이동통신 정보보호 현재와 미래

KT 컨버전스WIBRO사업본부 단말연구센터 단말인프라Task
박재민 (jmpark@kt.com)

Agenda

1. Introduction
2. 이동통신 정보보호 현재
3. 이동통신 정보보호 미래
4. 결론

1. Introduction

KT 소개 : olleh kt

- olleh 경영이란 발상의 전환과 끊임없는 소통을 통한 지속적인 혁신으로 고객을 위한 새로운 가치를 창조함으로써 고객에게 최고의 기쁨을 드리기 위한 통합 KT의 新 경영방향

'hello' 역순	'올来'	'올레'	'ole'
'역발상의 혁신적 사고를 통해 서비스를 제공하겠다는 의미'	'미래가 온다는 뜻으로 기존에 제공되지 않았던 새로운 가치를 의미'	'좋은 길, 작은 길의 제주도 방언으로 집과 큰길을 연결하는 골목처럼 항상 고객과 소통해 고객 입장에서 서비스 한다는 의미이자, 'KT로 올래?' 의미'	'투우에서의 감탄사로 고객, 직원, 업계 등 주요 이해관계자들이 KT와 만날 때마다 느끼게 되는 기쁨과 감동을 의미'

KT의 역할

1. **통신 사업자 = (Mobile) Operator = TelCo**
   - 통신 설비를 설치, 운용하여 그 설비에 의해 서비스를 제공하는 것을 본업으로 하는 사업자
   - 이동통신사업자는 **주파수**를 보유하고 있음
2. **기준 제시 = 규격 (Specification)**
   - 단말/USIM 등의 제조사, CP, 서버 인프라 개발사 등에 사업을 위한 기준을 규격 형태로 제시함
3. **기술에 의미와 가치 부여**
   - 내가 그의 이름을 불러 주기 전에는 그는 다만 하나의 몸짓에 지나지 않았다.
   - 내가 그의 이름을 불러 주었을 때 그는 나에게로 와서 꽃이 되었다.

이동통신 개요

- **사용자**가 **단말기**를 통해 **음성**이나 **영상**, **데이터** 등을 장소에 구애 받지 않고 통신할 수 있도록 **이동성**을 제공하는 **통신 서비스**를 말한다. (위키백과)

KT 3G 이동통신 서비스 소개

1 영상 전화

KT 3G 이동통신 서비스 소개

1 자동 로밍 서비스

KT 3G 이동통신 서비스 소개

3 제휴 서비스

KT 3G 이동통신 서비스 소개

4 USIM 금융 서비스

KT 3G 이동통신 서비스 소개

4 USIM 금융 서비스

- USIM의 **1) 안전한 정보 저장 기능**과 **2) 보안 연산 능력**을 활용하여, 하나의 USIM을 통해 Java Card Platform과 Global Platform 기반의 다양한 금융 부가 서비스 애플릿을 탑재하여 서비스를 제공함

교통

- USIM 칩에 교통 전자화폐를 다운 받아 버스/지하철에서 휴대폰으로 교통이용 (T-머니)
- 모바일 교통 VM 서비스 : 잔액조회/다양한 교통 컨텐츠/ 온라인 충전
- 이용 지역 : 수도권/거제/통영/안동/포항/제주, T-머니 가맹점(편의점 등)에서 결제 가능

뱅킹

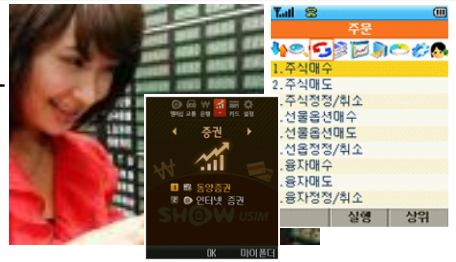
- USIM 칩에 UbiTouch 애플릿을 다운 받아 USIM 칩에 저장된 계좌 정보를 통해 빠르고 안전하게 CD/ATM 기기 기반 현금 카드 서비스 이용
- 세계 최초 One-Chip Multi-Banking (17개 은행), 100개 계좌 저장, 무선 구간 계좌 정보 암호화 제공
- 이용가능 서비스 : 현금카드 서비스

KT 3G 이동통신 서비스 소개

4 USIM 금융 서비스

증권

- USIM 칩에 증권 애플릿을 다운 받아 USIM칩에 저장된 인증정보를 통해 빠르고 안전하게 휴대폰을 통해 다양한 증권 서비스 이용
- 이용가능 서비스 : 주식거래, 관심종목 관리, 잔고/계좌조회, 계좌이체 등



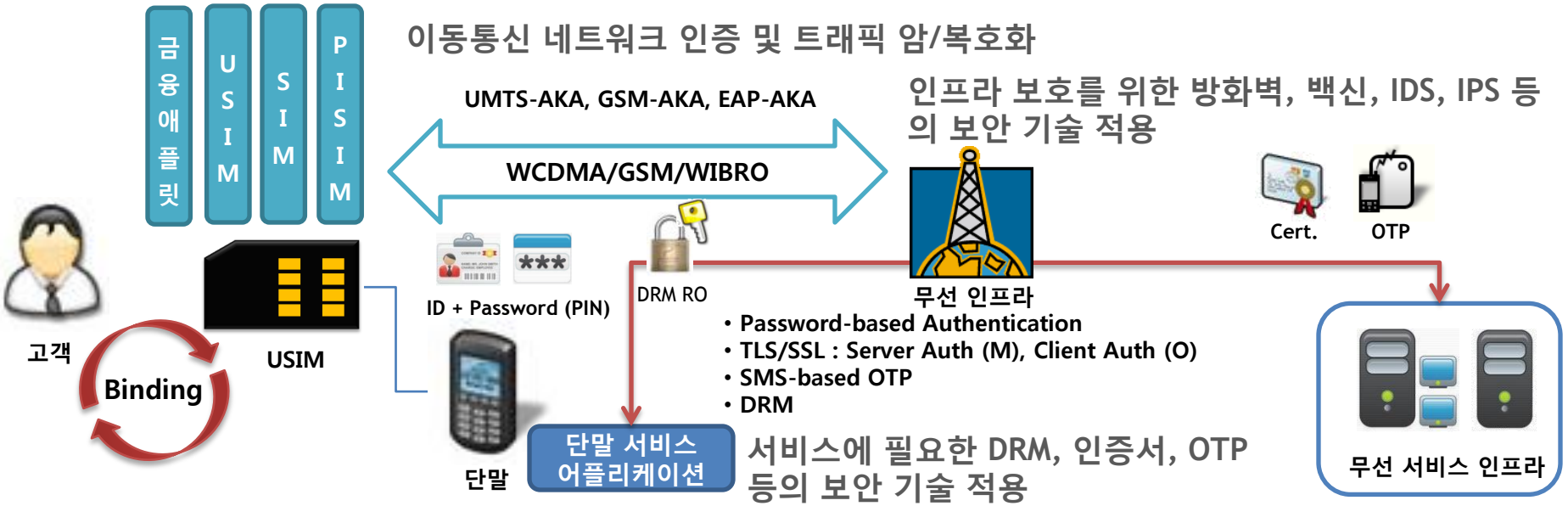
신용카드

- USIM 칩에 OTA 디지털 신용카드를 다운받아 온/오프라인 가맹점에서 휴대폰으로 결제
- 이용 지역 : 이통3사 Mobile Touch (동글) 가맹점
- VISA WAVE 와 MASTER PAYPASS 구현

이동통신에서 정보보호란?

