적으로 지원이 필요하고 USIM을 지원하는 단말기가 필요하여 적용이 다소 어려움. • H/W OTP와 동일한 방식으로 다양한 환경에 적용 가능하며, 멀티 OS 및 멀티 플랫폼에 추가 개발 없이 쉽게 적용 가능 **⇒ 다양한 환경에 적용이 가능하지만 이통사와의 협력 및 USIM 지원 단말이 필요함**
적용 비용	보통	• USIM OTP는 기존 OTP기술과 완벽하게 호환되어, 금융회사에 도입시 개발 비용이 크게 소요되지 않음 • USIM OTP는 물리적인 매체를 이용자에게 별도로 배포가 필요 없음 **⇒ 적용 비용이 매우 적음**
기술 중립성	보통	• USIM OTP를 이용시 단지 OTP를 입력만을 요하므로 순수 웹 표준기술만으로도 구현이 가능 • 스마트TV, ATM 등의 다양한 전자금융 환경에서도 기술개발 없이 적용 가능 **⇒ 표준기술로만으로도 구현이 가능**
기존 인프라 활용성	낮음	• 기존 OTP 기술과 완벽히 호환되므로, OTP 통합인증센터를 활용하여 최소한의 변경만으로 즉시 적용이 가능 **⇒ OTP 통합인증센터 인프라 활용이 가능**

적용성 검토결과	분류	적용 가능성	적용 비용	기술 중립성	기존 인프라 활용성	종합 (검토수치)
	검토결과	보통	우수	우수	우수	우수 (2.6)
	검토 우선순위	높음(3)	보통(2)	보통(2)	낮음(1)	

나. 편의성

검토항목	검토 우선순위	검토내용
소지 편의성	높음	• 사용자가 소지한 휴대폰, 스마트폰 등에 내장된 USIM을 이용하기 때문에 별도의 전용 매체를 소지할 필요가 없음 ⇒ **별도의 전용 매체 소지가 필요 없어, 소지 편의성은 높은 수준임**
사용 편의성	보통	• 기존 H/W OTP발생기와 사용이 유사하며, 단지 USIM에 접근하기 위한 PIN번호 입력이 필요하지만 사용 편의성을 저해하지 않음 ⇒ **PIN만을 요구하기 때문에 사용상의 불편이 없어 사용 편의성은 높은 수준임**
관리 편의성	보통	• USIM OTP는 기존 OTP와 동일하게 도난·분실 시, 즉시 사고신고가 가능하여 관리가 용이함 • 매체 복제가 원천적으로 불가능하여 관리상의 부주의에 의한 문제가 발생하지 않음 • USIM을 모든 금융회사에서 공통으로 사용가능 ⇒ **도난 등에 즉시 대응 가능하여 관리 편의성이 높음**

<table>
<tr><td>발급 편의성</td><td>낮음</td><td>• 직접 대면확인을 통해서 발급/재발급/폐기 등을 수행함
• 다만, USIM을 여러 금융회사와 공유가 가능하여 최초 1회만 대면확인이후 온라인으로 등록 등 절차 간소화가 가능
⇒ 대면 발급원칙으로 발급 편의성이 보통 수준임</td></tr>
<tr><td>교육 편의성</td><td>낮음</td><td>• USIM에 접근하기 위한 PIN 관리를 위한 교육이 필요
⇒ PIN 관리상의 교육이 필요하여 교육 편의성은 보통 수준임</td></tr>
<tr><td>편의성 검토결과</td><td colspan="2">
<table>
<tr><th>분류</th><th>소지 편의성</th><th>사용 편의성</th><th>관리 편의성</th><th>발급 편의성</th><th>교육 편의성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>우수</td><td>우수</td><td>보통</td><td>보통</td><td rowspan="2">우수 (2.8)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

다. 보안성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토된 내용</th></tr>
<tr><td>오프라인
공격에
안전</td><td>-</td><td>• OTP 생성에 필요한 비밀정보는 USIM으로 안전하게 보관되기 때문에 노출 및 복제가 불가능
• 비밀번호 추측공격 및 Phishing 공격으로 노출된 OTP를 통해 비밀정보 유추가 불가능 등 기존 OTP와 동일한 보안 강도를 가짐
⇒ 기존 OTP와 동일한 보안강도를 가지므로 우수함</td></tr>
<tr><td>온라인
공격에
안전</td><td>-</td><td>• OTP의 짧은 유효시간, 인증횟수 제한 등 임계치(threshold)을 통해 MITM 공격에 의한 사고발생을 줄일 수 있고,
• SSL/TLS 기술과 연계하면 MITM 공격에 안전함
⇒ MITM 공격에 의한 사고가 발생할 가능성이 있으나, 대응이 가능하므로 보통임</td></tr>
<tr><td>거래정보
변조 공격에
안전</td><td>-</td><td>• 일반적인 OTP의 경우, 메모리 변조공격에 의한 부정거래에 대응이 어려움이 있지만,
• 거래연동 OTP 기술을 USIM에 구현하여 사용하면 부정거래 방지가 가능함
⇒ 거래정보 변조 공격에 대응이 어려워 대응수준은 미흡.
단, 거래연동 인증기술 도입시 대응 가능함</td></tr>
<tr><td colspan="2">보안성 검토결과</td><td>
<table>
<tr><th>분류</th><th>오프라인
공격에 안전</th><th>온라인
공격에 안전</th><th>거래정보 변조
공격에 안전</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>보통</td><td>미흡</td><td rowspan="2">보통
(2.0)</td></tr>
<tr><td>검토
우선순위</td><td>- (1)</td><td>- (1)</td><td>- (1)</td></tr>
</table>
</td></tr>
</table>

제 2 절 거래연동 인증기술(Transaction Signing)

1. 기술소개

가. 배경

현재 해킹 공격 방식은 서버와 클라이언트의 통신채널에 침입하여 정보의 위·변조하는 공격 방식보다는 공격이 용이한 사용자 PC에 침입하여 중요정보의 유출이나 위·변조하는 공격 방식으로 진화하고 있다. 최신 해킹 공격기술인 브라우저 변조공격(Man-in-the-browser)은 메모리 변조공격의 일종으로, 브라우저상의 거래정보를 사용자 모르게 변조하는 공격으로 사용자의 전자금융서비스 이용시 위험성을 증가시키고 있다.

메모리 변조공격은 PC 메모리에 존재하는 거래정보를 위·변조하기 때문에 사용자의 비밀번호 및 공인인증서가 노출되지 않아도 부정거래가 가능하며, 해당 공격의 더 큰 위험성은 사용자가 인지할 수 없다는 것이다. 이러한 고도화된 공격에 대응하기 위해서 거래정보에 대해 사용자의 인지가 가능하고, 해당정보에 대해 인증을 제공하는 거래연동 인증기술이 필요하다.[7,13]

나. 기술 개요

거래연동 인증기술은 이용자가 인식 가능하도록 정보를 출력하는 화면과 계좌번호, 금액 등을 입력할 수 있는 키패드를 탑재하고, 개인의 식별정보 및 비밀정보를 안전하게 저장하는 거래서명 발생기가 필요하다. 본 연구보고서에서는 거래연동 OTP 기술을 대상으로 한다. 거래연동 OTP은

사용자가 전자금융서비스의 거래정보를 확인하고, 거래연동 OTP발생기에 직접 수신계좌번호, 금액 등의 거래정보를 입력하여 거래정보와 연동된 인증값인 OTP를 생성하고, 금융서버에서는 OTP의 검증을 통해 부정거래 여부를 검출할 수 있다.[7]

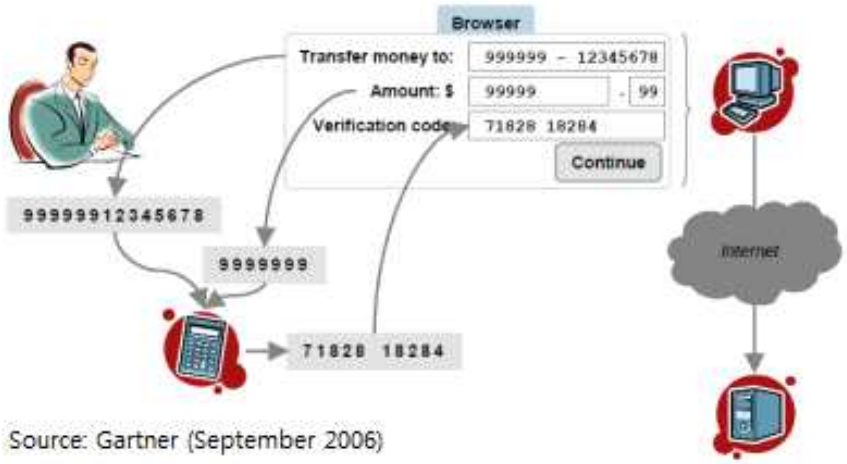

그림 12 거래연동 인증기술 흐름도

<적용 예시>

① 사용자가 전자금융거래서비스 사이트에 접속하여 보내고자하는 계좌번호 및 금액을 웹브라우저에 입력

② 사용자가 직접 거래연동 OTP발생기에 수신계좌번호와 이체금액 등 거래정보를 입력

③ 거래연동 OTP발생기 화면에 나타난 OTP를 웹브라우저를 통해 입력 후 금융서버로 전송

④ 금융서버는 전송된 거래정보와 OTP를 검증한 후, 검증결과에 따라 서비스 요청에 응답

2. 특징

가. 부정거래 방지

거래연동 인증기술은 거래정보와 연계된 OTP를 생성하므로, 세션가로채기(Session Hijacking), MITM 공격 등으로 거래정보 혹은 연계된 OTP를 위·변조할 경우에 금융서버에서 해킹공격에 대한 검출이 가능하여, 부정거래 방지기능을 제공한다. 또한 오·남용된 OTP를 통해서 부정거래에 이용할 소지가 있어, OTP 유효시간 제한, 인증 횟수제한 등과 같은 임계치(threshold)를 이용하여 추가적으로 부정거래를 예방할 수 있다.

나. 새로운 환경에 적용 가능

별도로 분리된 거래연동 OTP발생기를 통해서 OTP를 생성하기 때문에 새로운 전자금융거래환경별 거래연동 OTP생성모듈을 구현할 필요가 없고, 또한 숫자로 이루어진 OTP를 입력받아 금융서버로 전송할 수 있는 기능이 요구되지만, 이것은 웹 표준기술을 이용하여 구현가능하기 때문에 특정 기술에 종속되지 않고 다양한 환경에 적용 가능한 특징이 있다.

다. 악성코드에 원천적인 대응 가능

거래연동 인증기술은 거래정보를 사용자가 직접 입력하며, 물리적으로 분리된 안전한 H/W 기기에서 사용자가 입력한 거래정보와 연계된 OTP를 생성하므로 악의적인 코드에 의한 해킹에 안전하다.

