IT Shared Service 운영 환경에서 USIM 을 활용한 통합 인증에 관한 연구

김재흥
고려대학교 컴퓨터정보통신공학과 디지털정보미디어공학과
e-mail : ilovmt@gmail.com

A Study on USIM based Integrated Authentication in IT Shared Service Environment

Jae-Heung Kim
Dept. of Digital Information & Media Engineering ,
Graduate School of Computer & Information Technology, Korea University

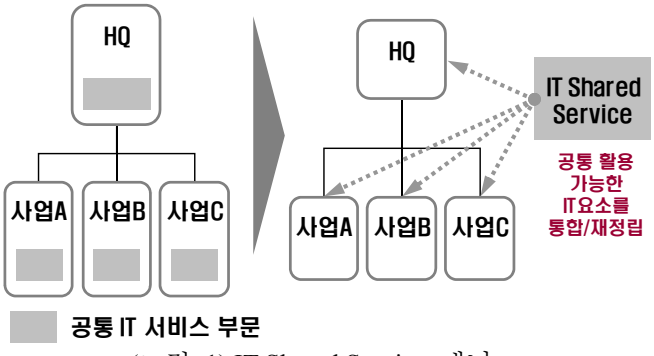
요 약

글로벌 기업은 공통 활용 가능한 IT 요소를 통합/재정립하여 비즈니스 전략을 효과적으로 지원하기 위한 IT Shared Service(이하 ITSS) 체계로 전환하고 있다. IT 자원은 통합되고 업무는 네트워크 기반의 가상화된 서비스로 제공되며, 모바일 중심의 개인 업무 환경으로 전환되고 있다. 본 논문은 상용화된 보안 인증 방식 중 ITSS 운영환경에 적합한 방식을 검토하고, 문제점 및 취약점을 찾아 개선 방안을 도출하고자 한다. 특히, 모바일 환경이 급속도로 확산되는 추세에서 USIM 을 활용한 인증 방식이 기업의 보안 요구사항을 충족 시킬 수 있는지 집중 검토하고자 한다.

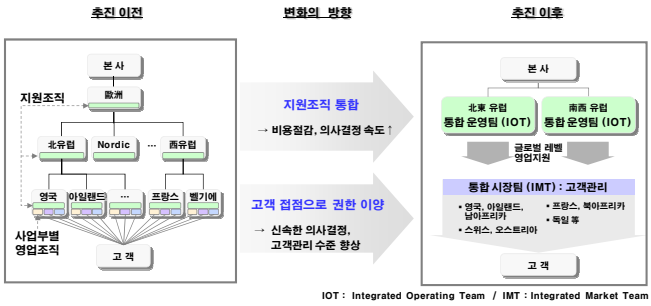
1. 서론

기업의 IT 복잡도 증가에 따라 IT 환경의 구조개선이 필요하며, 기간 시스템 글로벌화에 따른 유연한 IT 운영체계가 요구되고 있다. 이에 따라 많은 글로벌 기업들이 IT 감량 경영을 통하여 기존 운영 비용을 혁신투자 비용으로 전환하여 미래 성장 기반을 확보하고자 IT 서비스 체계를 혁신하고 있다. 기업의 비즈니스 전략을 효과적으로 지원 할 수 있는 서비스 체계 중 하나가 IT Shared Service 체계이다.

ITSS 는 기업의 여러 사업 조직에 각각 존재하던 유사/공통 업무를 하나로 통합하여 (그림 1)과 같이 별도의 핵심 서비스 조직으로 운영함으로써, 사업조직은 전략적 활동에 집중하고, 지원이나 운영 또는 비 전략적 활동은 Shared Service 조직에 위임함으로 전문성을 극대화하는 조직 체계를 의미한다.