1 고객 정보보호 수단

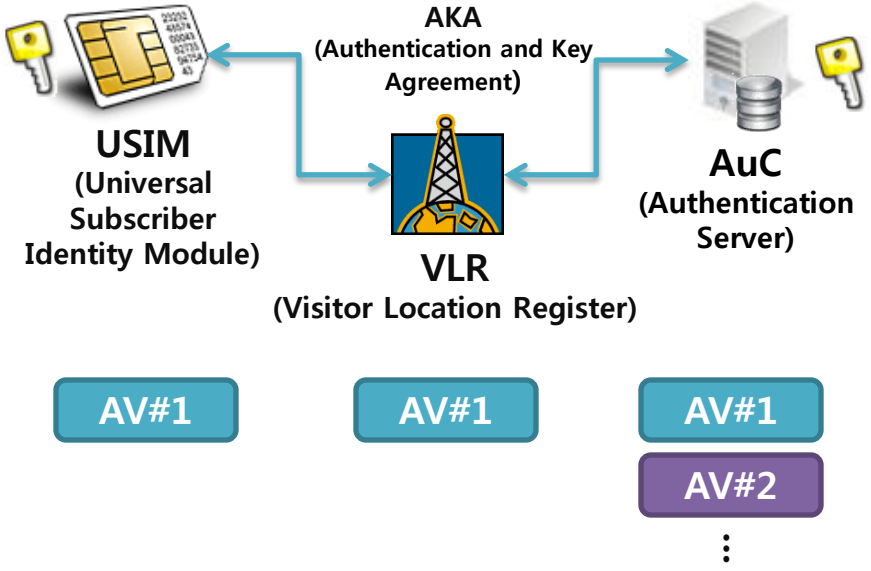
- 고객에게 고품질의 **안전하고 편리한** 이동통신 서비스를 제공하여 고객의 이용 경험(UX : User eXperience)을 더욱 풍요롭게 하는 수단임
- 이동통신 서비스의 **USIM-단말-단말SW-네트워크-서비스 인프라의 모든 영역**에 필요한 보안 기술이 적용되고 있음

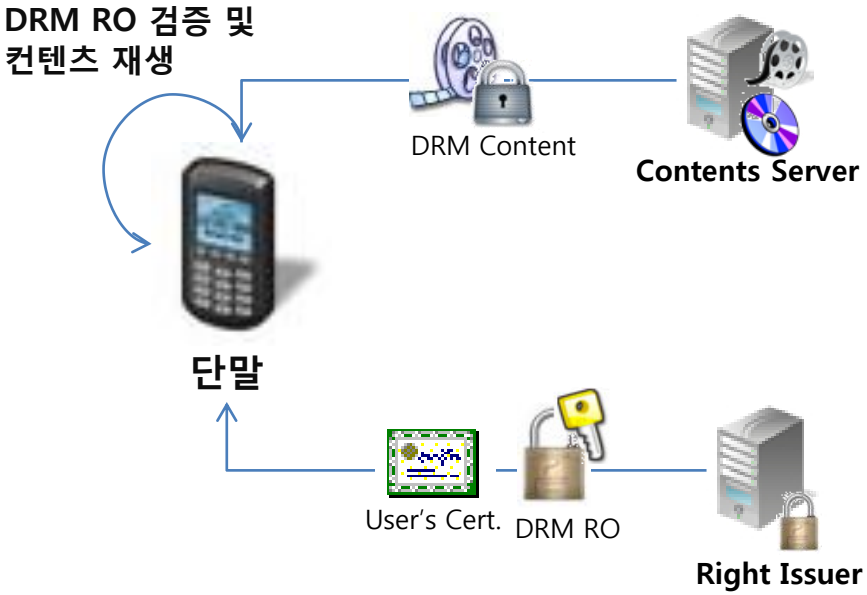


이동통신에서 정보보호란?

2 회사는 이익 집단 → 과금 기반이자 수익 보호 수단

- 비인가 사용자의 서비스 접근 방지 → 인증 기술 (WCDMA AKA)
- 불법적인 컨텐츠 (VM, 벨소리, 바탕화면, 음원 등) 다운로드 및 배포 방지 → DRM
- 비정상 트래픽 유입으로 인한 DoS, 오과금 등의 위협으로부터 이동통신망 보호 및 VOC (Voice of Customer) 해결 수단 → Firewall, IDS (Intrusion Detection System), IPS (Intrusion Protection System), UTM (Unified Threat Management) 등의 네트워크 보안 장비 적용

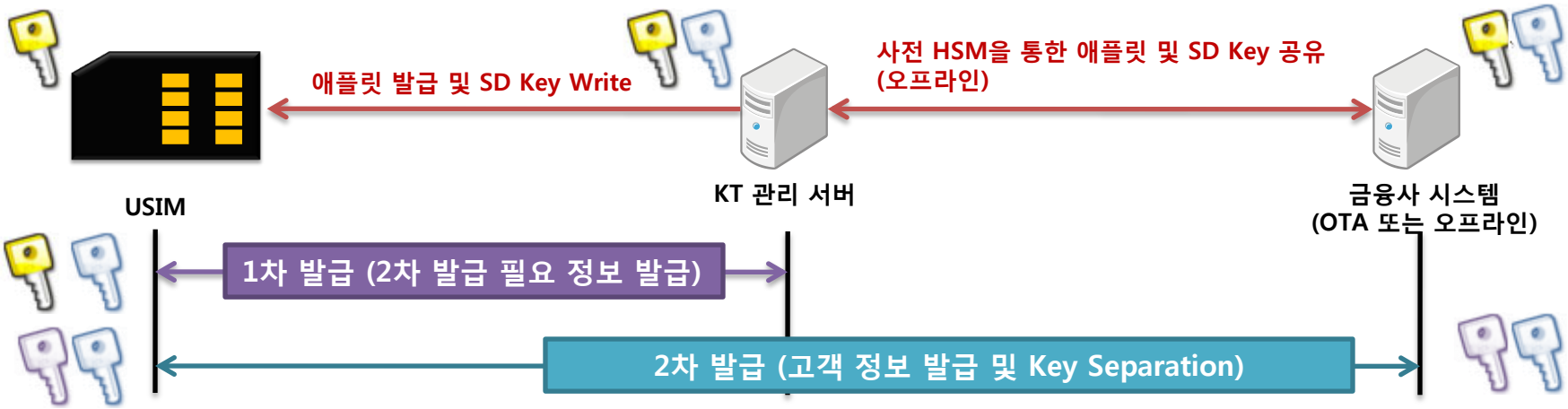




이동통신에서 정보보호란?

3 시장 주도권 확보 및 유지 수단

- 폐쇄적인 시장 구조, 모든 개발 항목에 대한 검증/검수 프로세스를 통해 사업자의 시장 주도권 확보 및 유지 수단으로 활용됨
- WIPI(Wireless Internet Platform for Interoperability)의 경우, VM 개발 시, 플랫폼 보안 레벨을 설정하여 단말 자원에 대한 접근 제어를 하며, 데이터 보안 정책을 통해 단말 메모리 접근 제어를 수행하며, 이를 검증/검수 프로세스에서 확인함
- USIM의 경우, GlobalPlatform 기반 SCP (Secure Channel Protocol)을 통해 USIM의 정보 및 애플릿 관리 기능을 수행하며, 이때 사용되는 Key를 사업자가 소유함



이동통신에서 정보보호란?