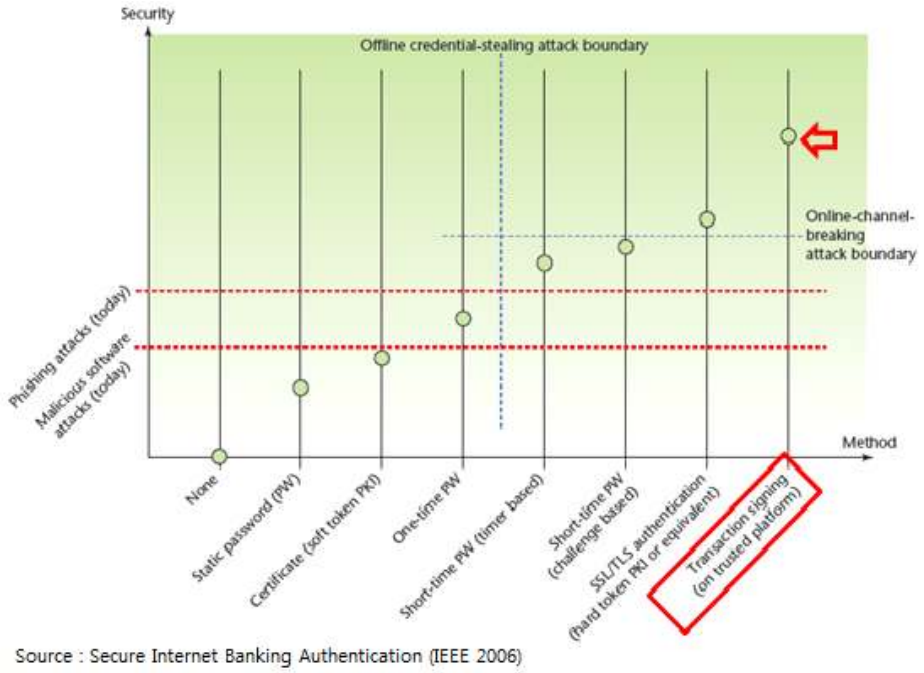

그림 13 공격에 대한 인증기술 안전성 분류

위 그림에서 볼 수 있듯이 안전한 H/W 기반(신뢰된 플랫폼)에서 생성한 거래정보와 연동된 OTP를 생성하는 인증기술은 오프라인 중요정보 유출 공격 (Offline credential-stealing attack), 온라인 통신채널 조작 공격 (Online-channel-breaking attack)에 안전하다.[7]

3. 기술적 근거 및 적용사례

가. 기술적 근거

□ "Transaction Verification Complements Fraud Detection and Stronger Authentication" (Gartner, 2006)

Phishing, pharming, MITM공격 등의 다양한 공격에 대응하기 위해서는 강화된 인증기술과 더불어 부정거래를 탐지할 수 있는 보안기술을 제공해야한다. 거래서명 기술은 거래정보의 무결성과 거래 발생자의 신원식별 기능을 제공하기 때문에 부정거래 공격에 대응 할 수 있다.

거래서명 기술은 인터넷 채널이외에 또 다른 채널을 이용한 방법과 비대칭 및 대칭 암호 알고리즘을 이용한 디지털서명 혹은 MAC 알고리즘을 이용한 방법이 존재한다.

특히, MAC을 이용하는 방법의 대표적인 예는 거래연동 OTP기술이다. 거래 정보를 사용자 직접 거래연동 OTP발생기에 입력하여, 거래정보와 연계된 인증값인 OTP를 생성하고 금융서버에 전송한다. 금융서버에서 OTP의 유효성 검증을 통해 위·변조를 검출 및 거래생성자의 신원식별도 가능하기 때문에 안전한 전자금융 이용시 고려해야 하는 기술임을 이 기술문서에서 기술하고 있다.[13]

□ "Secure Internet Banking Authentication" (IEEE, 2006)

이 논문에서는 다양한 공격기법을 공격수준별로 분류하고, 이에 대응 가능한 인증기술에 대해 보안성을 평가하였다. 평가된 인증기술로는 고정 비밀번호(Static password), 인증서, 보안카드, 시간동기화 OTP, HSM 등이 있으며, 이중에서 신뢰된 플랫폼에서 거래서명 인증기술이 모든 공격기법에 대응 가능한 인증기술로 평가하고 있다. 이 기술은 거래조작 공격과 같은 고도화된 해킹공격에도 대응이 가능하다고 기술하고 있다. 또한, 거래서명 인증기술의 대표적인 예로 EMV-CAP기술을 소개하고 있다.[7]

나. 적용 사례

거래연동 인증기술의 대표적인 기술은 CAP(Chip Authentication Program) 기술이다. CAP 기술은 APACS(영국 지불결제 연합)과 EMV 그룹에서 제안한 기술이며, 영국을 포함하여 유럽에서 서비스를 시작하여 현재 전 세계적

으로 가입자 수가 8백만명을 넘어섰다.

CAP기술을 이용하기 위해서는 <그림 14>과 같이 키패드와 출력화면을 가진 스마트카드 리더기와 CAP 인증모듈이 탑재된 스마트카드가 필요하다.

그림 14 CAP지원 스마트 카드 및 리더기

서비스 절차는 스마트카드 리더기에 개인용 스마트카드를 삽입하여, 웹브라우저에 표시되는 전자금융 거래정보를 사용자가 직접 스마트카드 리더기를 통해 입력을 한다. <그림 15 참조>

그림 15 거래정보 입력 (CAP Demo 화면)

사용자가 입력된 값과 스마트카드에 저장된 비밀정보를 기반으로 스마트카드내의 인증모듈에서 인증값인 OTP를 생성하고 스마트카드 리더기 화면에 출력을 한다. <그림 16 참조>

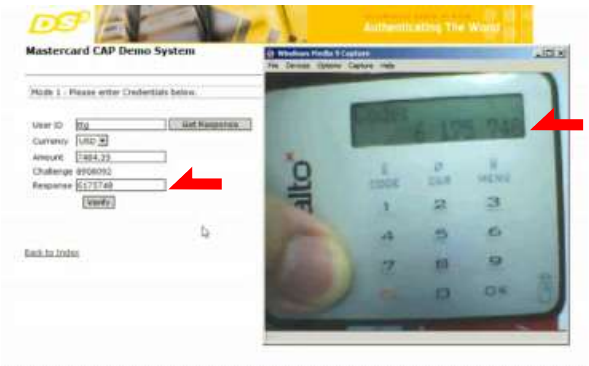

그림 16 인증값 생성 (CAP Demo 화면)

사용자는 다시 웹브라우저에 출력된 OTP를 입력한 다음, 금융서버로 전송한다. 금융서버는 전송된 거래정보와 OTP에 대해 검증을 수행한 후, 금융서비스를 수행한다. CAP 기술을 이용하여 생성된 인증값 OTP는 거래 서명의 한 형태로 볼 수 있다.[9]

4. 항목별 검토결과

가. 적용성

검토항목	검토 우선순위	검토내용
적용 가능성	높음	• 거래연동 OTP는 입력창에 OTP발생기에서 생성된 OTP를 입력하는 방식으로 적용되기 때문에, 별도의 추가적인 개발이 필요 없음 • 스마트폰, IPTV, ATM 등의 다양한 환경에 일관된 방식으로 적용 가능하며, 멀티 OS 및 멀티 플랫폼에 추가 개발 없이 쉽게 적용 가능 **⇒ 추가 개발이 필요 없어, 적용 가능성이 높음**
적용 비용	보통	• 거래연동 OTP는 기존 OTP 기술과 완벽하게 호환되어, 금융회사에 적용시 개발 비용이 크게 소요되지 않음 • 거래연동 OTP를 지원하는 물리적인 매체를 이용자에게 배포하는 비용이 소요됨 **⇒ 매체 비용이 예상되므로 적용 비용이 높지만, USIM을 이용할 경우, 적용 비용이 낮아질 수 있음**
기술 중립성	보통	• Active-X 등의 별도 모듈이 필요 없으며, 순수 웹 표준기술만으로도 구현이 가능 • 텔레뱅킹, 스마트폰, IPTV, ATM 등의 매체에서도 전문적인 기술개발 없이 적용 가능 **⇒ 순수 표준기술로만으로도 구현이 가능**

<table>
<tr><td>기존 인프라 활용성</td><td>낮음</td><td>• 기존 OTP 기술과 호환되므로, OTP 통합인증센터를 활용하여 최소한의 변경만으로 즉시 적용이 가능
⇒ OTP 통합인증센터 인프라 활용이 가능</td></tr>
<tr><td colspan="2">적용성 검토결과</td><td>
<table>
<tr><th>분류</th><th>적용 가능성</th><th>적용 비용</th><th>기술 중립성</th><th>기존 인프라 활용성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>미흡 (보통*)</td><td>우수</td><td>우수</td><td rowspan="2">우수 (2.5)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

*USIM OTP를 이용할 경우 적용비용이 다소 감소할 수 있음

나. 편의성

검토항목	검토 우선순위	검토내용
소지 편의성	높음	• 거래연동 OTP를 위한 물리적인 매체를 항상 소지해야 함 • 일반 H/W OTP에 비해 화면 크기 및 키패드 부착 등으로 인해 크기가 커짐 ⇒ **전용 매체를 이용하여 소지 편의성은 낮은 수준임**
사용 편의성	보통	• 계좌번호, 송금액 등 거래와 연동하기 위한 거래정보를 OTP발생기에 부착된 숫자판에 직접 입력해야 함 ⇒ **별도 입력이 필요하여 사용 편의성은 낮은 수준임**
관리 편의성	보통	• 거래연동 OTP발생기를 도난·분실 등에 의해 타인에게 노출되었을 때, 즉시 사고신고가 가능하여 관리가 용이함. • 매체 복제가 원천적으로 불가능하여 관리상의

<table>
<tr><td></td><td></td><td>부주의에 의한 문제가 발생하지 않음.
• 1개의 매체로 모든 금융회사에서 공통으로 사용가능
⇒ 도난 등에 즉시 대응 가능하여 관리 편의성이 우수함</td></tr>
<tr><td>발급 편의성</td><td>낮음</td><td>• 직접 대면확인을 통해 발급/재발급/폐기 등을 수행하여야 하며, 타기관 이용등록 시에도 은행권역의 경우에는 대면확인이 필요
• 다만, 최초 1회만 대면확인시 증권사 등의 경우에는 온라인으로 등록이 가능하며, 고장 재발급 등의 민원발생시에는 자동등록이 가능
⇒ 대면 발급원칙으로 발급 편의성이 보통 수준임</td></tr>
<tr><td>교육 편의성</td><td>낮음</td><td>• 피싱, 사기 등에 의해 OTP발생기의 숫자판에 해커가 요구하는 숫자를 입력하지 않도록 교육할 필요가 있음
• 그러나, 실제 해킹을 위해서는 OTP의 사용시간제한 등이 복합적으로 고려되어야 하므로 집중적인 교육이 필요하지 않음
⇒ 이용시 유의사항 등의 교육 편의성은 보통 수준임</td></tr>
<tr><td colspan="2">편의성 검토결과</td><td>
<table>
<tr><th>분류</th><th>소지 편의성</th><th>사용 편의성</th><th>관리 편의성</th><th>발급 편의성</th><th>교육 편의성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>미흡 (우수*)</td><td>미흡 (우수**)</td><td>우수</td><td>보통</td><td>보통</td><td rowspan="2">보통 (1.7)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

*USIM OTP를 이용할 경우 별도의 매체를 소지할 필요가 없음

**거래정보의 입력을 스마트폰의 카메라 또는 통신기능을 이용하여 간소화 할 수 있음

다. 보안성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토된 내용</th></tr>
<tr><td>오프라인
공격에
안전</td><td>-</td><td>• OTP 생성에 필요한 비밀정보는 H/W로 안전하게 보관되기 때문에 노출 및 복제가 불가능
• Phishing 및 Pharming 공격을 통해 OTP가 노출되더라도 이를 이용하여 비밀정보 유추가 불가능하고, 또한 OTP는 매번 상이한 값을 가지므로 재사용이 불가능
⇒ 비밀정보 추측공격, Phishing공격에 의해 사용자의 비밀정보 유출이 불가능하여 우수함</td></tr>
<tr><td>온라인
공격에
안전</td><td>-</td><td>• MITM 공격으로 전송되는 거래정보의 위·변조가 발생할 경우, 거래정보와 연계된 OTP를 금융서버에서 검증하므로 써 공격에 대응할 수 있어 안전하다고 판단됨
⇒ 공격에 의한 거래정보 위·변조에 대응 가능하므로 우수함</td></tr>
<tr><td>거래정보
변조 공격에
안전</td><td>-</td><td>• 메모리 변조공격으로 부정거래가 발생하더라도 OTP가 거래정보와 연계되어 있어 공격을 탐지·방어할 수 있음
⇒ 거래정보 변조공격인 메모리 변조공격 의한 부정거래에 대해 대응이 가능하여 우수함</td></tr>
<tr><td colspan="2">보안성 검토결과</td><td>
<table>
<tr><th>분류</th><th>오프라인
공격에 안전</th><th>온라인
공격에 안전</th><th>거래정보 변조
공격에 안전</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>우수</td><td>우수</td><td rowspan="2">우수
(3.0)</td></tr>
<tr><td>검토
우선순위</td><td>- (1)</td><td>- (1)</td><td>- (1)</td></tr>
</table>
</td></tr>
</table>

제 3 절 이상거래 탐지기술

1. 기술소개

가. 배경

최근의 금융사고는 Malware*, 바이러스 등으로 그 공격 방법이 더욱 정교해지고 있다. 각종 보안 소프트웨어를 온라인 금융거래 이용자들에게 강제하여 설치하더라도 이용자의 환경을 신뢰하기 어렵고, 또한 새롭게 개발되는 악의적인 공격에 대해 신속한 대응이 힘든 실정이다. 따라서 이용자에게 적용된 인증기술들이 고도화된 공격에 의해 무력화된 경우에도 금융서버에서 이용자의 전자금융 거래정보를 분석하여, 분석된 사용자의 전자금융 거래패턴과 상이한 이상거래에 대해서 탐지할 수 있는 이상거래 탐지 시스템(Fraud Detctection System, FDS)이 개발되었다.[14,15]

* 트로이 목마, 키보드 입력 유출 프로그램, 스파이웨어 등 정보를 유출하는 의도로 제작된 소프트웨어

나. 기술 개요

온라인 금융거래에서의 이상거래 탐지기술은 이용자의 거래 이용 정보(접속, 거래, 행위 등)를 각각의 미리 정의된 룰(Rule)에 따라 룰 엔진(rule engine)으로 분석하여 사용자의 패턴을 생성한 뒤에 현재 처리되는 거래와 비교하여 이상거래를 판별해 낸다.