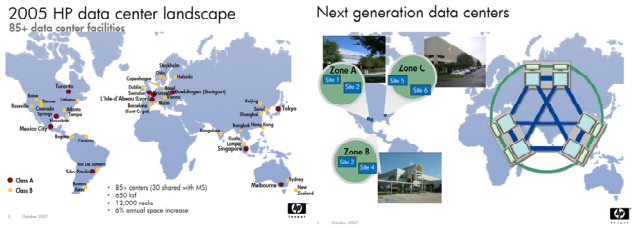


(그림 1) IT Shared Service 개념



(그림 2) ITSS 적용 사례 (IBM)

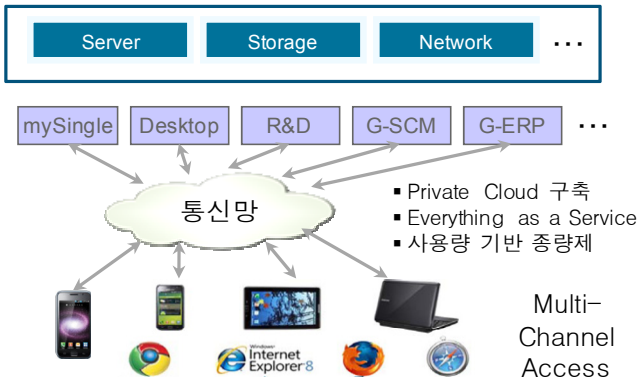
(그림 2)은 IBM(社)의 ITSS 적용 사례로 지원 조직을 통합함으로 비용 절감과 의사 결정 속도를 제고하였고, 고객 접점으로 권한을 이양하여 고객 관리 수준을 향상하여 현지 대응력을 강화 하였다.



(그림 3) Data Center 변화 (HP)

(그림 3)는 29 개국의 85+개가 넘는 Data Center 를 3 개 지역의 상호백업을 고려한 6 개 Data Center 로 IT

자원을 통합한 HP(社)의 사례이다.



(그림 4) IT 인프라 Shared Service 개념도

(그림 4)는 인프라 관점에서 Shared Service 가 적용된 개념도로, IT 인프라 자원은 Data Center 로 통합 운영되고, 업무 시스템은 Global One Instance 개념의 소프트웨어 서비스로 통합되며, 무중단 통신망 기반의 가상화된 인프라나 플랫폼 서비스가 제공되며, 유무선 통신망이 확산 되어 모바일 업무 환경이 급속히 개선 되고 있다. 또한, 스마트폰이 업무 전반에 걸쳐 활용 될 것이다.

개인 인증 과정을 완료하기 위해 기본적으로 개인정보(이름, ID, 주민번호 등)가 서비스 제공자에게 등록/관리 되어야 한다. 서비스와 접속 채널이 다양화 됨에 따라 관리 되는 개인 정보 역시 서비스 제공 형태별로 다원화 되어 관리 되어 지고 있다. E-mail 서비스를 PC 로 접근할 때와 스마트폰으로 접근할 때의 인증 방법이 상이하다. 본 논문에서는 서비스별로 관리되는 개인정보에 대하여 서비스 상호간에 동일성을 보장할 수 있는 인증 방식을 연구하고자 한다.

2. ITSS 운영 환경에서 USIM 을 활용한 보안 인증

사용자가 서비스를 사용할 때마다, 매번 서비스 제공자가 요구하는 인증 과정을 거쳐야 하며, 식별자와 인증 방법이 분산된 환경에서 임의의 공격에 의해 서비스 중단, 기업 정보 유출/훼손, 고객 정보 유출, 법/규제 등 컴플라이언스에 중점을 둔 보안 요구사항에 대응 해야만 한다. 관련된 보안 요구사항을 <표 1>에 정리 하였다. [1]

<표 1> Technical Requirements for Authentication

구분	요구사항	주요 기술
통합 식별 체계	데이터와 음성, 유선과 무선, 통신과 방송이 통합되는 BcN 환경에서 사용자, 망 및 서비스 요소들을 식별, 인증을 위해 사용되는 식별 체계	인터넷 주소자원, NGN 식별체계
유무선 통합	서비스 이용자가 망 종류에 관계없이 일관되고 끊김이 없는 서비스를 받을 수 있는 유무선 통합 네트워크	Vertical Handover, All IP 기반 이동성 지원 기술
ID 관리	인증정보를 비롯한 개인의 특징, 신상정보, 선호도와 같은 ID 의 생성부터, 변경, 유통, 폐기 등에 대한 관리 기술	식별자 체계, 보안토큰관리, Identity Ontology, Identity Sharing, Assurance
개인정보보호	사용자의 개인정보를 보호하기 위한 기술 및 정책	개인정보보호정책, 단말 개인정보관리, Interaction Service
암호 인증 권한	다양한 정보에 대해 안전하고 신뢰성 있게 전송 및 이용하기 위한 기반 기술	암호, 인증, 권한 관리