4 법, 규제, 가이드라인 등의 준수를 위한 수단

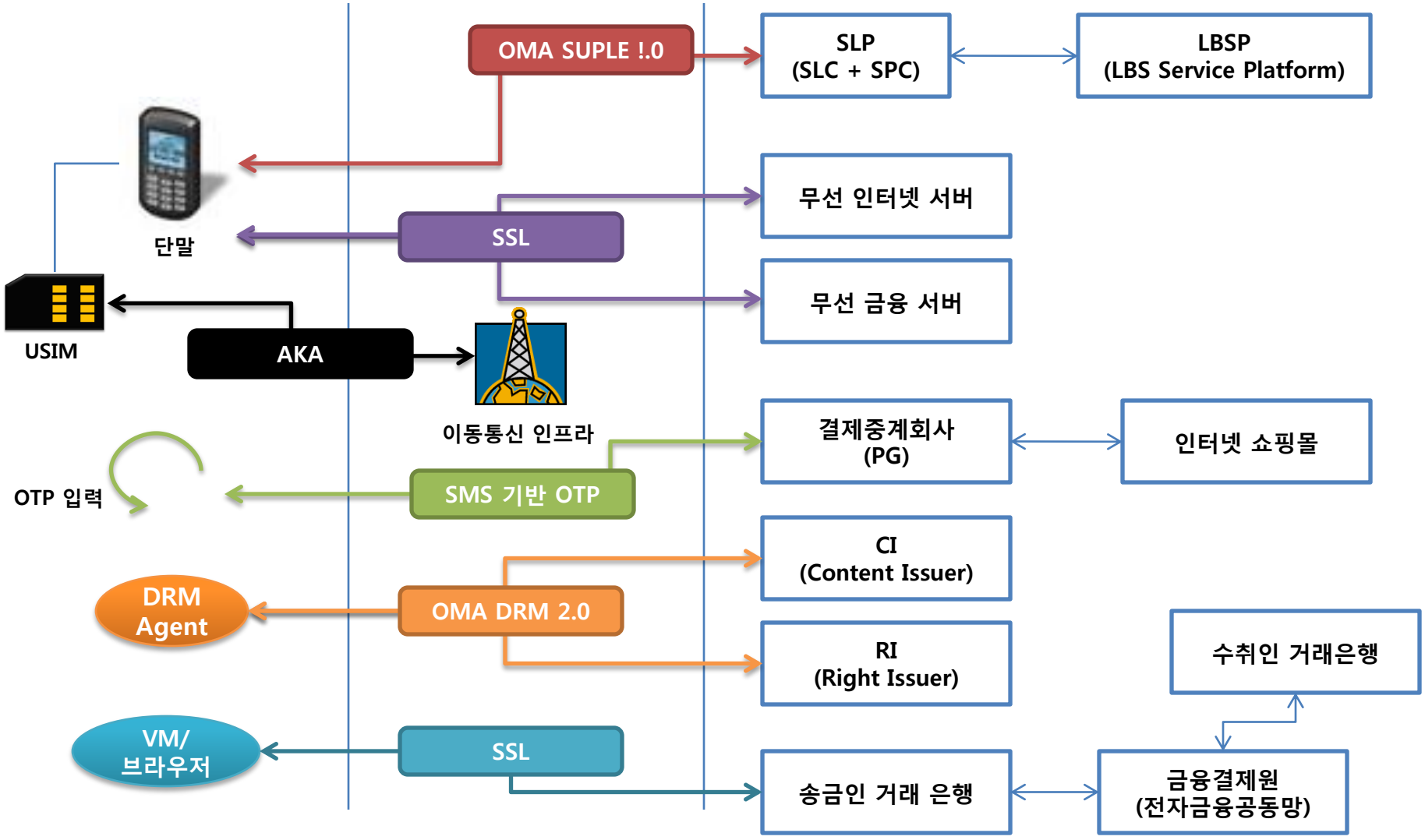
- 국내 통신 사업 및 부가 서비스 관련 법, 규제, 가이드라인 등의 준수를 위한 수단으로 활용됨
- **전자서명법** : 전자상거래에 있어 공인인증서, SEED 알고리즘 등의 사용을 의무화 함
- **통신 비밀 보호법**, **정보통신망 이용촉진 및 정보보호에 관한 법률**, **위치정보 이용 및 보호 등에 관한 법률**, **저작권법**, **전화스팸방지 가이드라인** 등이 존재하여 국민을 보안 위협으로부터 보호하고, 사업자는 이를 준수해야 함

이동통신 정보보호 기술 적용 현황

KTF ICET 서비스 및 보안기술 분석서 (2007)

분류	서비스	적용 보안 기술	설명
Information	브라우저 기반 무선 인터넷 서비스	(구) KTF SSL (표준 SSL 기반, SEED 알고리즘 적용)	표준 SSL을 준수하되, 과금 등과 같은 사업자 요구를 반영한 프로토콜이 추가됨
	LBS (Location-Based Service) 서비스	OMA SUPL (Secure User Plane Location) 1.0	단말(SET : SUPL Enabled Terminal)-측위서버(SLP : SUPL Location Platform) 간의 위치 측위 및 관리 프로토콜
Communication	영상/음성/SMS/MMS 등의 서비스	3GPP 표준 보안 기술 (AKA 등)	AKA를 통한 사용자 인증 및 세션 키 합의 그리고 합의된 세션 키로 Air 구간의 기밀성 및 무결성 보장
Entertainment	다운로드 및 스트리밍 컨텐츠 서비스	OMA DRM 2.0	DCF (DRM Content Format), 권한 표현어 (REL), 권환 획득 프로토콜, 서비스 시나리오 등 DRM 시스템에 필요한 내용 정의
		WIPI의 플랫폼 보안 및 데이터 보안 기술	어플리케이션에 등급을 할당하여 단말 자원의 접근을 제어하는 플랫폼 보안과 접근 가능한 단말 메모리 영역을 제어하는 데이터 보안 기술 적용
Transaction	브라우저 기반 서비스	(구) KTF SSL 및 인증 기술	ID/PW, 계좌비밀번호, 보안카드 기반 인증
	VM 기반 서비스	(구) KTF SSL 및 인증 기술	PIN, 계좌비밀번호, 보안카드 기반 인증
	IC 칩 기반 서비스	(구) KTF SSL 및 인증 기술	IC칩 접근 PIN, 계좌비밀번호, 보안카드 기반 인증
	소액 결재	OTP (One-Time Password)	SMS 기반 OTP

이동통신 정보보호 기술 적용 현황 (구조)