룰 엔진에 의해 분석되는 이용자 거래 처리 정보는 다음과 같이 분류할 수 있다.

1) 접속정보 : 이용자가 접속하는 IP주소, 접속하는 브라우저의 정보(회사, 언어, 버전), OS 환경 등의 일반적인 접속정보

2) 거래정보 : 송금자, 거래시간, 금액의 크기 등

3) 행동정보 : 연속적으로 거래를 모니터링 하여 이용자 세션에서 제공되는 특정한 행동과 처리 패턴

이러한 정보는 향후 이상거래 탐지를 위한 비교 패턴을 만드는 요소로 사용된다. 서버는 해당 정보를 이용하여 아래의 예시와 같은 이상거래로 간주할 수 있는 다양한 룰을 생성하여 시스템을 운용할 수 있다.

1) 한 번의 거래 후 1시간 안에 100km 이상 떨어진 위치에서 거래를 시도하는 경우

2) 연속적으로 인증실패를 한 IP 주소에서 접속한 이용자가 계좌 있는 모든 금액의 이체를 시도하는 경우

3) 해외계좌로 이체 한 적이 없는 이용자가 새벽 1시에서 5시 사이에 중국에 있는 계좌로 이체를 시도하는 경우

룰 엔진은 이러한 룰을 기준으로 이상거래를 판별하여 위험점수(risk score)를 계산하고 기준 점수를 초과하면 이상거래로 판단할 수 있다. 이상거래로 판단한 경우 실시간으로 거래를 취소하거나 거래단계별로 OTP나 2채널인증 같은 인증기법을 통해서 추가적인 인증을 요청할 수도 있다.

Day of week	Time of day	IP Address	Location	Browser
Monday	10:30 AM	10.10.10.10	Providence, RI	Mozilla Firefox 1.5
Tuesday	1:00 PM	10.10.10.10	Providence, RI	Mozilla Firefox 1.5
Thursday	12:00 PM	10.10.10.10	Providence, RI	Mozilla Firefox 1.5
Thursday	9:00 PM	192.168.10.10	Boston, MA	IE 5.5
Saturday	2:00 PM	192.168.10.10	Boston, MA	IE 5.5
Sunday	11:00 AM	192.168.10.10	Boston, MA	IE 5.5
Monday	3:30 PM	10.10.10.10	Providence, RI	Mozilla Firefox 1.5
Monday	7:30 PM	192.168.10.10	Boston, MA	IE 5.5
Tuesday	6:30 AM	192.168.10.10	Boston, MA	IE 5.5
Wednesday	9:00 AM	10.10.10.10	Providence, RI	Mozilla Firefox 1.5

그림 17 이상거래 탐지 방법의 예

이상거래 탐지 시스템에 <그림 17>과 같이 전자 금융거래 이용자A의 거래 내역이 통보되었다고 가정하자. 이용자A는 주로 Boston과 Providence 두 지역에서 접속하는 것으로 볼 수 있으며 해당 지역에서 접속 시 동일한 인터넷 브라우저를 사용한다는 것을 알 수 있다. 또한 업무시간과 그 이외의 시간에 따라 접속하는 곳이 다르다는 것도 알 수 있다

이용자A가 <그림 18>과 같은 거래를 하였다고 가정하면,

Day of week	Time of day	IP Address	Location	Browser
Tuesday	1:00 PM	172.16.17.18	Mountain View, CA	IE 5.5

그림 18 이용자의 거래내역 예

이상거래 탐지 시스템 서버의 룰 엔진은 정해진 룰에 따라 패턴을 비교하기 때문에 이용자A의 거래정보가 기존의 정상 패턴과는 다른 거래 패턴을 보이고 있어 이상거래 탐지 시스템은 해당 이용자의 거래를 이상거래로 판단할 수 있다. <그림 19> 참조

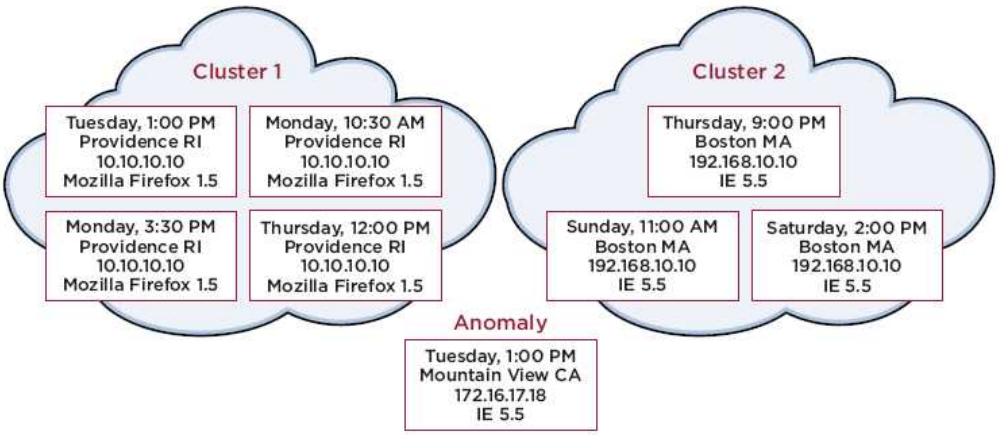

그림 19 패턴분석 개요도

그러나, 온라인에서는 빠르게 이상거래 패턴이 변화 및 진화되고 있어, 변화하는 이상거래를 탐지할 수 있도록 자동으로 거래패턴을 인지하고 분석하여 다양한 룰 설정이 가능한 룰 엔진을 도입한 이상거래 탐지 시스템 개발이 필요하다.

마지막으로 이상거래 탐지기술은 사용자의 거래패턴을 기반으로 탐지 기능을 제공하기 때문에 사용자의 거래패턴에 대한 신뢰된 정보수집이 요구된다. 이를 위해서는 사용자 인증 및 거래정보에 대한 인증 및 무결성 등을 제공하는 타 인증기술과 조합하여 사용해야만 효과적인 기능을 수행할 수 있다.

2. 특징

가. 서버기반 운영

이상거래 탐지기술은 금융서버에 구축되어 사용자의 전자금융 거래패턴을 비교·분석하여 이상거래를 탐지하는 기술로써, 시스템 구축 및 운영시

사용자 환경에 어떠한 영향도 미치지 않는다.

나. 새로운 환경에 적용이 가능

전자금융 환경은 사용자의 PC에서 스마트폰을 활용한 모바일 환경으로 빠르게 변화되고 있다. 새로운 전자금융 환경으로 변화함에 따라 이에 대응하는 각종 보안 수단들은 추가적으로 개발이 필요하지만, 이상거래 탐지 시스템은 이용자 환경에 영향을 주지 않기 때문에 향후 급격한 전자거래 환경의 변화에도 능동적인 대응이 가능하다.

3. 기술적 근거 및 적용사례

가. 기술적 근거

□ **"Sharing Transaction Fraud Data" (IETF, 2010)**

금융회사가 이상거래 탐지 시스템(Fraud Detection System)을 도입하여 효율적으로 운용하기 위해서는 각 금융회사별로 수집한 이상거래 데이터를 서로 공유하여 대응하는 것이 효과적이다. 위 논문에서는 금융회사별로 수집한 이상거래 데이터를 수집하여 IODEF(Incident Object Description Exchange Format)* 형식으로 만들어 공유할 수 있는 방법을 기술하고 있다.[16]

* 다중 도메인 환경에서 도메인 간 침해사고 이벤트를 교환하기 위한 포맷

나. 적용 사례

이상거래 탐지 시스템의 대표적인 적용 사례는 HSBC 은행이 도입한 미국 VeriSign社의 VIP 이상거래 탐지 서비스(Fraud Detection Service)이다.

VIP 서비스는 사용자를 2개 부류로 분류하여 차별화된 인증서비스를 제공하는 특징을 가진다. ID,비밀번호만을 사용하는 사용자 부류와 ID, 비밀번호 외에 OTP를 추가로 사용하는 사용자 부류로 분류된다.

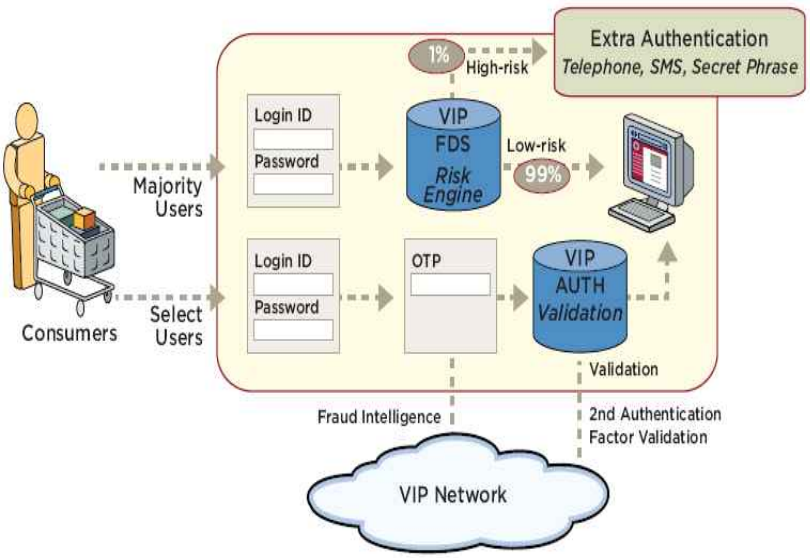

그림 20 VIP 서비스 구성도

VIP 서비스는 2팩터인증, 즉 비밀번호와 OTP을 사용하는 사용자(Select Users)는 이상거래 시스템의 감시 없이 2팩터에 의한 인증 값 검증만으로 전자금융 서비스를 이용하지만, 단일팩터인 비밀번호만을 사용하는 사용자(Majority Users)는 이상거래 시스템의 감시를 받으며, 시스템에 의해 이상거래 탐지가 될 경우에는 전화, SMS, 질의응답 등 추가적인 인증을 요구하여 이상거래를 차단하는 서비스이다.

단일팩터를 사용하는 일반사용자에 대한 이상거래 탐지 시스템의 서비스 절차는 <그림 21>과 같은 순서로 처리된다.

