MTM기반 스마트 단말 보안 기술

Ⅰ. 제안기술 개요

기술의 내용	기술의 동향	기술의 제품화 및 시장 전망
▪ 스마트 단말의 정보유출 방지를 위한 MTM(Mobile Trusted Module, 이하 MTM) 기반 보안 핵심 기술로서, 개방형 플랫폼 환경에서 스마트 단말의 전력, 메모리 등 자원 문제를 해결하고 분실/도난에 의한 정보 유출 방지, 비인가된 사용자의 불법 접근을 차단하는 MTM 하드웨어 기반의 단말 보안 시스템 기술임	[국내동향] ▪ 국내 스마트 단말용 보안 기술은 안티 바이러스, 방화벽 기능, 다바이스 잠금 기능 등과 같은 단품형 기술로 구성되어 있으며, MDM으로 스마트 단말을 제어하는 비교적 초기 단계의 기술 수준임 [해외동향] ▪ ARM(TrustZone), Intel, Global Platform 등에서 하드웨어 기반의 스마트 단말용 보안 기술이 개발되고 있으나 아직은 초기 단계이며, 안전한 스마트 단말 서비스 환경을 보장하기 위한 보안 인프라에 대한 개발은 이루어지고 있지 않음	▪ 대상 기술은 기존의 PC나 노트북용 보안칩(TPM)과는 달리 모바일 단말에 직접 적용 가능한 기술로써, MTM을 기반으로 수행되는 스마트 단말용 보안 기술임 ▪ 스마트 단말의 확산과 함께 스마트폰을 이용한 모바일 서비스 이용도 급격히 증가하는 추세임 ※ 스마트폰 기반 모바일뱅킹 이용 금액이 2012년 4분기 1일 평균 1조 719억원 기록 ▪ 따라서 MTM을 이용하여 단말 플랫폼 및 서비스의 안전성을 확보하기 위한 보안 기술은 꼭 필요함.

상용화단계	일반	①아이디어 ②연구단계 ③개발단계 ❹개발완료(시제품) ⑤제품화 단계
	의약바이오	①라이센싱 ②개발단계 ③제품화 단계
핵심키워드	한글	모바일 신뢰모듈, 스마트 단말보안, 하드웨어 보안 모듈
	영문	Mobile Trusted Module, Smart Device Security, Hardware Security Module

Ⅱ. 기술개발자 정보

기관명	한국전자통신연구원	부 서	모바일보안연구실
성 명	전용성	직 급	실장
전화/핸드폰		이메일	ysjeon@etri.re.kr

Ⅲ. 수행과제정보

지원지관명		연구사업명	
연구과제명		수행기간	
주관기관		공동연구기관	

Ⅳ. 특허정보

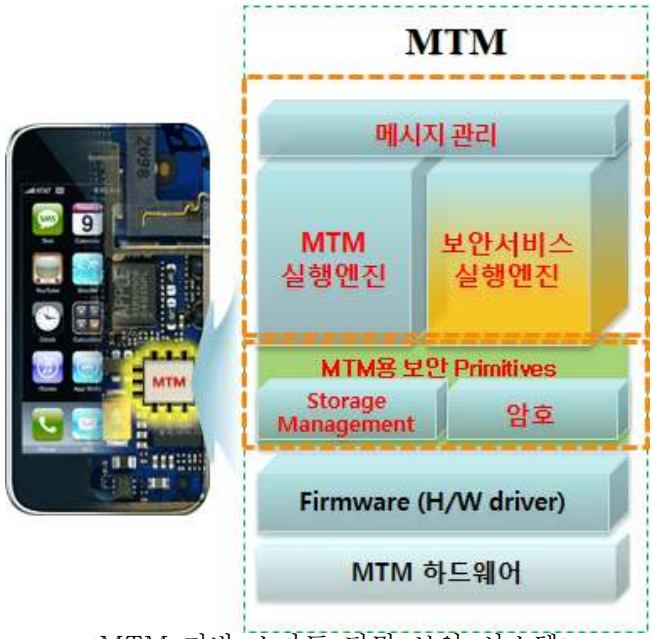
특허현황	사업화대상기술 관련특허 총 4 건				
상세현황	구 분	상 태	출원(등록)일자	권리번호	특허명
	대상기술	■출원□등록	2015.03.20	10-2015-0039016	사용자 장치 및 그것에 대한 무결성 검증 방법
	관련기술	■출원□등록	2014.12.04	10-2014-0173083	개선된 MTM의 세션 및 키 관리 방법
	관련기술	■출원□등록	2013.10.14	10-2013-0122129	인터페이스 변환장치, 상기 인터페이스 변환장치를 구비한 임베디드 시스템 및 이에 이용되는 데이터 신호 전달 방법
	관련기술	■출원□등록	2013.10.21	10-2013-0125490	신뢰 보안 플랫폼 모듈을 이용한 보안 애플리케이션 인증 및 관리 방법 및 장치