2. 이동통신 정보보호 현재

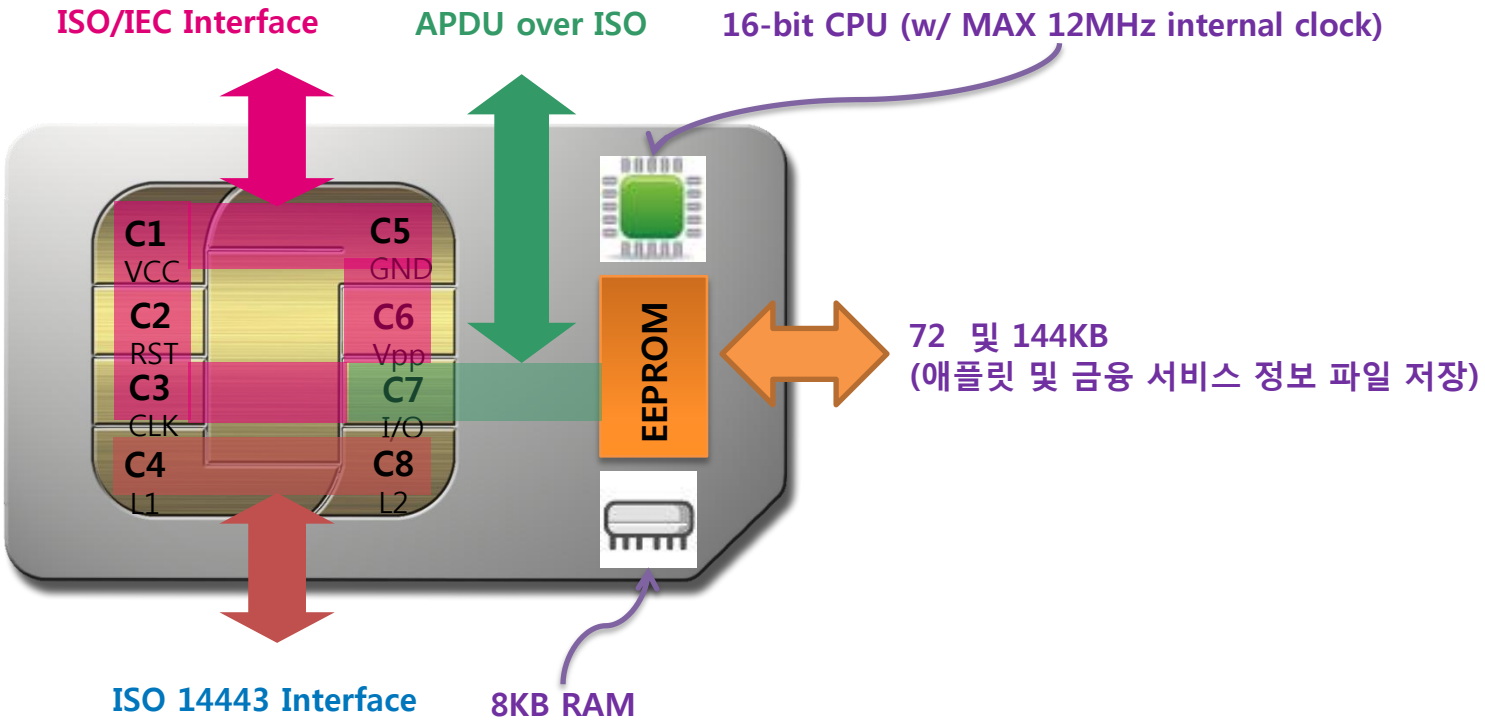
USIM (Universal Subscriber Identity Module)

- UMTS 네트워크 단말에서 사용되는 스마트 카드로 3G 단말에 기본 장착됨
- CPU, CCP, ROM, RAM, 메모리 (EEPROM, NAND Flash, NOR Flash), I/O Circuits로 구성됨
- USIM은 WCDMA 사용자 인증 모듈 → 국내에서는 IC칩(UICC) 자체를 의미하는 것으로 통용됨

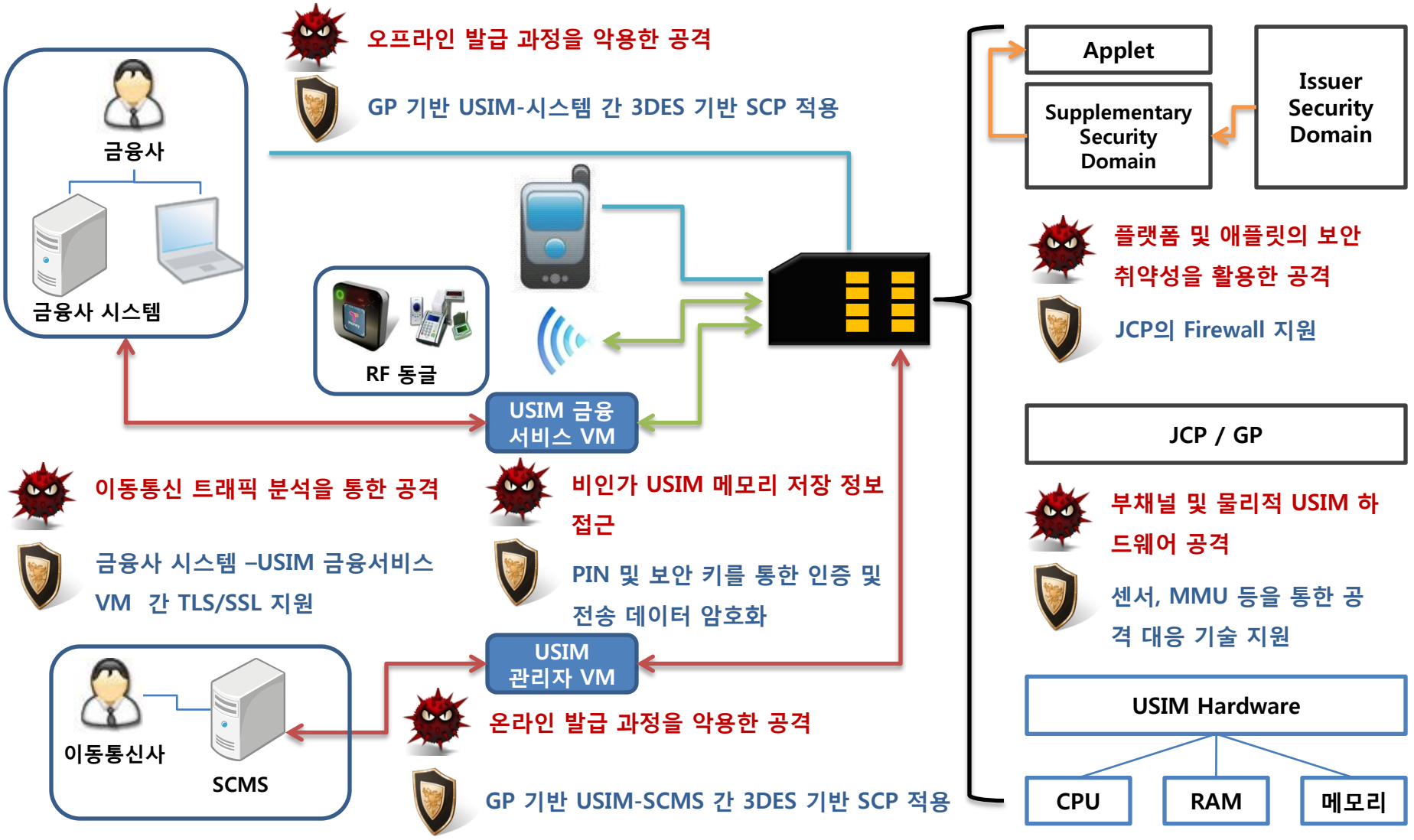
상용화	상용화 완료	상용화 완료	상용화 준비 중
상용 서비스	• 네트워크 인증, 로밍 • 기본 PIMS (폰북, SMS 저장)	• 교통, 뱅킹, 증권, 신용카드 • 멤버쉽, 모바일 캠퍼스	• SCWS 기반 서비스 • NAND Flash 기반 서비스
I/F	• ISO 7816	• ISO 7816 & 14443	• ISO 7816 & USB & NFC
탑재 기술	• Java Card Platform 2.2.1 • GlobalPlatform 2.1.1	• 72/144KB EEPROM • Java Card Platform 2.2.1 • GlobalPlatform 2.1.1	• Java Card Platform 2.2.2 • GlobalPlatform 2.2 • OMA SCWS 1.1 • 32-bit CPU & Mbyte NAND Flash