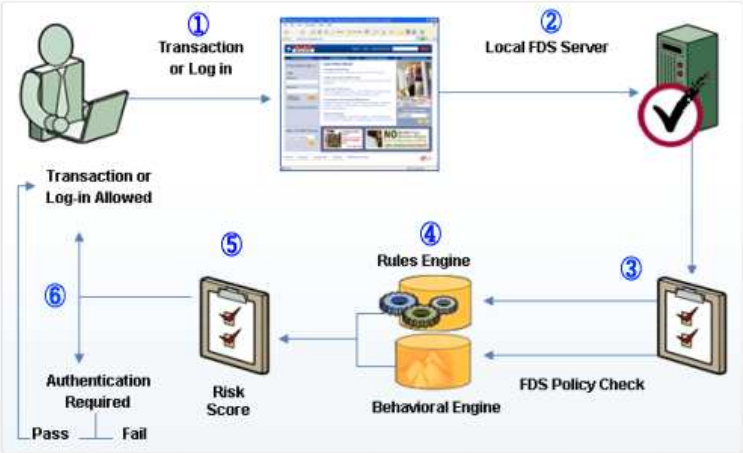

그림 21 이상거래 탐지 시스템 처리절차

<적용 예시>

① 전자금융서비스 이용자가 전자금융 거래를 위해서 금융회사에 온라인 접속

② 이상거래 탐지 시스템은 금융거래 이용자의 거래 내역 수집

③ 미리 정의된 룰에 따라서 해당 거래 내역의 데이터를 선별

④ 엔진에서 데이터를 분석하여 이상거래 패턴을 분석

⑤ 분석된 패턴을 위험 위험 점수(Risk Score)로 측정

⑥ 위험 점수를 정의해둔 임계치와 비교하여 거래를 허용 여부 판단

4. 항목별 검토결과

가. 적용성

검토항목	검토 우선순위	검토내용
적용 가능성	높음	• 이상거래 탐지 시스템은 금융서버에만 설치되어 사용자의 거래 패턴, 위치 등과 같은 알려진 사실을 이용하기 때문에 금융회사 시스템의 전반적인 개발이 필요하지 않음 • 다만, 충분한 정보수집 및 분석기간이 필요하여, 도입 초기에는 오탐률이 높아 적용하는데 어려움이 있음 • 또한, 이상거래 탐지의 경우에도 이체 등 거래를 제한하는 것은 현실적으로 불가능하기 때문에, VIP 고객 중 신청자를 대상으로 선 적용하는 것이 필요 • 이상거래 탐지시 사용자 인증을 위해 추가적인 인증 기술이 필요할 수 있음. **⇒ 초기 오탐율이 높기 때문에 정보수집 및 분석기간이 소요되므로 적용 가능성은 보통임**
적용 비용	보통	• 이상거래 시스템의 설치·운영과 지속적인 모니터링을 위해 비용발생 • 정확한 이상거래 탐지를 위해서 개인별 프로파일 수집과 패턴 설정을 위해 비용발생 • 사용자가 부담해야하는 비용은 없음 **⇒ 개인별 정보수집 및 패턴 분석 등 기간 및 운영비용이 발생으로 적용 비용 등급은 낮음**

<table>
<tr><td>기술 중립성</td><td>보통</td><td>• 기존 전자금융 서비스에 영향을 주지 않고, 저장된 거래정보 데이터을 통해 탐지하는 기술이며,
• 이상거래 탐지 데이터를 타시스템과 공유할 수 있는 표준기술 규격이 있어 시스템간 호환이 가능
⇒ 전자금융 환경에 영향을 받지 않고, 타 시스템과의 호환이 가능하여 기술중립성은 우수함</td></tr>
<tr><td>기존 인프라 활용성</td><td>낮음</td><td>• OTP 통합인증센터와 같은 공동망을 활용하여, 사용자의 모든 인증수행 정보를 금융회사에 제공이 가능하여 상호운용하기에 적합
⇒ OTP 통합인증센터 인프라 활용이 가능</td></tr>
<tr><td colspan="2">적용성 검토결과</td><td>
<table>
<tr><th>분류</th><th>적용 가능성</th><th>적용 비용</th><th>기술 중립성</th><th>기존 인프라 활용성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>보통</td><td>미흡</td><td>우수</td><td>우수</td><td rowspan="2">보통 (2.1)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

나. 편의성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토내용</th></tr>
<tr><td>소지 편의성</td><td>높음</td><td>• 사용자가 매체를 소지해야할 필요가 없음
• 다만, 이상거래 탐지시 거래 차단은 현실적으로 불가능하므로 거래를 계속 진행하기 위해 추가적인 인증을 요구할 수 있으며, 추가 인증기술에 따라 소지가 필요할 수 있음
⇒ 소지의 필요성이 없어서 소지 편의성은 우수함</td></tr>
<tr><td>사용 편의성</td><td>보통</td><td>• 사용자는 기존 전자금융 서비스와 변경되는 사항이 전혀 없이, 동일하게 이용이 가능하여 사용자의 편의성을 저해하지 않음
⇒ 사용 편의성은 우수함</td></tr>
<tr><td>관리 편의성</td><td>보통</td><td>• 사용자가 이상거래 탐지 시스템이 운영 중인 전자금융서비스에 접속을 위해서 추가적인 관리 사항이 없음
⇒ 관리 편의성은 우수함</td></tr>
<tr><td>발급 편의성</td><td>낮음</td><td>• 이상거래 탐지 시스템을 위한 사용자의 매체 발급은 필요 없음
⇒ 발급 편의성이 우수함</td></tr>
<tr><td>교육 편의성</td><td>낮음</td><td>⇒ 별도의 교육이 필요 없음 교육 편의성은 우수함</td></tr>
<tr><td colspan="2">편의성 검토결과</td><td>
<table>
<tr><th>분류</th><th>소지
편의성</th><th>사용
편의성</th><th>관리
편의성</th><th>발급
편의성</th><th>교육
편의성</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>우수</td><td>우수</td><td>우수</td><td>우수</td><td rowspan="2">우수
(3.0)</td></tr>
<tr><td>검토
우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

다. 보안성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토된 내용</th></tr>
<tr><td>오프라인
공격에
안전</td><td>-</td><td>• 기존 전자금융에 사용된 인증기술을 사용하고, 오프라인 공격을 대응하기 위해 추가적인 보완 기능이 없어 기존 인증기술의 안전강도와 동일하여 변화가 없음
⇒ 기존 인증기술에 의존적이고 또한 공격에 안전을 위해서 강화된 기능을 제공하지 않아 보통임</td></tr>
<tr><td>온라인
공격에
안전</td><td>-</td><td>• 프락시(Proxy), VPN을 이용한 MITM공격에 대응하기 위해 프로파일 항목을 다양화하여 세분화된 룰로 탐지 기능을 강화하면 일정수준만 대응이 가능함
• MITM 공격이 발생하는 경우 사용자의 IP, 디바이스 ID 등의 거래시작점 정보는 일부분 탐지할 수 있음.
⇒ MITM 공격에 의해 공격에 일정수준만 대응이 가능함</td></tr>
<tr><td>거래정보
변조 공격에
안전</td><td>-</td><td>• 거래정보 변조공격으로 사용자의 거래정보가 변조될 경우에 특정 거래정보(계좌번호, 금액 등)에 대한 룰에 의해 탐지가 불가능
⇒ 거래 변조공격으로 변조된 정보를 탐지가 불가능하므로, 대응수준은 낮음</td></tr>
<tr><td>보안성 검토결과</td><td colspan="2">
<table>
<tr><th>분류</th><th>오프라인
공격에 안전</th><th>온라인
공격에 안전</th><th>거래정보 변조
공격에 안전</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>보통</td><td>보통</td><td>미흡</td><td rowspan="2">미흡
(1.6)</td></tr>
<tr><td>검토
우선순위</td><td>- (1)</td><td>- (1)</td><td>- (1)</td></tr>
</table>
</td></tr>
</table>

제 4 절 PKI 서명센터

1. 기술소개

가. 배경

PKI 서명센터는 새로운 개념의 인증기술이 아닌 기존 PKI기술의 관리적 취약점을 보완하기 위해 PKI 기술을 변형하고 다른 인증기술들을 결합시킨 새로운 인증기술 구조를 제안한 것이다.

현재 PKI 구조에서는 공격자가 사용자의 로컬PC에 저장되어 있는 개인키, 인증서와 함께 개인 키 접근을 위한 비밀번호를 탈취하여 전자서명을 할 수 있는 취약점이 존재하기 때문에 정당한 사용자가 전자서명을 수행한 사실여부를 입증하는 것에 어려움이 존재한다. 특히 부인방지를 제공하기위해서는 사용자의 개인키 및 인증서의 도난, 복제와 같은 관리적 문제를 해결해야만 한다.[7,12]

이를 위해서 PKI 서명센터 구조에서는 사용자의 개인키 및 인증서 관리시스템인 중앙PKI 서명센터를 설치하고, 가입된 모든 사용자의 개인키와 인증서를 중앙PKI 서명센터에 저장함으로써, 사용자PC보다 상대적으로 안전하게 관리가 가능하여 인증서의 관리적 문제를 해결할 수 있다. 또한 중앙PKI 서명센터에서 PKI의 암호기술인 전자서명 기능을 제공하기 때문에 언제 어디서나 전자서명을 수행할 수 있어, 인증서의 휴대가 필요 없는 이점도 있다.

가. 기술소개

PKI 서명센터는 <그림 22>과 같이 중앙PKI 서명센터(Central infrastructure), 사용자(Customer), 금융시스템(Merchant) 3개의 객체들로 구성된다.

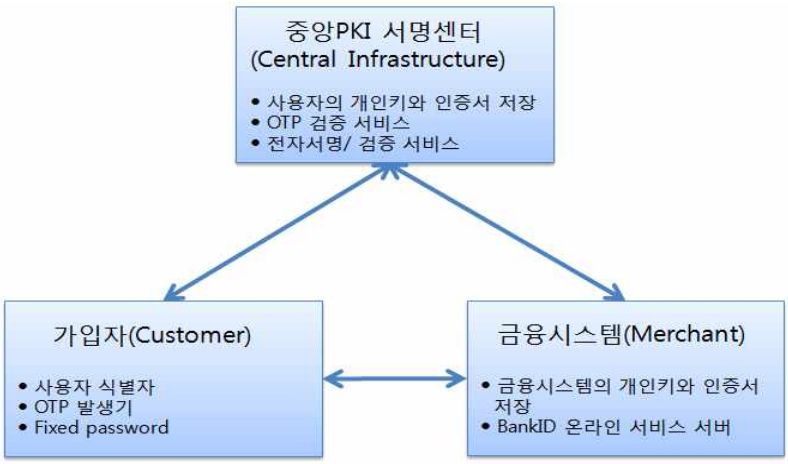

그림 22 PKI 서명센터 구성도

중앙PKI 서명센터는 사용자의 개인키와 인증서 저장 기능, 전자서명 생성 및 검증 기능, OTP 검증 기능을 제공한다. 금융시스템(Merchant)은 자신의 서버용 개인키와 인증서를 저장하여 필요시마다 전자서명을 수행하고 온라인 전자금융서비스를 제공한다. 가입자는 OTP발생기와 자신의 개인키에 대한 비밀번호를 소지하여 전자금융 서비스에 이용한다.

중앙PKI 서명센터의 서비스를 이용하기 위해서는 먼저 사용자는 대면 확인 등 안전한 신원 확인 과정을 거쳐, 개인키의 비밀번호 설정과 함께 OTP발생기를 발급받게 되고, 동시에 개인키와 인증서가 발급되어 중앙 PKI 서명센터에 안전하게 저장된다.

이후 중앙PKI 서명센터의 전자서명을 이용하기 위해서는 먼저 사용자 인증 절차를 거쳐야 한다. 사용자의 인증절차는 <그림 23>과 같이 중앙PKI 서명센터와는 2팩터인증 절차를 거치고 금융시스템과는 시도-응답 절차를 거치는 구조이다.