인증은 어떤 사람이나 사물이 실제로 신고된 그 사람(사물)인지를 판단하는 과정이다. 통상적으로 아래와 같은 인증요소를 2 개 이상 결합하여 사용하고 있으로 관련된 보안 취약점을 <표 2>로 정리하였다. [2]

<표 2> 인증 요소별 보안 취약점

구분	내용	취약점
인증서	개인키와 공개키에 기반하여 인증	개인키 및 인증서 유출
IP-지리위치	할당된 IP 와 지리적 위치로 식별	이동성 지원 불가
핑거 프린트	사용자 시스템의 프로파일로 식별	인식오류
ID/PW	대표적 개인 인증 수단으로 암기에 기반하여 식별	복잡성과 주기적 갱신에 취약
Out-of-Band	전화 응답, e-mail, SMS 를 이용하여 OTP 로 식별	통신 채널 침해 용이
OTP	하드웨어 토큰을 사용	짧은 시간 프레임 동안 해킹

기술적 측면과 보안 및 상호운영성 측면에서 보면 클라이언트 SW 없는 토큰방식의 공인인증서 방식이 가장 우수한 것으로 분석되었다. 여기에 HW 기반의 OTP 방식을 적용한 인증 방식인 금융결제 시스템이 현재 적용된 가장 강력한 인증 방식로 국제적으로도 통용되는 기술이며, 아래의 보안 기술이 적용 된다.[3]

- 인증/기밀성/무결성/부인방지 서비스
- 웹 기반의 클라이언트-서버 환경의 보안 기술
  - HTTP (Hyper Text Tramsfer Protocol)
  - SSL (Secure Socket Layer)
  - SSL 보안 프로토콜에서의 서버인증서
- 클라이언트 인증
  - 패스워드 기반
  - 인증서 기반(인증 및 부인 방지 서비스)
- 전자 서명과 OTP

객관적인 안정성을 확인하기 위해 몇 가지 통계와 인증 방식의 특성들을 비교 검토하였다.

<표 3> 주요 국가별 인터넷뱅킹 사고 규모

국가	기간	사고 금액	보안 수단	출처
한국	' 08년	1.5억원(총8건)	암호통신 + 보안카드(OTP) + 공인인증서	' 09년 국정감사 자료 (금융감독원 제출)
	' 09년 1~8월	2.3억원(총14건)		
미국	' 09년 3분기	약 1,352억원	SSL(암호통신) + OTP	미국 FDIC의 RSA Conference발표 자료(' 10년 3월) FDIC: Federal Deposit Insurance Corporation
영국	' 08년	약 900억원	SSL(암호통신) + OTP	UK Payment http://www.banksafeonline.org.uk/faqs/faqs_13.html
	' 09년 상반기	약 664억원		Financial Fraud Action UK 보도자료('09.10.7)

국내 인터넷뱅킹의 거래 규모는 일평균 29 조 4,577 억원 (일 평균 건수 2,800 만건)이며, <표 3>의 인터넷 뱅킹 사고 규모를 보면, 국내는 연간 3 억원 미만 수준에 불과하다. 국내의 공인인증 방식이 적용 시 미국과 영국 대비 신뢰성이 보장됨을 알수 있다.[4]

<표 4> 인증서 방식의 보안 취약점

취약점	대응방안
플러그인 설치에 앞서 서버가 내려주는 플러그인이 그 서버의 위험성을 유저에게 알려줄 가능성이 없음 (HTTP + Plugin 방식의 문제점)	웹브라우저 내장 모듈로 클라이언트 인증(인증서기반)을 통하여 접속
SSL + OTP 는 부인방지 기능의 약화	인증서
복수 이용자가 사용하는 컴퓨터에 저장된 공인인증서는 모든 유저의 계정에서 접근 가능	보안토큰, USIM 등 저장 매체 사용
인증서 암호는 기존 이메일, 블로그, 포털 로긴 등에 입력하는 암호와 대부분 일치	OTP

현재 사용되는 공인인증서는 대부분 PC 하드디스크나 USB 메모리에 공인인증서를 보관하여 사용하고 있다. 이에 따라, 공인인증서 개인키 유출과 같은 보안 취약점이 존재하며, 모바일 업무에 대한 지원이 부족한 상황이다. 이와 관련된 문제점들을 <표 4>에 정리 하였다.