금융 USIM 구조

- USIM 금융 서비스 제공에 기반이 되는 USIM (Combi USIM이라 불림)
- 현재 애플릿 탑재 가능 메모리 크기에 따라 72 및 144KB 2가지 종류가 존재함
- 국내에서만 사용되는 combi RF interface를 제공함 (해외의 경우, NFC 기술을 활용함)



USIM 금융 서비스에 대한 가능 공격 유형 및 안전성 제공 방안



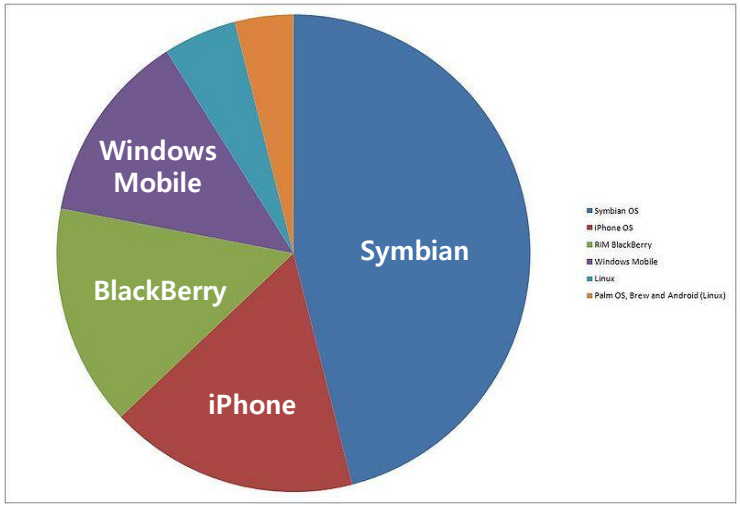
이동통신 환경 변화 - 1

1 스마트폰 도입

- 국내 사업자들이 경쟁적으로 Symbian (Nokia), BlackBerry (RIM), Windows Mobile (MS), iPhone (Apple), Android (Google), Linux, Palm, BREW 등의 플랫폼을 탑재한 스마트폰을 출시하고 있음
- Mobile device containing both cellular components and Internet access, with powerful computing components similar to those found on desktop PC's (Wikipedia)
  - A phone that runs complete operating system software providing a standardized interface and platform for application developers
  - A miniature computer that has phone capability

BlackBerry (RIM)

Symbian (Nokia)

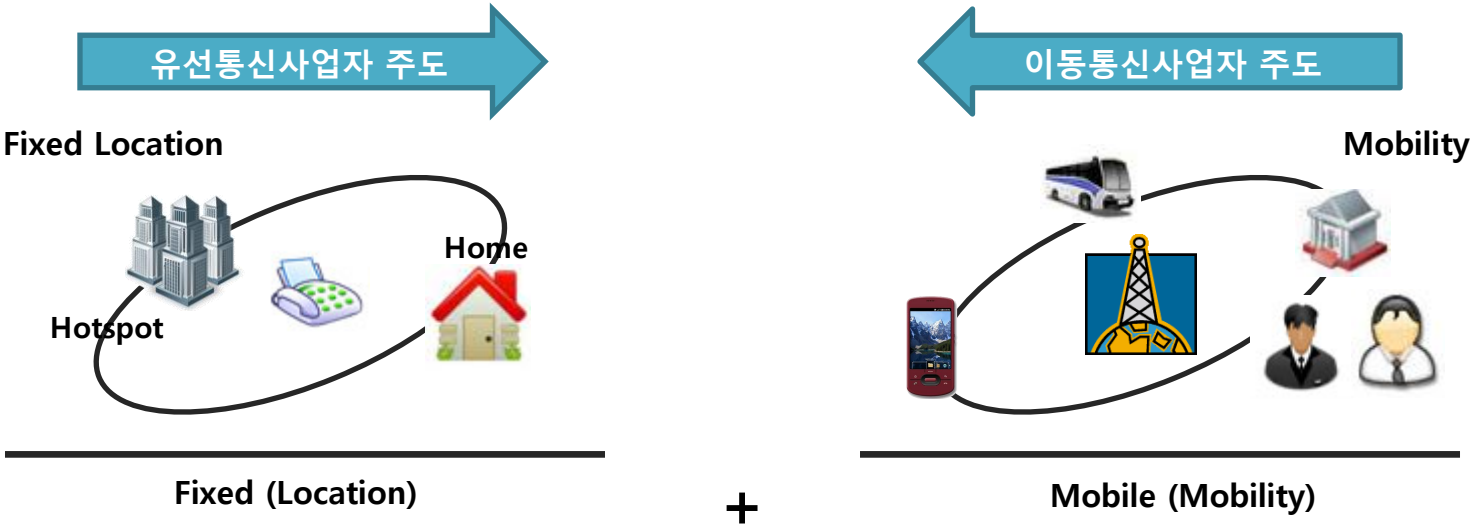


Market Share (2008)

이동통신 환경 변화 - 2

2 FMC (Fixed Mobile Convergence)

- 유무선 컨버전스가 대세임 → KT-KTF 합병, SKT의 SK Broadband(하나로텔레콤) 인수
- 하나의 단말로 유무선 인프라에 접속하여 다양한 유무선 컨버전스 서비스를 제공하는 것
- 접속 대상 네트워크 기술 : WCDMA/WIBRO (기존) + WiFi
- 접속 대상 서비스 인프라 : 무선 서비스 인프라 (기존) + 유선 서비스 인프라 (예, IPTV 등)