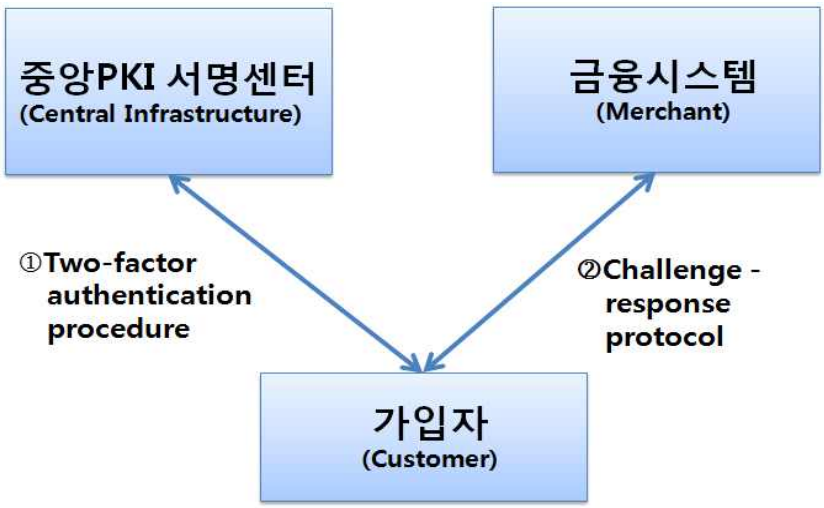

그림 23 인증절차 구조도

사용자는 ① OTP와 사용자의 개인키 비밀번호를 이용하여 중앙PKI 서명센터와 2팩터인증 절차를 거치면 사용자의 개인키에 대한 접근권한을 획득할 수 있다. 이후 ② 중앙PKI 서명센터는 사용자를 대신하여 시도(Challenge)에 대한 전자서명을 수행하여 응답(Response)을 생성하고, 금융시스템에 전송하여 시도-응답 인증절차를 진행한다. 모든 과정이 끝나면 중앙PKI 서명센터와 금융시스템에 대한 사용자 인증절차는 종료하게 된다.[18]

사용자 인증이 완료된 후, 사용자가 전자서명을 생성하기 위해서는 아래와 같은 절차를 거친다.

<전자서명 생성 예시>

① 사용자가 전자금융서비스 사이트에 접속하여 사용자 인증절차를 수행하고 전자금융서비스 웹페이지로 이동

② 사용자가 웹브라우저에 보내고자하는 계좌번호 및 금액을 입력·확인 후 이체 실행

③ 웹브라우저는 사용자에게 OTP와 비밀번호 입력을 요구하고, 사용자가 입력한 값과 거래 정보를 중앙PKI 서명센터로 전송

④ 중앙PKI 서명센터는 OTP로 사용자를 인증하고, 전송된 비밀번호로 저장되어 있는 사용자의 개인키를 복호화하여, 전송된 거래정보에 전자서명을 수행

⑤ 중앙PKI 서명센터는 전자서명 값을 사용자를 통해 금융시스템으로 전송

⑥ 금융시스템은 전송된 전자서명 값을 검증하고, 전자금융서비스 제공

⑦ 금융시스템은 전자서명 값을 다시 사용자에게 전송하고, 사용자는 부인방지를 위해 전자서명을 로컬PC에 저장

전자서명 생성 예시에서 기술했듯이 사용자는 비밀번호와 OTP발생기만을 소지하면 되고, 중앙PKI 서명센터에 개인키 및 인증서를 위탁하여 전자금융 이용 시마다 비밀번호와 OTP를 이용하여 사용자 인증을 거쳐 전자서명을 생성하는 구조로 요약될 수 있다.

2. 특징

가. 사용자 인증서의 관리 및 이동 편리성

사용자의 개인키와 인증서는 사용자의 로컬PC에 저장되는 것이 아니라 상대적으로 보안이 높은 중앙PKI 서명센터에 저장하기 때문에 악성코드에 의한 노출에 안전하고 사용자의 인증서 관리부주의에 의한 단점을 보안할 수 있다. 또한 중앙 시스템에 개인키와 인증서를 저장하기 때문에 다수의 PC에 사용하기 위해서 개인키와 인증서의 이동이 필요 없는 장점이 있다.

나. 2팩터 사용자 인증을 제공

사용자가 소지하고 있는 OTP발생기를 통해 생성된 OTP와 사전에 설정한 비밀번호를 이용하여 사용자 인증을 하기 때문에 기존 단일 팩터를 이용한 인증기술보다 안전함을 보장한다.

다. 서버기반의 전자서명 생성

전자서명 생성은 사용자PC에서 생성되는 것이 아닌 중앙PKI 서명센터에 보관된 사용자의 개인키와 인증서를 이용하여 중앙PKI 서명센터에서 전자서명을 생성하기 때문에 공격자가 사용자의 개인키 및 인증서를 유출하여 전자서명을 생성하는 것을 방지할 수 있다.

3. 기술적 근거 및 적용사례

가. 기술적 근거

□ "Risk Assessment of a National Security Infrastructure" (IEEE, 2009)

현 PKI 구조에 대한 설명과 PKI 구조를 변형하여 구현된 BankID 구조 및 각 구성요소의 기능을 상세히 설명하고 있다. 또한 PKI의 변형된 형태인 BankID 구조에서 부인방지 서비스를 지원하기위한 방법과 이를 이용하기 위한 사용자 인증절차를 설명하고 있다. 또한 BankID 구조에 대한 취약점 분석과 더불어 최신 해킹기법인 DDos 공격, Phishing/MITM 공격에 대한 BankID 구조의 위험도를 분석하고 있다.[18]

나. 적용사례

PKI 서명센터 구조의 대표적인 적용사례는 노르웨이 은행연합회(Norwegian Banking Community)에서 안전한 전자금융서비스를 위해 제안하고 노르웨이 은행에 적용된 BankID이다. 사용자 수는 2007년에 70만명에서 2009년에는 약 250만명으로 급속히 증가되는 추세이다. 이를 기반으로 국가적인 전자주민시스템에 도입을 고려중이다.[17]

BankID도 PKI 서명센터와 동일하게 사용자의 개인키와 인증서는 사용자의 로컬PC에 저장되는 것이 아니라 상대적으로 보안이 높은 중앙인증센터(Central Infrasuructure)에 저장한다. 중앙인증센터는 전자서명 생성서비스, 전자서명 검증서비스, 인증서 유효성검증서비스, OTP 검증서비스 등을 제공한다.[18,19]

BankID의 서비스절차는 사용자가 전자금융서비스 사이트에 웹브라우

저를 통해 접속을 하고, 사용자 ID, 비밀번호, OTP의 순차적 입력을 통해 인증절차를 마친다. <그림 24> 참조

비밀번호는 중앙인증센터에 저장된 사용자의 개인키에 접근하기위한 용도로 사용된다.

그림 24 사용자 인증을 위한 입력화면

이후, 중앙인증센터에 전자서명을 요청하기 위한 절차도 사용자 인증절차와 비슷하다. 전자금융 거래내역에 대한 전자서명 요청시 ① 사용자가 웹브라우저를 통해 거래내역를 확인하고, ② OTP와 비밀번호를 입력하여 중앙인증센터에 전자금융 거래내역에 대한 전자서명을 요청한다. ③ 중앙인증센터에서 OTP 검증을 통해 사용자 인증을 수행하고, 전송된 비밀번호를 이용하여 사용자의 개인키를 복호화하여 전자서명을 수행 후 사용자에게 전송한다.[21]

BankID는 중앙인증센터에서 사용자의 인증절차를 거쳐 전자서명을 생성하는 PKI 서명센터 절차를 적용한 유일한 사례이다.

4. 항목별 검토결과

가. 적용성

검토항목	검토 우선순위	검토내용
적용 가능성	높음	• PKI 서명센터는 인증값 생성을 위한 별도의 추가적인 개발이 필요 없지만 전자서명을 위한 별도의 프로토콜을 수행할 모듈 개발이 필요 • 인증서 및 개인 키가 사용자PC가 아닌 서버에 저장되기 때문에 안전한 저장시스템 구축이 필요 • PKI 개인키를 사용자가 아닌 타 기관에서 보관하는 기술이므로, 적용 타당성에 대해 전자서명법.전자금융감독규정 등 법리적인 해석이 필요. ⇒ **추가 개발 및 법·규정 해석이 필요하므로 적용 가능성은 낮음**
적용 비용	보통	• 사용자의 인증서 저장, 전자서명 생성/검증, 강한 접속인증 등을 제공하는 PKI 서명센터의 구축 비용이 소요됨 • PKI 서명센터에 접근하기 위해 필요한 강한 접속인증을 제공하는 별도 인증매체의 배포에 따른 사용자의 발급비용이 발생 가능 ⇒ **매체 비용 및 센터 초기 구축 비용이 높은 수준으로 적용 비용 등급은 낮음**

<table>
<tr><td>기술 중립성</td><td>보통</td><td>• 사용자 전자서명 및 인증을 위한 별도의 plug-in 모듈이 필요하여, OS 및 플랫폼별 개발 기술에 연관됨
• 기존 PKI기술을 변형한 것으로 표준기술이 존재하지 않음
⇒ 순수 표준기술로만으로는 구현이 어려움</td></tr>
<tr><td>기존 인프라 활용성</td><td>낮음</td><td>• 현 인증서 발급기관인 공인인증기관을 활용 가능함
⇒ PKI 기술 인프라 활용이 가능하지만, OTP 검증 기능 등 추가 기능을 구현해야함</td></tr>
<tr><td colspan="2">적용성 검토결과</td><td>
<table>
<tr><th>분류</th><th>적용 가능성</th><th>적용 비용</th><th>기술 중립성</th><th>기존 인프라 활용성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>미흡</td><td>미흡</td><td>미흡</td><td>보통</td><td rowspan="2">미흡 (1.1)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

나. 편의성

검토항목	검토 우선순위	검토내용
소지 편의성	높음	• PKI 서명센터에 인증서를 저장하기 때문에 인증서에 대한 소지가 불필요하지만, PKI 서명센터 접근을 위해 부가적인 인증매체를 사용해야 하므로 소지의 불편함이 발생할 수 있음 **⇒ 인증매체를 소지해야 하므로 소지 편의성은 낮은 수준임**
사용 편의성	보통	• 現 공인인증서 사용방식과 크게 다르지 않아 사용상 불편함이 없으며, • 공인인증서를 PC에 저장하지 않고, 사용 시마다 PKI 서명센터에 접근하여 사용하므로 사용편의성이 크게 개선될 수 있음 • 다만, Active-X 등의 플러그인 모듈은 여전히 필요하며, PKI센터 접속을 위해 추가적인 인증매체를 사용하여야 하므로 이에 따른 편의성 저하가 발생할 수 있음 **⇒ 공인인증서 방식과 유사한 수준의 편의성이 보장됨**
관리 편의성	보통	• 공인인증서를 사용자 PC에 저장하지 않고, 안전하게 PKI센터에서 보관하므로 관리상의 문제가 발생할 확률이 다소 감소함 • 인증서의 도난·분실 등에 의해 타인에게 노출되지 않으며, 접속용 인증매체의 분실시 즉시 PKI센터 사용을 정지할 수 있음 • HSM과 동일하게 공인인증서가 여러 위치에 복제되지 않아, 관리 편의성이 우수함 **⇒ 도난 등에 즉시 대응 가능하여 관리 편의성은 우수함**

<table>
<tr><td>발급 편의성</td><td>낮음</td><td>• 現 공인인증서와 동일하게 여러 금융회사에 온라인으로 등록이 가능하므로 발급 편의성이 좋음
• 다만, 최초 1회 발급 시에는 대면확인이 필요하며, 접속용 인증매체의 발급/재발급/갱신 등의 관리 업무를 위해 추가적인 대면확인이 필요할 수 있음
⇒ 접속용 인증매체의 발급 등으로 편의성은 보통 수준임</td></tr>
<tr><td>교육 편의성</td><td>낮음</td><td>• 現 공인인증서와 동일하게 사용자 교육이 별도로 필요하지 않지만,
• 중앙 서명센터에 저장된 인증서에 접근하기 위해 별도의 모듈 설치가 필요하기 때문에 이를 악용한 악성코드의 설치가 가능하여 보안모듈 업데이트 등의 보안교육이 필요
⇒ 일반적인 보안교육이 필요하여 교육 편의성은 보통 수준임</td></tr>
<tr><td colspan="2">편의성 검토결과</td><td>
<table>
<tr><th>분류</th><th>소지 편의성</th><th>사용 편의성</th><th>관리 편의성</th><th>발급 편의성</th><th>교육 편의성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>미흡 (우수*)</td><td>보통</td><td>우수</td><td>보통</td><td>보통</td><td rowspan="2">보통 (1.9)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