대부분의 기업과 해외에서는 SSL+OTP 방식의 인증 방식으로 사용하고 있으나, 부인 및 변조 방지 그리고 감사 기능이 필요한 시점에서 부인 방지의 검증이 어려운 SSL+OTP 는 ITSS 환경의 인증 체계로 적용하기에는 한계가 있다. <표 5>은 구축 방식에 따른 특성들을 비교한 자료이다.

<표 5> 공인인증서 vs. SSL+OTP 방식 비교

구분		공인인증서 기반	SSL+OTP
구축방식		사용자PC에 별도 보안프로그램 설치	웹 서버에 SSL인증서 설치
제공기능	사용자 인증	○	○
	전자 서명	○	×
	데이터 암·복호화	○	○
	데이터 무결성	○	○
보안성	부인방지기능	○	×
	Replay 공격	양호	양호
	MITM 공격 (Man In The Middle)	양호	△ (시간 오차범위 또는 이벤트 오차범위 내 인증가능)
활용성		전자서명을 이용하는 다양한 분야에 적용가능	서버인증 및 통신데이터 암호화 수단

업무 처리 방식이 PC 에서 스마트폰 중심의 이동중에 있으며, 기업 정보 시스템에 접속하는 채널이 다양화 되고 있다. <표 6>는 Gartner 에서 전망한 스마트폰 시장 규모이다.[5]

USIM (Universal Subscriber Identity Module)은 가입자 정보를 탑재한 SIM(Subscriber Identity Module) 카드와 UICC (Universal IC Card)가 결합된 형태로써 통신 인증 기능 외에 전자상거래 등 다양한 기능을 1 장의 카드에 구현한 것이며, 3 세대 이동통신(WCDMA)의 단말기에 기본적으로 탑재된다. USIM 은 현재까지 나온 가장 안정적인 저장매체로 공인인증서를 스마트폰의 USIM 에 저장하여 웹브라우저를 활용하는 인증 방식이 가장 안정적인 구성이라고 할 수 있다.

<표 6> 국제 스마트폰 시장규모 및 점유율 전망

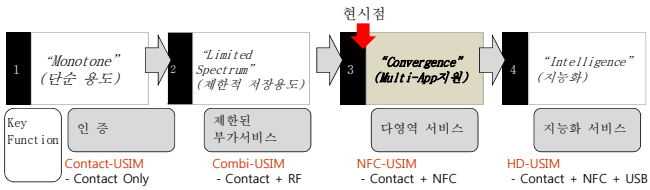
구분	2005	2006	2007	2008	2009	2010(e)	2011(e)	2012(e)
점유율 (%)	6.6	8.3	10.6	11.7	15.6	22	31	39.9
시장규모 (만대)	5,373	8,179	12,244	14,456	19,082	29,499	44,688	61,924

USIM 기술은 하드웨어, 인터페이스, 플랫폼, 소프트웨어 영역으로 <표 7>과 같이 구분된다.