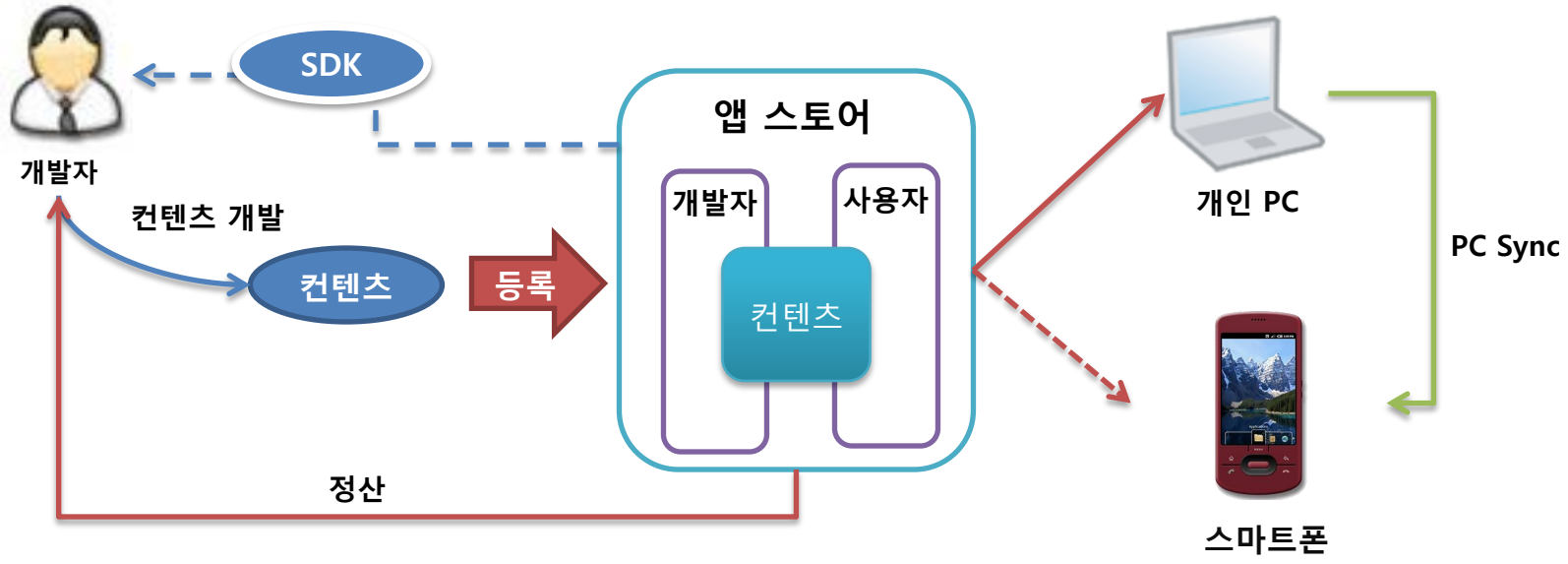
Fixed Mobile Convergence

유무선통합(FMC) 서비스의 해외 동향 및 확산요인 분석 ('09.02, KISDI)

이동통신 환경 변화 - 3

3 앱 스토어 도입

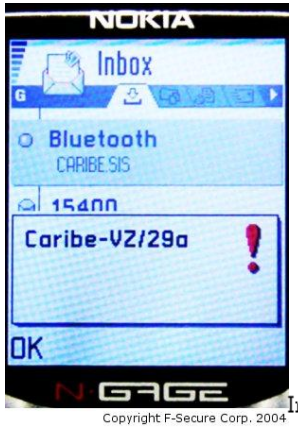
- 사업자, 제조사 등 Apple AppStore의 성공을 계기로 스마트폰 시장의 앱 스토어 시장에 진출함
- 앱 스토어란 컨텐츠 배포의 새로운 트랜드로 단말과 같은 IT 기기에 필요한 다양한 응용 프로그램이 거래되는 온라인 장터
  - 애플 AppStore (‘08.7), 구글 Android Market (‘08.11), Nokia Ovi (‘09.05), RIM AppWorld (‘09.03), MS (‘09.4Q)
  - KT (가칭 SHOW 스토어), SKT (가칭 T 스토어) 준비 중, 삼성전자 (‘09년 2월 영국), LG전자(해외 오픈)



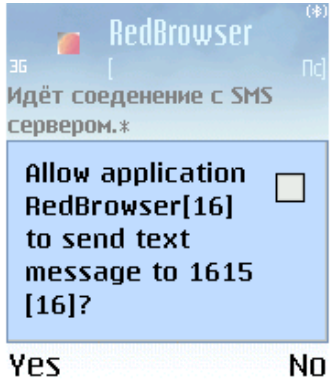
1 이동통신 미래 환경의 보안 위협(요구) - Mobile Virus

- **개념** : 개인정보 유출, DoS (Denial of Service), DDoS 공격 등 악의적인 용도의 소프트웨어로 사용자의 허가 없이 자가 복제를 하고 다른 기기 (스마트 폰 등)를 감염시킬 수 있음
- **공격 대상** : Content, Mobile Device 및 Network (Infra 포함)로 스마트 폰 기반 이동통신 서비스 전 구간에 걸쳐 영향을 줄 수 있는 가장 위협적인 존재
- 스마트 폰 환경이 되면서, 다양한 네트워크 인터페이스를 통해 다양한 인프라와 연동함으로써 모바일 바이러스의 감염 경로(PC, Bluetooth, SMS, MMS 등)가 다양해지고 감염 확률이 높아짐
- 스마트 폰을 대상으로 한 다양한 Anti-Virus 솔루션이 전세계적으로 존재함

종류	대상 OS	증상 및 영향	감염 경로
Cabir (Worm, 2004)	Symbian	단말이 켜질 때마다 'Caribe' 텍스트를 출력하며, 다른 Bluetooth 기기에 연결을 시도하여 자신을 복제함 → 배터리 소모 초래	Bluetooth
Brador (Backdoor, 2004)	Pocket PC	시작 폴더에 자신을 복제하고 감염 PDA가 온라인이 되면 이를 Cracker에 알려 TCP door를 통해 PDA를 통제함	감염 파일
RedBrowser (Trojan Horse, 2006)	J2ME	Java Midlet이 SMS를 통한 무료 인터넷을 주는 것처럼 가장하여, 유료 SMS들을 전송함 → 비인가 과금 발생	Internet Download
FlexiSpy (Spyware, 2006)	Symbian	비인가 통화 기록 전송, SMS 및 MMS 복제 → 개인 프라이버시 침해	Internet Download