*USIM OTP을 이용할 경우 별도의 매체를 소지할 필요가 없어 소지의 편의성이 우수함

다. 보안성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토된 내용</th></tr>
<tr><td>오프라인
공격에
안전</td><td>-</td><td>• HSM과 동일하게 공인인증서는 PKI센터에 외부로 유출되지 않으므로, 오프라인 공격에 안전
• 더욱이, 접속용 인증매체를 사용하므로 비밀정보 추측공격, 비밀정보 유출 등에 안전함
⇒ 비밀정보 추측공격, Phishing공격에 의해 사용자의 비밀정보 유출이 불가능하여 우수함</td></tr>
<tr><td>온라인
공격에
안전</td><td>-</td><td>• SSL, 서버인증서 등의 보안기능을 적용한 경우라도, 금융서버를 위장한 프락시 서버(Proxy Server)에 사용자가 부주의하게 접속하는 경우에는 MITM 공격이 가능할 수 있음.
• 하지만, 강한 사용자 인증기술(멀티팩터)을 이용하여, 중간자 공격에 대응이 가능함
⇒ MITM 공격 및 대응이 모두 가능하므로 보통</td></tr>
<tr><td>거래정보
변조 공격에
안전</td><td>-</td><td>• 거래정보 변조공격에 의해 원천적인 대응은 불가하지만, 부정거래가 발생한 경우 사용자PC에 저장되는 영수증에 포함된 전자서명을 검증하여 부정거래의 발생 유무를 확인할 수 있음
⇒ 부정거래 방지는 불가하나, 사후 탐지기 가능하므로 공격에 대응수준은 보통임</td></tr>
<tr><td colspan="2">보안성 검토결과</td><td>
<table>
<tr><th>분류</th><th>오프라인
공격에 안전</th><th>온라인
공격에 안전</th><th>거래정보 변조
공격에 안전</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>보통</td><td>보통</td><td rowspan="2">보통
(2.3)</td></tr>
<tr><td>검토
우선순위</td><td>- (1)</td><td>- (1)</td><td>- (1)</td></tr>
</table>
</td></tr>
</table>

제 5 절 바이오정보 인증기술

1. 기술소개

가. 배경

인터넷, 스마트 폰 등 IT기술을 활용한 다양한 통신서비스가 보편화됨에 따라서 원격지에서 접속한 사용자에 대한 신원확인이 필요한 온라인 서비스가 증가되었다. 특히, 온라인 서비스의 일례인 전자금융서비스는 개인의 자산과 관련이 있기 때문에 안전한 사용자 인증이 요구된다. 사용자 인증을 위한 기존의 비밀번호, IC카드 등과 같은 인증방식은 분실, 도난, 위조가 가능하다는 한계를 가진다. 이에 안전하고 휴대 및 이동이 편리한 바이오정보를 이용한 인증기술의 요구가 증가하고 있다.

나. 기술 개요

바이오정보 인증기술은 사람이 가지고 있는 고유한 바이오정보를 추출하여 사전에 인증시스템에 등록한 바이오정보와 비교하여 동일함을 결정함으로써 사용자를 인식하는 일종의 패턴인식(Pattern Recognition) 기술이다. 이와 같은 바이오정보 인증기술에 이용되는 바이오정보로는 <표 10>와 같이 크게 생물학적 바이오정보와 행동학적 바이오정보로 분류될 수 있다.

표 8 바이오정보의 분류

생물학적 바이오정보	행동학적 바이오정보
지문(Fingerprint)	서명(Dynamic Signature)
얼굴(Face)	
장문(Palmprint)	음성(Voice)
손모양(Hand Geometry)	키보드 입력(Key Dynamics)
홍체(Iris), 망막(Retina)	
정맥(Vein)	걸음걸이(Walking Style)

다른 인증기술과는 달리 바이오정보 인증기술은 사전에 바이오정보를 획득하고 등록하는 과정과 등록과정을 거친 바이오정보를 이용하여 사용자를 식별 하는 과정으로 나뉜다. 바이오정보 인증기술의 인증절차는 <그림 25>와 같다.

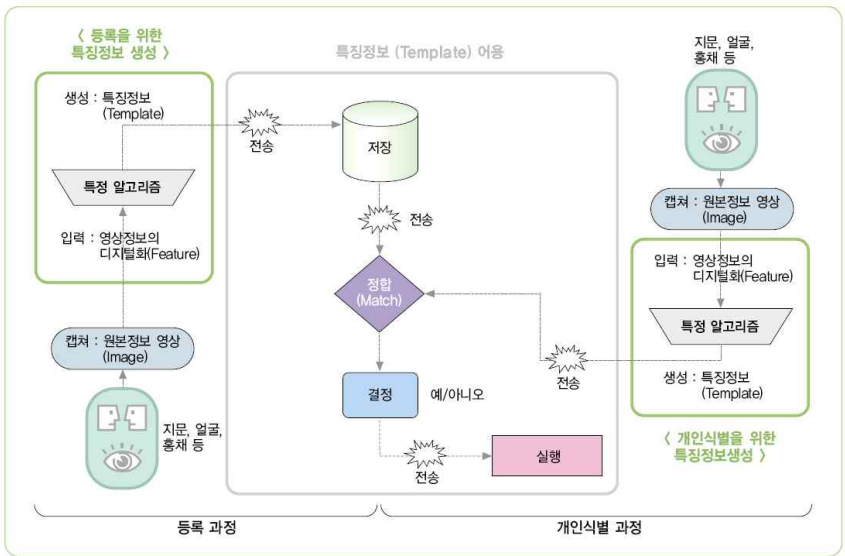

그림 25 바이오정보 인증기술의 처리절차[22]

< 바이오정보의 등록과정 >

① 바이오정보 인식장치를 통해서 바이오정보(지문, 홍채, 얼굴 등)를 입력

② 입력정보를 바이오정보 인식알고리즘을 이용하여 특징정보를 획득하여 바이오정보 템플릿(Tamplate)를 생성

③ 생성된 바이오정보 템플릿을 저장소에 저장

< 개인식별 과정 >

④ 개인식별이 필요할 경우, 바이오정보 인식장치를 통해서 바이오정보(지문, 홍채, 얼굴 등)를 입력

⑤ 입력받은 바이오 정보를 동일한 인식알고리즘을 이용하여 템플릿 생성

⑥ 생성된 템플릿과 저장소에 저장된 템플릿을 비교하여 인증여부 결정

이러한 바이오정보 인증기술은 사용자가 기억하거나 소지할 필요가 없으므로 분실 및 도난 등의 문제가 없고 복제가 어려워 비교적 높은 보안성 제공한다. 하지만 바이오정보 인증기술은 신원확인만이 가능하며 암호화, 무결성, 부인방지 등의 기능을 제공하지 않아 바이오정보 기술만으로는 전자금융서비스에 도입하기 어렵기 때문에 거래서명 및 부인방지 기능을 제공하는 다른 인증기술과 조합을 통해서 효과를 낼 수 있다.

바이오정보 인증기술은 바이오정보 인증을 서버에서 수행 방식과 사용자의 바이오정보 인증매체에 접근통제를 위한 방식의 두 가지로 구분할 수 있다. 서버에서 바이오 인증을 수행하는 방식은 바이오정보가 인터넷을 통해 노출될 위험이 존재하므로, 현재로서는 바이오정보의 전송이 필요 없는 사용자단의 인증매체 활성화 용도로 사용되는 것이 상대적으로 안전하다. 이에 본 연구보고서에서는 PKI 기술을 지원하는 보안토큰(HSM)과

보안토큰을 활성화하기 위해 바이오정보 인증기술을 연계한 인증기술을 하나의 예로써 검토한다. 조합된 인증기술의 개요는 보안토큰에 바이오정보 인식센서를 추가하여, 보안토큰의 개인키에 접근하기 위해 비밀번호 대신 바이오정보를 이용하는 것이다. 개인키에 대한 접근을 보안성이 낮은 비밀번호 대신 보안성이 높은 바이오인증으로 대체하고, PKI 기능을 이용할 수 있는 장점이 있다.

<그림 26>은 검토할 바이오정보 인증기술의 구성요소와 전자서명 생성 절차를 나타내고 있다.

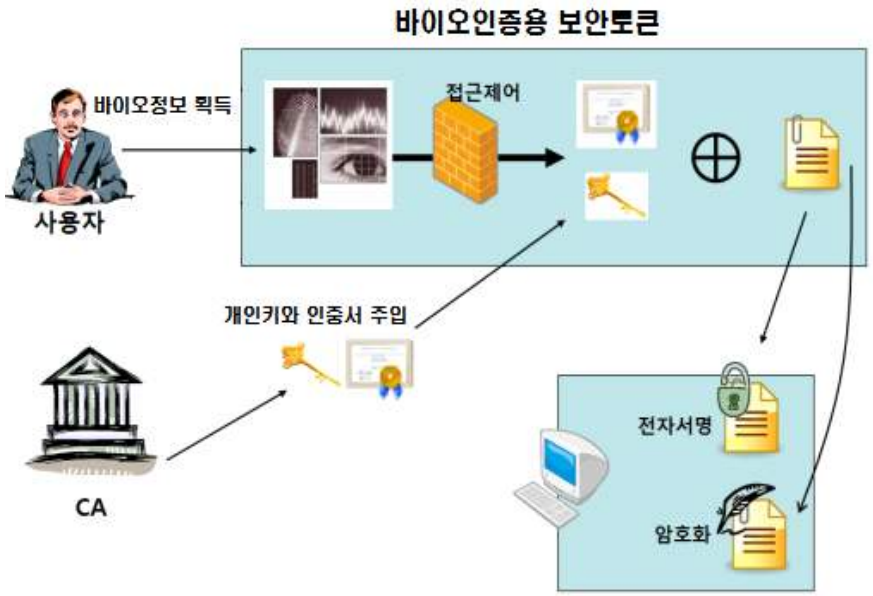

그림 26 바이오인증용 보안토큰 구조 및 사용 예

① 사용자는 바이오인증용 보안토큰을 발급받아, 바이오정보 인식센서를 통해서 자신의 바이오정보 템플릿을 등록

② 사용자는 CA로부터 인증서와 개인키를 발급받아 바이오정보용 보안토큰에 바이오정보 인증을 통해 저장

③ 이후, 전자서명을 생성하기 위해서는 사용자는 바이오인증용 보안토큰의 바이오정보 인식센서를 통해 바이오정보를 입력

④ 사용자로부터 입력된 바이오정보 템플릿과 바이오인증용 보안토큰에 저장된 바이오정보 템플릿을 비교하여 사용자 인증을 수행

⑤ 사용자 인증에 성공한 경우 바이오인증용 보안토큰에서 인증서와 개인키를 이용해서 전자서명 수행

⑥ 생성된 전자서명을 금융서버에 전송하여 서비스 이용

인증서와 바이오정보 템플릿을 분리하지 않고 바이오정보를 포함한 인증서를 이용하여 사용가능하고[23], 바이오정보 데이터 교환 규격*(Common Biometric Exchange File Format, CBEFF)의[24] 바이오정보를 포함한 속성 인증서를 만드는 표준이 연구되고 있어 향후에는 바이오인증서(Biometric Certificate, BC)가 사용될 것으로 보인다.

* 이기종간의 어플리케이션과 기기 등에서 수집한 지문, 얼굴, 홍체 등의 바이오정보를 교환하기위해 개발된 규격

2. 특징

가. 휴대 및 관리의 편리함

일상생활에서 널리 사용되고 비밀번호 등 사용자가 알고 있는 정보 또는 소지하고 있는 장치를 이용한 사용자 인증 방법은 분실 또는 도난의 사유로 관리적 보안 이슈가 발생할 수 있지만, 바이오정보 인증기술은 사용자만이 가지고 있는 고유한 바이오정보를 이용하는 것으로, 사용자가 기억하거나 소지할 필요가 없어 휴대가 용이하고, 분실 및 도난 등의 문제가 없어 타 인증기술에 비해 편리하다.