1. 기술성 분석

1. 기술의 내용 및 특징

○ 본 기술은 스마트 단말의 정보유출 방지를 위한 MTM(Mobile Trusted Module, 이하 MTM) 기반 보안 핵심 기술로서, 개방형 플랫폼 환경에서 스마트 단말의 전력, 메모리 등 자원 문제를 해결하고 분실/도난에 의한 정보 유출 방지, 비인가된 사용자의 불법 접근을 차단하는 MTM 하드웨어 기반의 단말 보안 시스템 기술임

○ 본 기술은 스마트 단말에서 MTM을 기반으로 수행되는 보안 기능에 관한 것으로, MTM은 하드웨어적으로 분리되어 단말시스템에서 보안 서비스가 안전하게 실행될 수 있는 보안기능을 제공해 줌



<MTM 기반 스마트 단말 보안 시스템>

○ TM은 저전력, 저성능의 하드웨어모듈로서, 매우 낮은 동작 주파수(20MHz 이하)를 가지고 있으므로, PC또는 여타의 임베디드 시스템에 비해 프로그램의 수행시간이 많이 소요됨. 따라서, 이를 극복하기 위하여 본 기술은 저성능의 프로세서에 맞게 암호 및 보안엔진의 실행코드를 최적화함.

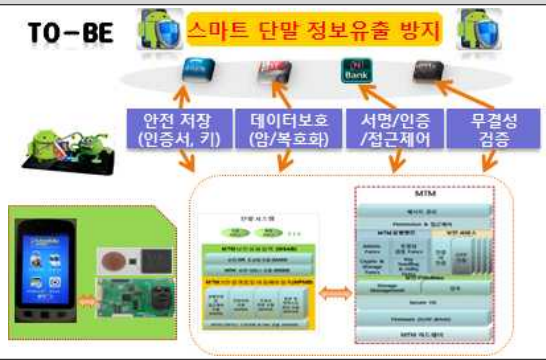
○ 또한 MTM 내의 암호 기능에는 국산 암호알고리즘인 SEED, ARIA를 포함

하고 있으므로, 국내의 기존 보안 시스템과의 연동에도 전혀 문제가 없음

○ 기존의 응용 수준의 단말 보안 기술에 비해 모바일 단말 플랫폼에서 높은 안전성을 얻을 수 있으며, 물리적 해킹에 대한 방지가 가능한 정도의 보안성을 제공함에 따라, 모바일 단말을 이용한 다양한 서비스를 보다 안전하게 수행할 수 있음

○ 인증, 지불·결제 등 다양한 모바일 서비스의 안전성과 신뢰성을 요구하는 스마트 단말 환경에서 정보유출을 방지하는 저전력 하드웨어 핵심 기술 및 단말 보안 플랫폼 기술임

- ✓ 저전력 MTM 하드웨어 핵심 기술
- ✓ MTM 연동 단말 보안 플랫폼 기술

기존 모바일 백신 및 MDM 솔루션 적용	MTM기반 보안 기술
	
– SW 기반의 모바일 보안 기술 ✓ 안티바이러스, 모바일 백신 등 ✓ 디바이스 원격 관리를 위한 MDM (Mobile Device Management) 솔루션	– MTM 하드웨어 기반 보안 기술 ✓ MTM내부에 인증서 및 키 저장 ✓ MTM내부에서 암호,전자서명 수행