<표 7> USIM 관련 기술

항목	내용
하드웨어	RISC(Reduced Instruction Set Computer) 프로세서 ROM(Read Only Memory): 운영체제 탑재 RAM(Random Access Memory): 응용프로그램 구동 응용프로그램과 사용자 데이터 저장을 위한 EEPROM(Electrically, Erasable and Programmable Read Only Memory) 플래시 메모리를 적용한 대용량 메모리 NFC(Near Field Communication)
인터페이스	IC-USB(Inter Chip USB), BIP(Bare Independent Protocl) ISO/IEC 7816, SWP(Single Wire Protocol)
플랫폼	자바 카드 3.0 MULTOS 등 개방형 플랫폼
소프트웨어	SCWS(Smart Card Web Server) : USIM 의 서비스 접근 및 확장 지원

통신, 금융, 방송 등 다영역 서비스가 급속도로 융합되는 환경에서 소형 컴퓨터의 기능을 갖춘 USIM 은 기존의 저장매체와는 다르게 복제가 거의 불가능하고 대용량 정보 저장과 데이터 처리가 가능하며 (그림 7)과 같이 발전하고 있다.[6]



(그림 7) USIM 발전과정

또한, 독립된 유무선 네트워크들을 연동하여 끊김없이 서비스가 제공되기 위해서는 인증 및 권한부여, 과금 정보가 통합 관리되어야 하며, 서비스별로 상호 연동 되어야 한다. 이에 따라, 사용자와 단말장치 프로파일은 서비스의 원활한 제공에 필수적인 부분으로 통합 및 표준화된 관리가 필요하다. [7]

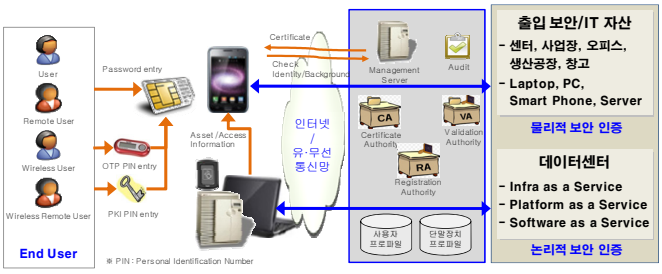
적법한 사용자 및 장치 식별과 전송 정보의 무결성 보장하는 인증 기술을 정리하면 <표 8>과 같다.

<표 8> 상용화된 인증 기술

항목	내용
USIM 등 모바일 환경에서의 인증서비스 모델 및 인증 기술	USIM 칩이 탑재된 스마트폰, 3G 폰 등의 보급 확대에 따라, 모바일 환경에서 인증서 기반의 다양한 인터넷 서비스 이용을 위한 USIM 기반의 인증서비스 이용 모델 및 관련 기술에 대해 정의
인터넷 전화 등에 이용가능한 디바이스 인증 기술 및 응용	인터넷 전화기, CCTV, 휴대단말기, 지능형 가전 등 네트워크에 참여하는 디바이스에 대한 신뢰된 인증 서비스를 제공하기 위한 기술
일회용패스워드(OTP) 인증 기술 및 응용	일회용 패스워드(OTP) 보안 서비스 제공을 위한 암호키 관리 및 정책 요구사항, 배포 절차 및 요구사항, 인증 보증레벨 등 OTP 인증기술 및 응용에 대해 정의
일회용패스워드(OTP) 인증 프레임워크	OTP 인증 기본 모델, 통합인증 모델, 대체인증서버가 있는 통합인증 모델, 센터간 통합인증 모델 등 총 4개 인증 서비스 모델을 포함하는 OTP 인증 서비스 프레임워크를 정의
익명성을 보장하는 인증 기술	웹사이트 가입, 성인인증 등 개인의 실명이 필요 없는 곳에서 프라이버시 보장을 위해 가명 또는 익명을 사용할 수 있도록 보장하면서 익명성 남용을 방지하기 위한 기술
바이오정보를 이용한 전자서명 기술	기존 공개키 기반의 전자서명 기술에서의 단점을 보완하기 위해 지문, 홍채 등 바이오 정보를 포함한 전자서명 인증 기술 및 이용 효율성 제고를 위한 융합 기술 등 정의

공인인증서 방식의 취약점에 대응하고, 사용자 프로파일을 통합 관리하고, 모바일 환경 변화에 적절히 대응 할 수 있는 환경을 구성하기 위하여, 인증서의 PC 하드디스크 저장을 제한하고, 개인키 유출을 원천적으로 봉쇄할 수 있는 스마트폰의 USIM 에 개인인증서를 저장하여 인증서 기반의 인증 서비스를 적용하는 것이 필요하다.