나. 복제의 어려움

바이오정보의 경우 그 사람만이 가지고 있는 행동학적, 생물학적 특징이기 때문에 다른 기술들과 비교해 복제가 비교적 어렵다. 바이오정보 인증기술 중 하나인 정맥 인식 기술의 경우 손등과 피부로부터 적외선 조명과 필터를 사용해 피부에 대한 혈관의 밝기 대비를 최대화한 다음 입력된 디지털 영상으로부터 정맥 패턴을 추출하는 기술이다. 적외선을 사용하여 혈관을 투시한 후 잔영을 이용해 신분을 확인하는 방식이기 때문에 복제가 거의 불가능하다.

3. 기술적 근거 및 적용사례

가. 기술적 근거

□ "Telebiometrics digital key framework – A framework for biometric digital key generation and protection"(ITU-T, 2008)

위 표준은 바이오 인식 정보에서의 정보획득 절차, 인증을 위한 정합 절차 및 키 생성 절차 등을 정의하며 전자서명 생성키에 대한 안전한 보호 및 추출 과정에 대해 제반 방법과 절차를 제시한다. 또한 바이오 인식 정보로부터 생성된 전자서명 생성키를 이용한 전자서명 등 응용 방법에 대해 제시한다.[25]

□ “Biometric Information Management and Security" (ANSI X9.84, 2001)

개인만이 고유하게 가지고 있는 지문, 홍채, 얼굴 패턴등의 바이오정보 데이터를 효율적으로 관리하고 안전하게 주고받기 위한 바이오인증

데이터의 구조와 바이오인증 데이터에 대한 최소보안 요구사항을 정의한 표준문서 이다.[26]

나. 적용 사례

바이오 인식 기술과 PKI 기술을 조합하여 적용된 사례는 조달청의 나라장터의 전자입찰 서비스에 도입한 지문인식 전자입찰 시스템이 대표적이다. [27]

나라장터는 조달청에서 운영하며 정부기관에 필요한 물자 구매와 공공분야 시설공사 계약 발주 등을 처리하는 국가종합전자입찰 시스템이다. 전자입찰시스템의 특성상 비대면 방식으로 진행되면서 인증서와 비밀번호만 있으면 전자입찰시스템에 참여할 수 있어 인증서 대여를 통한 불법 대리입찰을 통하여 부정입찰이 발생하기 시작했다.

이에 공인인증서 대여로 발생한 불법 전자입찰의 차단하기 위해 지문보안토큰*을 이용한 지문인식시스템을 도입 하였다.

* 지문인식 센서를 탑재한 보안토큰으로 기기내부에서 지문인식 센서를 통해 가입자의 지문정보를 입력받아 사전에 보안토큰에 저장된 지문정보와 비교하여 사용자 인증을 처리

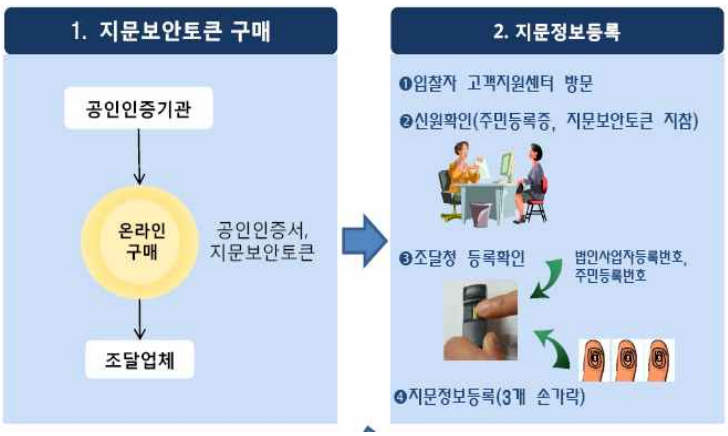

그림 27 지문인식 전자입찰 서비스 등록절차

<전자입찰 서비스 등록절차>

1. 지문보안 토큰의 구매

① 공인인증기관 홈페이지에 접속하여 공인인증서, 지문보안토큰을 온라인 구매

② 공인인증기관에서 지문보안토큰 수령증 발급

2. 조달청 지문등록

① 입찰자는 조달청의 대면확인 절차를 통해 신원확인 후, 지문보안토큰에 지문정보 등록 후, 등록된 지문정보의 정상 인식 여부를 확인

② 나라장터 홈페이지에 링크된 공인인증기관 또는 생산업체 홈페이지를 통해 법인용 및 개인용 공인인증서를 지문보안토큰에 복사

그림 28 지문인식 전자입찰 서비스 입찰참여 절차

<전자입찰 서비스 입찰참여 절차>

3. 지문보안토큰을 이용하여 전자입찰에 참가

① 나라장터의 전자입찰 사이트에 접속하고, 안내 화면에 따라 지문보안 토큰을 이용하여 시스템에 로그인

② 전자입찰서 작성하고, 지문보안 토큰을 이용하여 전자서명을 생성

③ 전자입찰 시스템에 제출하여 입찰에 참여

4. 항목별 검토결과

가. 적용성

검토항목	검토 우선순위	검토내용
적용 가능성	높음	• 바이오 정보가 보안토큰 활성화용(예, 지문인식 HSM)으로 사용되는 경우에는 금융회사의 전자금융시스템에 직접적인 변경은 없지만, • 바이오 정보를 보안토큰 등에 등록하는 업무 등을 금융회사에서 수행하여야 하는 경우에 대한 고려가 필요함. • 바이오 인증 표준기술을 사용하는 경우에는 멀티OS를 지원할 수 있으며, 멀티 플랫폼을 지원하기 위해서는 모든 플랫폼마다 지문 인식기 등의 인식 센서를 설치하여야 하여야 함 **⇒ 추가적으로 바이오 정보 등록업무, 인식센서 설치 등이 필요**
적용 비용	보통	• 바이오 정보의 등록, 폐기 등 관리를 위한 시스템의 구축비용이 발생 • 바이오 인식센서를 탑재하기 위한 비용 및 바이오인증 보안토큰의 배포 비용 등이 발생 **⇒ 관리 시스템 구축, 인식센서 장착, 보안토큰 발급 등 비용이 발생**
기술 중립성	보통	• 바이오 인식기술은 개인정보 보호를 위해 외부 시스템과의 연계 및 상호 운용성을 제한하여야 하므로 기술 중립성의 검토 필요성이 적음. • 다만, 보안토큰 활성화용으로 사용되는 경우에는 HSM 등과 동일하게 보안토큰 구동모듈이

<table>
<tr><td></td><td></td><td>부가적으로 필요하며, PKCS#11, #15 등의 관련 표준을 활용할 수 있음
⇒ 타 시스템과 연계 등이 제한적이어서 기술 중립성은 우수함</td></tr>
<tr><td>기존 인프라 활용성</td><td>낮음</td><td>• 공인인증서 발급 RA 등에서 신원 확인한 지문인식 HSM 등을 전자금융에 도입하여 즉시 사용 가능
• 만약, 지문인식 OTP 등 타 바이오 인증기술을 도입하는 경우에는 금융회사의 전 지점에서 바이오 센서를 설치해야 하며, 등록 시스템을 새롭게 구축해야 하는 등 기존 인프라의 활용이 불가함
⇒ 기존 인프라의 활용이 제한적으로 가능함</td></tr>
<tr><td colspan="2">적용성 검토결과</td><td>
<table>
<tr><th>분류</th><th>적용 가능성</th><th>적용 비용</th><th>기술 중립성</th><th>기존 인프라 활용성</th><th>종합 (검토수치)</th></tr>
<tr><td>검토결과</td><td>보통</td><td>미흡</td><td>우수</td><td>보통</td><td rowspan="2">보통
(2.0)</td></tr>
<tr><td>검토 우선순위</td><td>높음(3)</td><td>보통(2)</td><td>보통(2)</td><td>낮음(1)</td></tr>
</table>
</td></tr>
</table>

나. 편의성

검토항목	검토 우선순위	검토내용
소지 편의성	높음	• 보안토큰의 활성화용으로 사용되는 경우에는 보안토큰을 소지해야 하며, 경우에 따라 인식센서 장비를 소지해야 할 필요가 있음 • 그러나, 일반적인 바이오 인증기술은 자체로는 휴대가 불필요한 기술임 **⇒ 소지 편의성은 우수함**

사용 편의성	보통	• 직관적으로 바이오정보의 입력만을 요하기 때문에 사용 편의성은 높음 ⇒ **바이오인식을 통해 사용가능하므로 사용 편의성은 우수함**
관리 편의성	보통	• 바이오 정보는 신체의 일부분으로 구성되므로 복제 및 노출이 어려워, 특별한 관리가 필요하지 않음 • 다만, 일단 디지털화된 바이오 정보가 인터넷 등을 통해 유출되는 경우에는 정보의 회수 및 변경이 불가능해 주의가 요구됨 ⇒ **신체에 대한 특별한 관리가 요구되지 않음**
발급 편의성	낮음	• 최초로 바이오정보 등록 및 인증서 발급받는 때는 대면확인이 필요하고 이후 온라인 등록 등 절차간소화가 가능 ⇒ **대면 발급원칙으로 발급 편의성이 보통 수준임**
교육 편의성	낮음	• PIN 대신 바이오정보를 이용하기 때문에 비밀정보 관리를 위한 별도의 교육이 필요 없음 • 바이오정보의 노출시 위험이 크지만, 현재는 보안토큰의 활성화 용도로 사용되기 때문에 외부 노출에 안전하여 별도의 교육이 필요 없음 ⇒ **교육 편의성은 우수함**

편의성 검토결과

분류	소지 편의성	사용 편의성	관리 편의성	발급 편의성	교육 편의성	종합 (검토수치)
검토결과	우수 (미흡*)	우수	우수	보통	우수	우수 (2.9)
검토 우선순위	높음(3)	보통(2)	보통(2)	낮음(1)	낮음(1)	

*바이오정보 자체의 소지 편의성은 우수하지만, 보안토큰과 조합시 소지 편의성이 낮아짐

다. 보안성

<table>
<tr><th>검토항목</th><th>검토
우선순위</th><th>검토된 내용</th></tr>
<tr><td>오프라인
공격에
안전</td><td>-</td><td>• 바이오 정보가 서버에서 인증되는 경우에는 인증 프로토콜에서 재사용을 방지하는 기술 등을 반드시 사용하여야 안전함
• 바이오 정보를 보안토큰 활성화용으로 사용하는 경우에는 바이오 정보를 수집하는 것이 원천적으로 차단되어 안전함
• 보안토큰에 등록된 바이오정보는 내부에서만 사용가능하고 외부노출이 불가능하여 노출에 안전함
⇒ 비밀정보 추측공격, Phishing공격에 의해 사용자의 바이오 정보 유출이 불가능하여 우수함</td></tr>
<tr><td>온라인
공격에
안전</td><td>-</td><td>• MITM 공격을 대응하기 위해 SSL/TLS와 같은 보안 기술을 필수적으로 사용해야하고,
• 반드시 SSL/TLS상에서 사용자 인증을 수행하도록 설정이 필요
⇒ SSL/TLS와 같은 추가적인 보안기능이 필요하므로, 보통 수준임</td></tr>
<tr><td>거래정보
변조 공격에
안전</td><td>-</td><td>• 거래정보 변조공격에 대한 대응이 불가능함
• 거래연동 인증기술 등의 추가 보안기술과 연계하여 공격에 대응할 수 있음
⇒ 부정거래 방지가 불가능함</td></tr>
<tr><td colspan="2">보안성 검토결과</td><td>
<table>
<tr><th>분류</th><th>오프라인
공격에 안전</th><th>온라인
공격에 안전</th><th>거래정보 변조
공격에 안전</th><th>종합
(검토수치)</th></tr>
<tr><td>검토결과</td><td>우수</td><td>보통</td><td>미흡</td><td rowspan="2">보통
(2.0)</td></tr>
<tr><td>검토
우선순위</td><td>- (1)</td><td>- (1)</td><td>- (1)</td></tr>
</table>
</td></tr>
</table>

제5장

결 론

제 1 절 新인증기술 검토결과 요약

본 연구보고서는 현재까지 국내 전자금융에 도입되지 않은 新인증기술을 대상으로 금융회사에서 도입 검토시 활용할 수 있는 검토항목과 검토방법을 제시하였다. 본 연구보고서에서 제시된 인증기술의 3가지 검토항목은 다음과 같다.