	세부 기술
MTM용 암호 기술	o 해쉬 함수 – SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, HMAC-SHA1 o 대칭키 기반 암호 – AES, T-DES, ARIA, SEED (key size : 128/192/256bit) o 공개키(RSA)기반 암호 및 서명 – RSA 기반 데이터 암호 기능 제공 (RSA-2048 연산 가능) – RSA 기반 서명 기능 제공 (RSA-2048 연산 가능) o 참난수(True Random Number)기반의 공개키 생성

단말 무결성 측정 및 검증 기술	o SRTM(Static Root of Trust Module) – 모바일 단말의 부팅 단계에서 시스템 컴포넌트에 대한 위.변조 탐지 기능 o DRTM(Dynamic Root of Trust Module) – 모바일 단말의 부팅 이후에 시스템 컴포넌트에 대한 위.변조 탐지 기능

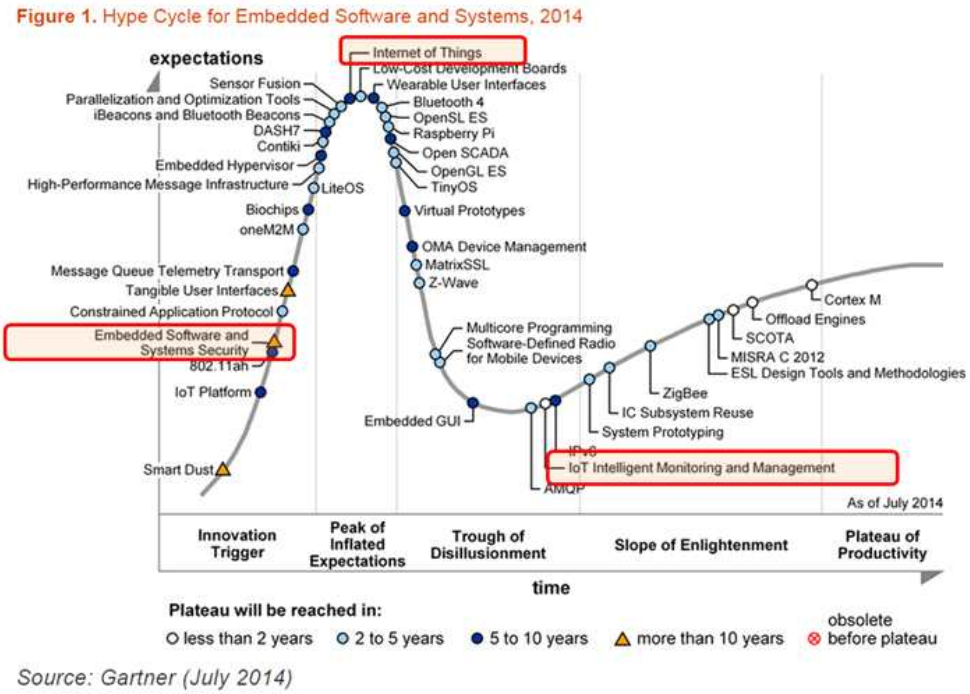
2. 기술의 수준

○ 기술수명

– 대상 기술은 ESS(Embedded Software and System Security)기술에 해당되며 상품화가 적용 가능한 분야는 IoT(Internet of Things) 디바이스의 보안 기술에 적용 가능함.

– 따라서 아래 그림에서 보는 바와 같이, ESS기술은 안정기에 도달하는데 10년 이상이 필요하며, IoT 분야의 경우는 안정기에 도달하는데 5년에서 10년을 예상하고 있음. 결국, 대상 기술을 활용하여 수익을 창출할 수 있는 기간은 5년에서 10년 이상으로 예측됨

Hype Cycle for ESS



Source: Gartner (July 2014)

○ 모방용이성(기술의 난이도)

- MTM은 스마트폰 등 모바일 기기에 장착되어 스팸, 해킹 등을 완벽하게 차단해주는 모바일용 정보보안기술로서 물리적 해킹방지가 가능한 하드웨어 보안 칩임. 따라서 대상 기술을 하드웨어적인 리버스엔지니어링이 불가능함

○ 회피비용(회피설계비용)