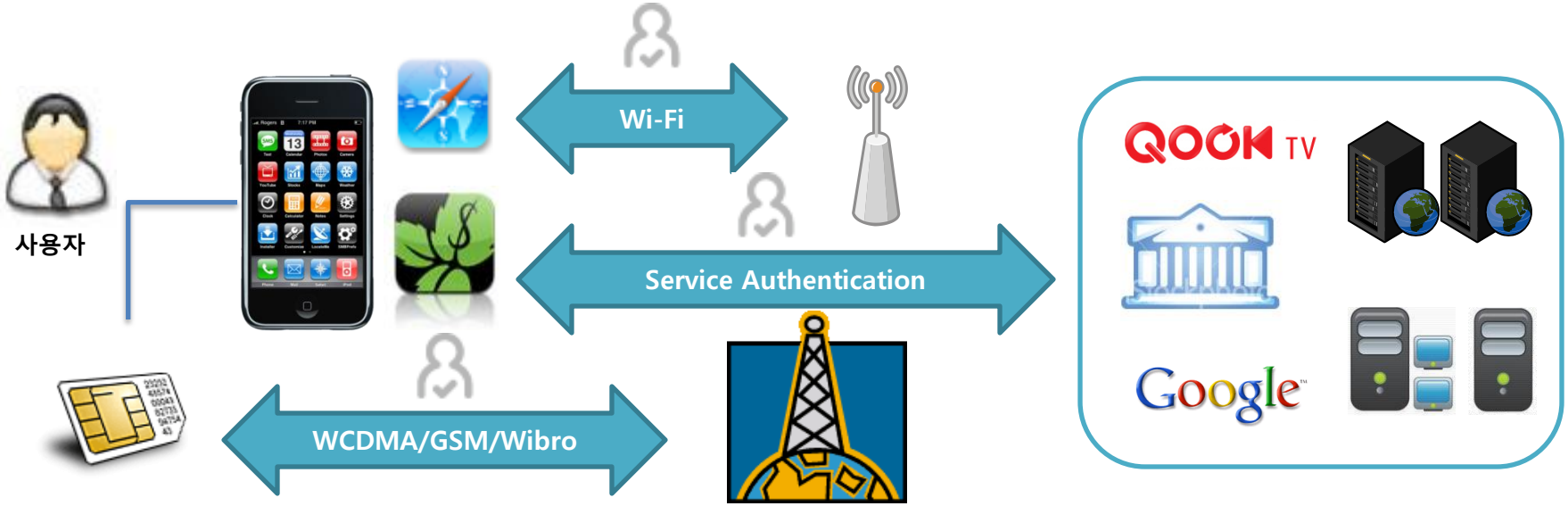
Carbir



RedBrowser

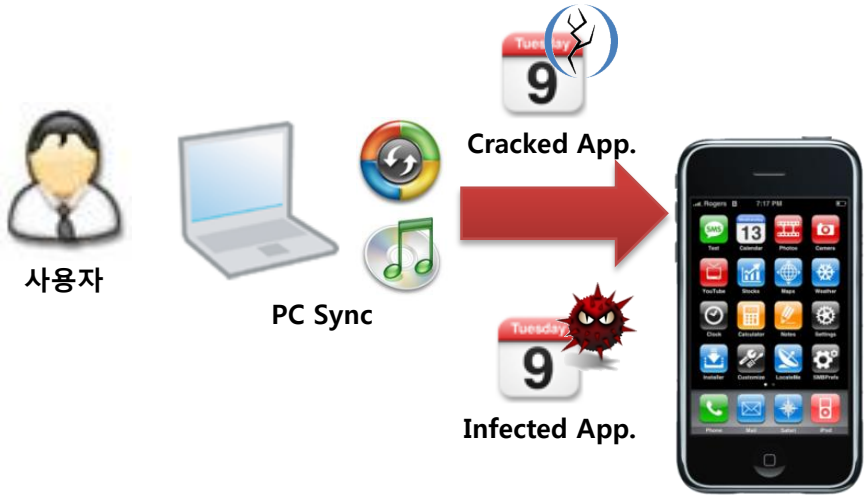
2 이동통신 미래 환경의 보안 위협(요구) - 통합 인증

- 스마트 폰 환경의 Openness와 다양한 네트워크 인터페이스 및 연동 인프라로 인해 사용자 또는 기기에 대한 안전하고 효율적인 “통합 인증”이 매우 중요함
- **“통합 인증”이란** 스마트 폰을 중심으로 사용자 또는 기기에 대한 **네트워크 인증** (WCDMA, GSM, Wi-Fi 등)과 **서비스 인증** (IPTV, 금융 인프라, 인터넷 포털 등)을 의미하며, 통합 인증을 통해 단말-네트워크-서비스 인프라 간의 Secure Channel이 형성됨
- 현 상황은 WCDMA, GSM 등의 네트워크 인증은 (U)SIM을 통해, Wi-Fi 및 서비스 인증은 스마트 폰 OS 또는 단말 어플리케이션 계층에서 분산적으로 이뤄지고 있음



3 이동통신 미래 환경의 보안 위협(요구) - Content Theft & Piracy

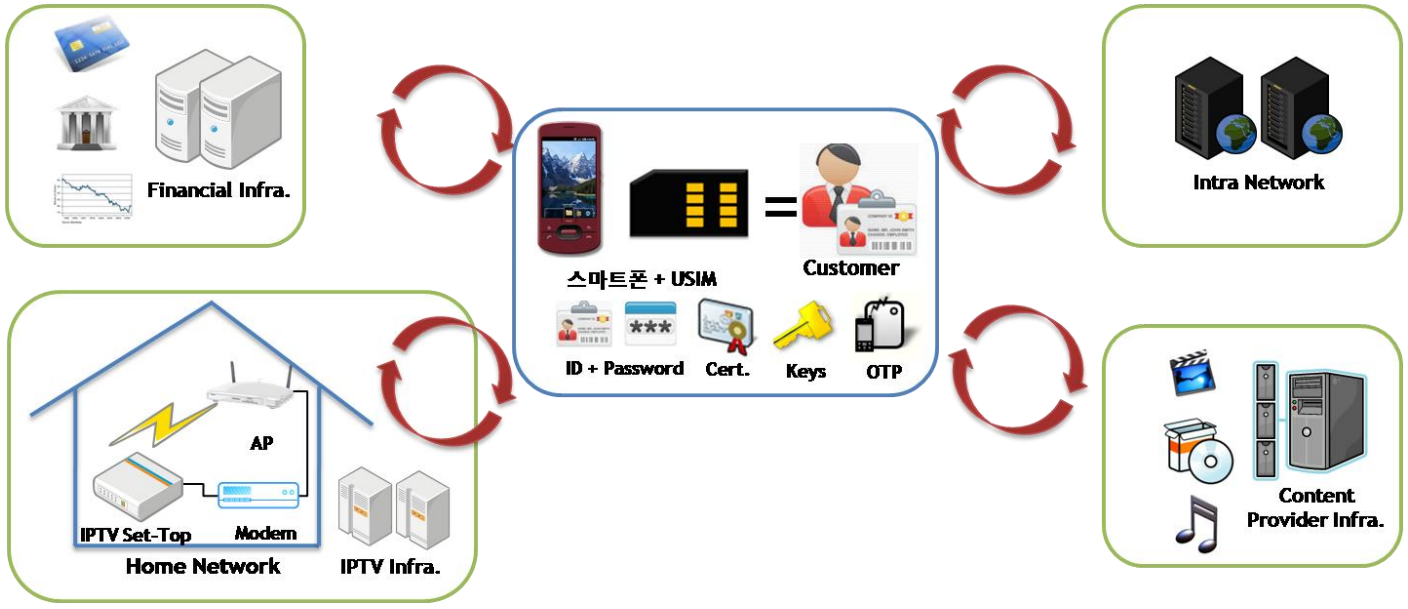
- 스마트 폰 환경은 기존 이동통신의 폐쇄적 서비스 환경과 다른 Openness 환경임
- 단말 어플리케이션이 기존 무선 다운로드 방식에서 PC Sync 기반까지 확장되며, 사용자는 다양한 컨텐츠 유입 경로를 통해 단말 어플리케이션을 획득할 수 있음
- 국내에서는 폐쇄적인 서비스 환경과 DRM 기반의 컨텐츠 보호를 통해 생소했던 휴대 단말 어플리케이션의 불법 복제 이슈가 스마트 폰 환경에서 발생하게 됨
- 불법적인 경로로 유입된 단말 어플리케이션으로 인해 사업자 BM 피해 및 경제적 손실이 불가피할 수 있으며, 바이러스에 감염된 단말 어플리케이션의 설치로 인해 Mobile Virus로 인한 피해까지 발생할 수 있음