이미 아이폰 환경에서 공인인증서 호환성을 확보하여 인증서 기반의 스마트폰 결제 서비스가 적용 되어 있어, 기업시스템에 적용하기에 문제가 없다. (그림 8)은 스마트폰의 USIM 을 이용한 인증서비스를 기업환경에 적용하도록 개념화 하였다.



(그림 8) USIM 을 활용한 인증 서비스 개념

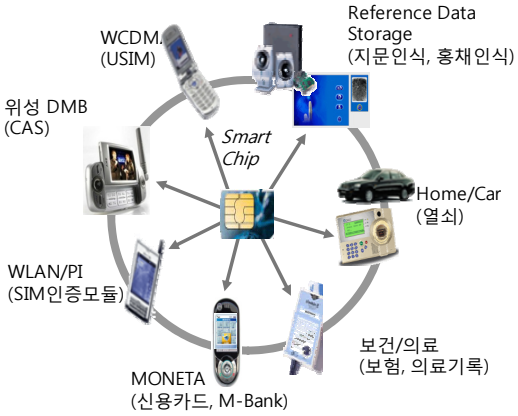
USIM 에 저장된 인증서 기반의 정책 적용, 사용자 및 단말장치 프로파일 통합, USIM 과의 인터페이스를 위한 리더기 설치, 그리고 인증 관련 어플리케이션을 개발한다면 기업내 모든 업무 시스템과 IT 자산에 대한 통합 인증이 가능해 진다. 즉, 물리적/논리적 보안을 단일화된 인증체계로 통합 관리 할 수 있게 된다.

3. 결론

기업은 PIN, 암호, 스마트카드, 생체정보, 디지털인증서 등을 포함한 다양한 인증기법을 사용할 수 있다. 어떤 인증 기법을 사용할 것인지는 보안 위험에 대한 경영진의 평가에 기초하여 기업 내부적으로 결정할 수 있다.

본 논문에서 제안하는 인증서비스를 도입 하면, 기존의 업무시스템에 대한 인증뿐 아니라, 무선 업무 시스템의 인증을 포함하여, 출입보안 등 물리적 보안까지 단일화된 체계로 통합관리가 가능해진다. 노트북 같은 개인 단말 사용시에도 실시간 인증을 통하여 사용 권한을 확인 할 수 있어, 분실과 도난에 대한 보안성도 확보 할 수 있다. 또한, 신규 서비스 적용 시에 인증 시스템의 신규 구축 없이 소프트웨어 기반으로 동일한 인증 서비스를 제공할 수 있게 된다.

USIM 을 활용한 모바일 기반의 통합 인증 체계를 구축하여 금융 결재 분야까지 확대 한다면, 약 10 만 조원 규모의 세계 전자지급결제 시장에서 1% 이상의 수익을 낼 수 있는 새로운 서비스를 만들 수 있게 된다. 대략 1,000 조원 규모의 서비스가 된다. (그림 9)는 향후 확대될 서비스에서 USIM 의 역할을 보여준다. USIM 은 단순한 인증 도구의 역할을 넘어 다양한 서비스를 제공할 수 있는 인프라로 진화되고 있다.



(그림 9) USIM 의 향후 역할

향후 계획으로 USIM 과 무선망 기반의 인증 서비스를 활성화 할 수 있도록 개인 인증방식, 암호화 및 프로토콜 운영과 제도에 대하여 연구하고자 한다.

참고문헌

[1] ICT Standardization Roadmap 2010
[2] 클라우드 컴퓨팅 보안 기술 정보보안학회 2009.6
[3] 클라우드 컴퓨팅과 개인 인증 서비스 정보보안학회지 제 20 권 제 2 호 2010.04
[4] 김성천 [전자금융환경의 변화와 기술동향 및 진화방향] {제 4 회 인터넷&정보보호 세미나 2010.03.10]
[5] 김남훈 [스마트폰이 금융서비스에 미치는 영향], {하나금융포럼 4 월 기자간담회}
[6] 차세대 USIM 기술 표준기술동향 2008.04
[7] 통합 프로파일 관리 및 인증 제어 기술 동향 전자통신동향분석 제 21 권 제 6 호 2006 년 12 월