- 적용성: 스마트폰, IPTV 등 새로운 전자금융환경에 적합한 인증기술인지 여부에 대한 4가지 세부 검토항목* 제시
  * 적용 가능성, 적용 비용, 기술 중립성, 기존 인프라 활용성

- 편의성: 휴대 및 이용이 간편하고, 언제 어디서든지 쉽게 이용할 수 있는 인증기술인지 여부에 대한 5가지 세부 검토항목* 제시
  * 소지, 사용, 발급, 관리, 교육 편의성

- 보안성: 지속적으로 발전하는 신규 해킹기술에 대응하여 부정거래를 방지하는데 효과적인지 에 대한 3가지 세부 검토항목* 제시
  * 오프라인 공격대응, 온라인 공격대응, 거래조작 공격대응

이미 많은 금융회사에서는 새로운 인증기술 또는 보안제품의 도입시 보안성 이외에도 금융회사의 비용효과인 적용성과 사용자 비용인 편의성을 동시에 고려하고 있다. 본 연구보고서는 이러한 금융회사의 검토항목을 명시적으로 정의하며, 실제 도입 검토시 활용할 수 있도록 세부 검토항목과 구체적인 검토방법을 제시하였다.

본 연구보고서에서는 국내외에 소개된 다양한 인증기술 중에 국내의

새로운 전자금융환경에 적용이 가능한 5가지 新인증기술을 선정하였고, 제시된 검토항목 및 검토방법을 이용하여 내·외부 전문가와 공동으로 검토를 실시하였다. 선정된 5가지의 新인증기술 검토결과를 기반으로 각 인증기술의 종합적인 분석결과는 다음 표 8와 같다.

표 8 선정기술 新인증기술의 비교

항목 / 인증기술	적용성	편의성	보안성
USIM기반 모바일OTP	우수	우수	보통
거래연동 인증기술	우수	보통	우수
이상거래 탐지기술	보통	우수	미흡
PKI 서명센터	미흡	보통	보통
바이오정보 인증기술	보통	우수	보통

마지막으로 선정된 5가지 新인증기술을 금융회사에서 도입하고자 하는 경우 추가적으로 고려해야 할 사항들을 살펴보면 다음과 같다.

- **USIM 기반 모바일 OTP**: OTP발생기의 휴대 편의성이 매우 높고, 現 USIM의 제한된 용량으로 전 금융회사의 통합 서비스가 필요함.
  (단, 대상 고객이 전체 휴대폰 사용자의 30% 이내로 한정됨)

- **거래연동 인증기술**: 전자금융 부정거래를 원천적으로 차단하여 보안성이 매우 높으나, 거래연동 OTP발생기의 발급비용 발생과 휴대편의성이 다소 낮음.
  (단, USIM 기반 모바일 OTP로 구현이 가능하여 편의성을 높일 수 있음)

- **이상거래 탐지기술** : 각 상황별 이상거래 사실에 기반하여 추가적인 인증을 제공하여 사용자의 편의성과 보안성을 균형 있게 유지할 수 있음. 특히, 사용자의 거래패턴 프로파일을 금융회사 간에 연계하는 경우 보안효과가 매우 높아짐. 다만, 초기 구축비용이 높음.

- **PKI 서명센터** : 공인인증서의 도난을 방지할 수 있는 기술로 새로운 전자금융 환경에서도 공인인증서 기반의 부인방지를 제공할 수 있음. 다만, PKI 서명센터에서 사용자를 대신하여 전자서명을 생성하기 때문에 불공정한 부인방지라는 평가가 있어 도입시 법적 해석이 필요

- **바이오정보 인증기술**: 바이오정보를 통해 인증하므로, 타인에 의한 인증정보의 오남용이 원천적으로 방지됨. 다만, 개인정보의 노출, 재사용 방지 등을 위해 타 보안프로토콜과 연계가 필요하고, 타인의 위협에 의한 거래승인 등의 부작용이 발생 가능함.

제 2 절 결론

2009년 말부터 거세진 스마트폰 열풍은 전자금융환경에도 큰 변화를 예고하고 있다. 기존의 전자금융환경은 유선전화, 휴대폰, PC 등의 채널에 한정되어 있어 일률적인 인증기술의 적용이 가능하였다. 하지만, 스마트폰, 스마트패드, IPTV 등 다양한 전자금융환경을 제공해야 하는 상황에서는 다양한 환경에 적합한 新인증기술의 요구도 점점 커지고 있다. 본 연구보고서는 이러한 환경에서 금융회사가 新인증기술을 도입하고자 하는 경우 참고할 수 있는 검토사항을 제공하기 위해 작성되었다. 본 연구보고서의 검토결과는 다음과 같다.

첫째, 새로운 전자금융환경에 적합한 **新인증기술은 보안성만을 강조하기 보다는 다양한 환경에 적용이 가능하고, 쉽고 편리하게 이용될 수 있는지에 대한 복합적인 검토가 필요**하다. 따라서, 본 연구보고서 에서는 新인증기술의 검토항목을 적용성, 편의성, 보안성의 3가지 검토항목으로 분류하여 검토하는 방법론을 제시하였다.

둘째, 국내외에 소개된 다양한 인증기술 중 5가지 新인증기술을 선정하여 검토한 결과,

- (적용성)금융회사에서 쉽게 적용할 수 있는 新인증기술로는 **USIM기반 모바일 OTP와, 거래연동 인증기술**이 기존 금융회사의 인프라 등을 활용하여 쉽게 적용이 가능하며,

- (편의성)사용자의 편의성 측면에서는 보안매체를 소지할 필요가 없는 **USIM기반 모바일OTP, 이상거래 탐지기술, 바이오정보 인증기술** 등이 우수한 것으로 분석되었다.

- (보안성)보안성 측면에서는 대부분의 新인증기술이 현재 수준의 보안 위협에는 대응이 가능한 것으로 분석되었다. 추가적으로 **거래연동 인증기술**은 MITB(Man In The Browser), 메모리 해킹 공격등의 거래변조 공격에도 대응이 가능하여 보안성이 우수한 것으로 분석되었다.

셋째, 검토결과에 대한 활용방안으로 **모든 검토항목을 완벽하게 만족하는 인증기술은 찾을 수 없었으며, 각각 장단점이 있어 2가지 이상의 인증기술을 조합하여 사용하는 것이 효과적인 것으로 분석**되었다. 이에 따라 조합이 가능한 보안기술을 예로 들자면,

- (1)USIM기반 모바일OTP와 거래연동 인증기술을 조합하는 경우 적용성, 편의성, 보안성이 모두 우수한 인증기술이 되어 새로운 전자금융환경에 도입시 효과적이다.

- (2)이상거래 탐지기술은 편의성 측면에서 매우 우수하지만, 보안성이 낮아 2채널 인증, 거래연동 인증기술 등을 조합하여 적용하는 경우 효과적이다. 특히, 이상거래를 탐지한 경우 거래를 중단시키는 것 보다 조합한 인증기술을 추가로 요구하도록 하여 적용성과 보안성을 향상시킬 수 있다.

- (3)바이오 인증기술은 해당 기술 자체로는 적용성과 보안성이 보통수준이지만, 타 인증매체의 활성화를 위해 사용될 경우에는 해당 사용자 이외에는 사용할 수 없는 인증매체가 되어 보안성이 크게 향상된다. 즉, HSM, OTP 등의 인증매체의 접근통제용 PIN 입력 대신 사용하는 경우 보안성이 향상되며, 여권, 전자주민증과 같이 스마트카드와 조합하는 것도 효과적이다.

참고 문헌

[1] 한국은행, “2010년 3/4분기 국내 인터넷뱅킹서비스 이용현황”, 10 2010.
[2] 금융감독원, 전자금융감독규정, 2010. 06.
[3] 방송통신위원회, ‘전자금융거래 인증방법의 안전성 가이드라인’ 확정, 2010. 05.
[4] CA technologies, Managing Strong Authentication: A Guide to Creating an Effective Management System, 2007.
[5] 금융결제원, “공인인증서 의무사용 규제완화 관련 주요이슈 및 현황”, 2010. 07.
[6] D.Dolev and A.C.Yao, "On the Security of Public Key Protocols", Proc. IEEE 22nd Ann. Symp. Foundations of Computer Science.
[7] Hiltgen, A., Kramp, T. and Weigold T., "Secure Internet Banking Authentication", IEEE Security & Privacy, March/April 2006.
[8] NIST SP800-63-1, "Electronic Authentication Guideline", December 2008.
[9] MasterCard Inc., Chip Authentication Program - Function Architecture, 2004. 09.
[10] IBM, "The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks", 2008.
[11] Giesecke & Devrient, http://www.gdai.com/pls/portal/Master%20OTP%20Final.pdf
[12] Gemalto, http://www.gemalto.com/brochures/download/mobile_id.pdf
[13] Gartner, Transaction Verification Complements Fraud Detection and Stronger Authentication, 2006. 09.
[14] Gartner, Where Strong Authentication Fails and What You Can Do About It, 2009. 12.
[15] Entrust, Defeating Man-in-the-Browser, 2010. 03.
[16] D. M'Raihi, S. Boeyen, M. Grandcolas, S. Bajaj, "Sharing Transaction Fraud Data", RFC5941, August 2010.
[17] K.J. Hole, V. Moen, and T. Tjøstheim, “Case Study: Online Banking

Security," IEEE Security and Privacy, January 2009.

[18] K.J. Hole, V. Moen, and T. Tjøstheim, "Risk Assessment of a National Security Infrastructure" IEEE Security and Privacy, January 2009.

[19] Y. Espelid et al., "A Proof-of-Concept Attack against Norwegian Internet Banking Systems," Proc. 12th Int'l Conf. on Financial Cryptography and Data Security (FC08), LNCS, 2008.

[20] K. J. Hole, T. Tjøstheim, V. Moen, L.-H. Netland, Y. Espelid, and A. N. Klingsheim. Next generation internet banking in Norway. Technical Report 371, Department of Informatics, University of Bergen, February 2008.

[21] Kristian G., "Weaknesses in BankID, a PKI-substitute Deployed by Norwegian Banks", LNCS, June 2008.

[22] 바이오인식정보시험센터, 바이오정보보호 가이드라인 해설서, 2007. 09.

[23] S.Santesson, M.Nystrom, T.Polk, Internet X.509 Public Key Infrastructure:Qualified Certificates Profile, RFC3739, March 2004.

[24] Fernando L. Podio, Jeffrey S. Dunn, Lawrence Reinert, Common Biometric Exchange Formats Framework, NIST April 2004.

[25] Telebiometrics digital key framework (TDK) – A frameworkfor biometric digital key generation and protection,Recommendation ITU-T X.1088, May 2008.

[26] Biometric Information Management and Security for the Financial Services Industry, ANSI X9.84, 2003.

[27] 조달청 나라장터, http://www.g2b.go.kr/

이 연구보고서 작성을 위해 다음 분들께서 수고하셨습니다.

2011년 3월

총괄책임자	금융보안연구원	본부장	강우진
참여연구원	인증기술팀	팀장	심희원
		선임연구원	김진형
		주임연구원	김근옥
		주임연구원	송성현
		인턴	김수정
외부전문가	우리은행	차장	전유승
	현대증권	과장	김형림
	고려대학교	교수	임종인
	국민대학교	교수	이옥연
	세종대학교	교수	권태경
	ETRI	팀장	진승헌
	KISA	팀장	강필용
	MCurix	사장	박현주
	KT	차장	김상곤
	LG U+	차장	정성엽
	SKT	매니저	이응주
	미래테크놀러지	사장	정균태
	이니텍	상무	김기영
	AT솔루션	상무	홍성렬

전자금융 新인증기술 연구보고서

2011년 3월 인쇄

2011년 3월 발행

발행인 : 곽 창 규

발행처 : 금융보안연구원
서울시 영등포구 여의도동 36-1
키움파이낸스 스퀘어 빌딩 15층
Tel: (02) 6919-9114

인쇄처 : 현대기획(TEL : 02-2263-7084)

<비 매 품 >