미래 이동통신 정보보호 전망

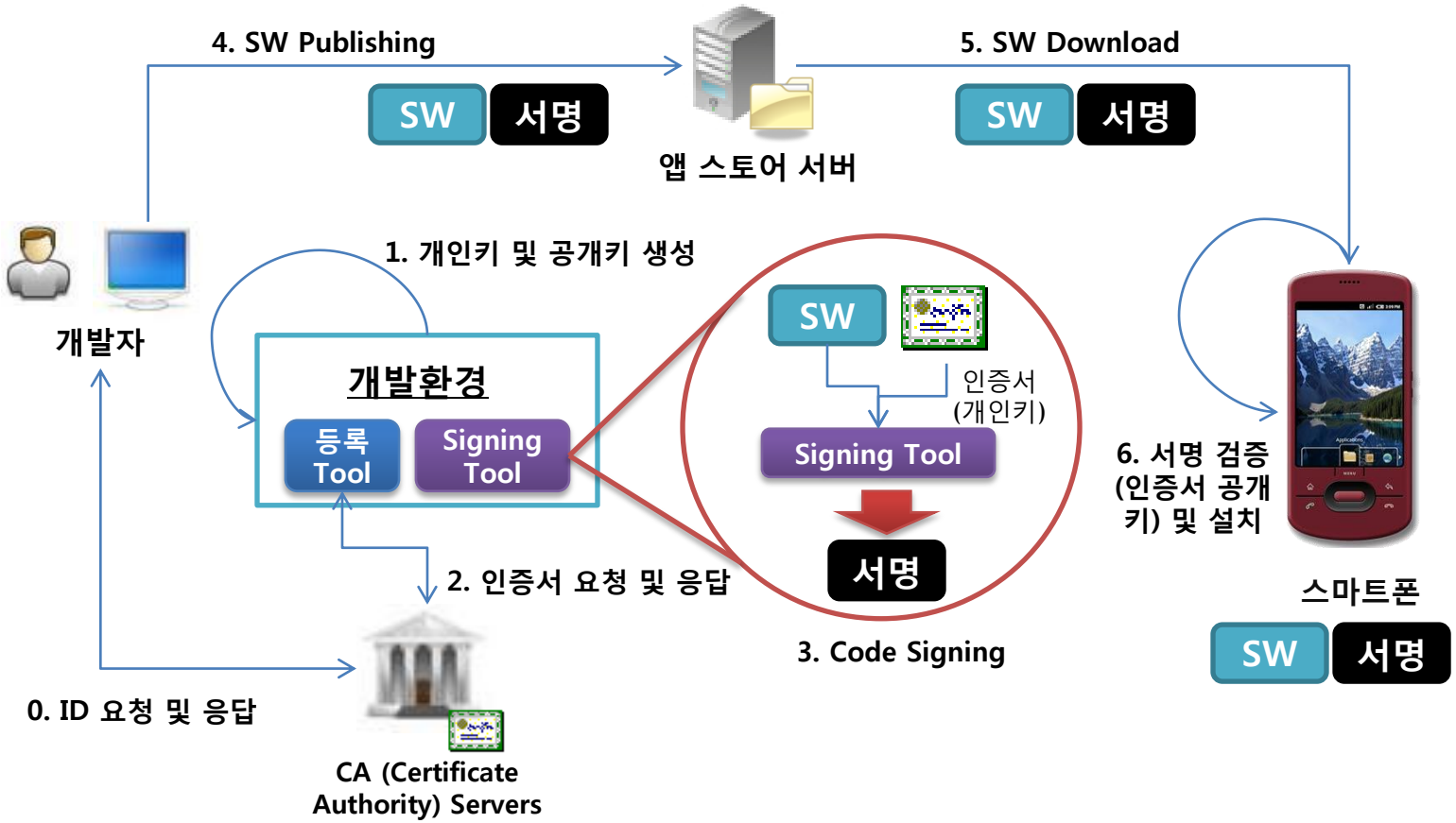
1 주도권 확보 → 통합 인증 및 코드 서명

- 스마트폰 및 앱 스토어 도입에 따른 **단말 제어권 확보**와 FMC 환경에 따른 **단말 중심으로 통합 인증 Needs**에 따라 코드 서명 및 통합 인증 기술에 대한 수요가 클 것으로 예상됨
- 코드 서명이란? 단말 응용 프로그램 자체에 대해 서명을 하고 이를 단말에 탑재할 때마다 검증함으로써 프로그램 자체의 **무결성(변조 여부)**, **출처 검증**, **안전성 보장**하는 보안 기술
  - 적용사례 (단말플랫폼) : Symbian S60, Google Android, MS Windows Mobile, Apple iPhone



미래 이동통신 정보보호 전망

1 주도권 확보 → 코드 서명 기술 (계속)



미래 이동통신 정보보호 전망

2 바이러스 및 DDoS 대응 - AV (Anti-Virus), Key Protection 등

- 오픈 플랫폼의 스마트폰 활성화와 DDoS 위협으로 모바일 바이러스에 대한 위협이 급증할 것으로 생각되며, 이를 위한 백신 솔루션 (Anti-Virus) 기술에 대한 수요가 클 것으로 예상됨
- 스마트폰의 Key Hooking 위협으로 스마트폰을 통해 입력되는 개인 정보의 노출 위협이 급증함에 따라 이를 대응하는 Key Protection 기술에 대한 수요가 클 것으로 예상됨

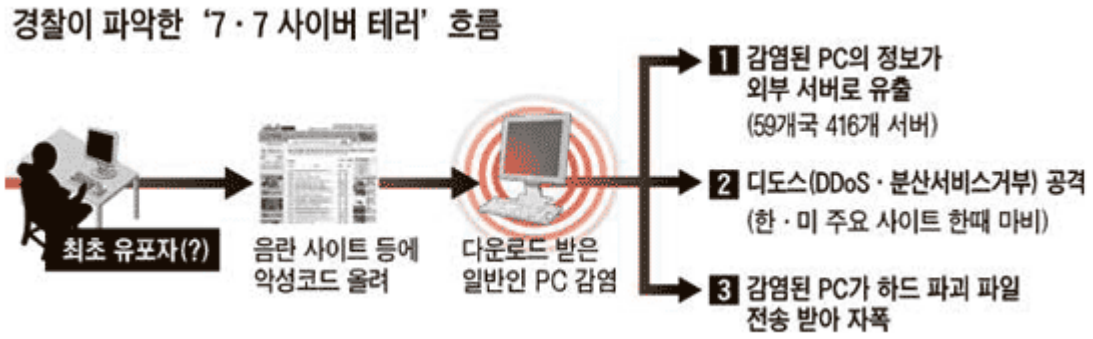
미래 이동통신 정보보호 전망

3 정보의 안전한 관리 - 저장 공간 (USIM), 원격 관리 기술 (DM), PC-Sync 기술

- 단말에는 다양한 개인 정보가 저장되기에 이를 안전하고 저장하기 위한 Secure Storage로써의 USIM 활용 방안 (고성능 USIM)에 대한 수요가 높을 것으로 예상됨
- 단말 분실로 인한 보안 위협을 최소화하고 사용자의 정보를 안전하게 백업하였다가 복원해주기 위한 **원격 관리 기술(DM : Device Management)** 및 **안전한 PC-Sync 기술 기반**에 대한 수요가 높을 것으로 예상됨

4. 결론

세상이 필요로 하는 것을 사명감을 갖고 준비하자!



DDoS 대란 ('09.07.07, 중앙일보)

CIH 바이러스 대란 (1999, KBS)

안철수 교수의 MBC 무릎팍도사 출연 (2009)

Thank You~!!

박재민 (jmpark@kt.com)