- 대상 기술 즉, MTM기반 스마트 단말 보안은 MTM 하드웨어 기술, MTM 보안 소프트웨어 기술, MTM기반 단말 보안 기술 등으로 구성되다.
- 따라서 유사한 기술을 개발하기 위해서는 하드웨어 및 시스템 레벨의 보안 소프트웨어 개발이 필요하므로 개발 기간만 3년 이상이 소요됨. 따라서 개발 비용을 년 25억으로 추산하는 경우 총 75억 이상의 비용이 소요될 것으로 추산됨

○ 대체기술 존재 여부

- 대상 기술은 모바일에 직접 적용 가능한 기술로써, 상용화된 MTM기반 스마트 단말 보안 기술은 아직 없음
- 단, 대상 기술의 유사 또는 경쟁기술로는 Atmel, Infieon, STMicroelectronics사가 있음
  - ✓ 이들 업체는 PC용으로 메인보드에 별도의 하드웨어 보안 칩(TPM)으로 플랫폼의 보안성을 제공함
  - ✓ 모바일용은 아직 규격정의와 소트프웨어 기반의 에뮬레이터로 단계로, 스마트 단말에 대한 적용이 상용화 되지는 않음

○ 경쟁자에게 미치는 영향

- 경쟁자의 시장은 PC용에 적용되는 하드웨어 보안 칩(TPM)인 반면, 대상 기술은 모바일에 직접 적용 가능한 기술이므로 아직 시장이 형성되어 있지 않음. 따라서, 경쟁자의 시장을 나눠가지는 것이 아니고 새로운 수요시장을 창출할 것임

3. 기술의 필요성

○ 파급성

- 대상기술이 적용 가능한 분야는 IoT 디바이스용 보안 기술이므로, IoT 디바이스 제품에는 다양하게 적용 가능함
- 안전한 모바일 환경 구축을 위한 인프라, 단말, 서비스 분야의 집중화된 단말 보안 신기술 개발을 통해 국내 보안 기술의 국제적 경쟁력 확보
- 스마트 단말 내장형 보안 핵심 신기술 및 IPR 조기 확보를 통해 미래 선도 기술에 대한 기술 우위를 확보하고 세계시장 및 기술 주도권 확보 가능
- 신뢰보안모듈 등 스마트 단말 보안 원천기술 확보를 통해 선진국과의 기술개발 제휴 및 협상력 향상
- 현재 국내에서 방송통신 정보보호기술이 타 기술개발에 미치는 영향력 정도를 조사한 결과 높음과 아주 높음이 각각 61.9%, 23.8%로 조사되어 파급성이 높은 것으로 분석됨
- 상대적 기술수준에 대한 전문가들의 국가별 응답에서 미국이 가장 높은 평균 93.1%(100%기준)의 기술수준으로 응답되었으며 그 뒤를 이어 한국이 80.2%의 상대적 차이를 가지는 것으로 조사됨
- 현재의 최고기술 보유국인 미국의 기술수준에 도달하기 위한 기간으로는 약 1~2년 정도가 소요될 것으로 전망됨

< 기술격차 축소 >

주요 기술분야	기술 선도국 및 기업/연구소	기술격차(년)	상대적 수준(%)
방송통신 정보보호	미국	1~2년	80.2
		1년 미만	90
신뢰보안모듈 SoC	Atmel, Infineon, STm	1~2년	85
		1년 미만	95

○ 고객에게 미치는 영향

– 관련 제품/서비스의 국내외 시장규모(향후 매 5년 간 추정)

(단위 : 백만불, 억원)

관련 제품/서비스	시장	1차년도 (2016)	3차년도 (2018)	5차년도 (2020)
모바일 보안시장	해외	2,220	3,298	4,392
	국내	689	1025	1,526

– 예상 제품/서비스의 국내외 시장점유율(생산/판매부터 향후 매 5년 간)

(단위 : %)

예상 제품/서비스	시장	1차년도 (2016)	3차년도 (2018)	5차년도 (2020)
모바일 보안서비스	해외	1	5	8
	국내	5	10	15

– 예상 제품/서비스의 예상매출액(생산/판매부터 향후 매 5년 간 추정)

※ 예상매출액=관련 제품/서비스의 국내외 시장규모×예상 제품/서비스의 국내외 시장점유율

(단위 : 백만불, 억원)

예상 제품/서비스	시장	1차년도 (2016)	3차년도 (2018)	5차년도 (2020)
모바일 보안서비스	해외	22	165	351
	국내	34	124	229

○ 연구개발지원

- 대상 기술은 IoT 서비스를 보호하기 위한 용도로 활용 가능함. IoT 기술은 국가적 차원에서 전략적으로 추진하고 있으며, 2014년 10월 미래창조과학부에서는 “사물인터넷(IoT) 정보보호 로드맵”을 발표한 바가 있음. 따라서 향후 IoT 보안에 대한 정부차원의 지원이 확대될 것으로 예측됨

4. 기술의 차별성

○ 차별성

- 기존에는 모바일 단말의 중요한 데이터를 보호하기 위해 모바일 백신, 원격제어와 관련된 기술이 있으나, 이들 기술은 루팅 등을 통한 악의적인 공격으로부터 중요한 데이터를 보호하기 위해서는 다소 부족한 면이 있음.
- 본 기술은 스마트 단말 장치에서 중요한 정보를 원천적으로 보호하기 위한 수단으로 하드웨어 기반의 보안 기술임
- 개방형 스마트 단말 환경에서, 모바일 서비스 이용에 대한 최고 수준의 안전성 제공
- 악의적 수단(악성코드, 해킹 등)에 의한 스마트 단말의 개인정보 유출 방지 및 모바일 백신으로 탐지가 어려운 시스템 레벨의 Rootkit/Bootkit 공격 방어로 침해 확산 방지 제공
- 스마트 단말을 위한 H/W 기반의 보안 기술 개발과 스마트 단말 보안 플랫폼 중심의 에코 시스템 구축 및 공격적 시장 선점 가능
- 스마트 단말 서비스 환경에 적합한 수출 주도형 전략제품 확보를 통한 시장 경쟁력 강화 및 세계시장 선도
- 국내외적으로 기술 초기 단계에 있는 스마트 단말 보안 플랫폼 기술의 조기 개발을 통해, 스마트 단말 서비스 산업 활성화 및 신규 보안 서비스 시장 창출
- 스마트 단말 서비스 활성화의 걸림돌인 보안 위협 해소 및 서비스의 안전성 및 신뢰성 확보를 통한 모바일 산업의 급속한 발전 기대
- 안전한 스마트 단말 인증 인프라 구축을 통해 다양한 모바일 신규 응용 서비스 시장 창출

- 스마트단말 서비스에 대한 각종 사이버공격으로 인한 사회, 경제적 손실의 최소화

2. 특허성 분석

1. 국내외 특허 동향

○ 기업에서 스마트폰과 같은 모바일 기기를 업무에 활용하기 위해, 기기에 대한 완벽한 통제 방안이 최우선적으로 요구되므로, 모바일 기기의 라이프 사이클 전반에 걸쳐 총체적인 관리를 제공하는 MDM이 급부상하고 있는 것과 궤를 같이 하여, 국내외에서 해당 기술분야에 관한 특허 활동이 점차 활발해지는 경향을 나타내고 있음.

○ 스마트 단말 보안 시스템 기술과 관련하여, 한국의 특허 점유율이 가장 높게 나타나고, 그 다음으로 미국이 뒤따르며, 일본 및 유럽에서의 MTM 기반 스마트 단말 보안 시스템 기술은 많지 않은 것으로 분석됨.

○ 한편, 출원인의 국적의 측면에서, 양적으로 한국 기업(연구소 및 대학 포함)이 해외 기업에 비하여 다수의 특허 출원을 기록한 반면, 질적으로는 한국 기업의 특허 출원과 해외 기업의 특허 출원은 유사한 수준을 갖고 있는 것으로 분석됨.

2. 선행특허분석

특허번호	KR2010-0065012	JP2011-519235	KR2009-0055994	JP2006-018685
특 허 명	이동단말에 대한 사용 제한 방법 및 이를 위한 이동단말	트래픽 암호화 키의 파생 방법	공정편차에 기반한 보안 시스템 및 방법	멀티태스크 실행 시스템
출 원 인	한국전자통신연구원	MEDIATEC INC	(주)시큐트론	NTT DOCOMO INC
기술요약	이동단말에 사용되는 USIM을 MTM의 사용 권한을 가진 단말 소유자만이 MTM에 등록할 수 있게 하고 이후에 MTM을 통한 검증을 통해 등록된 USIM만이 이동단말을 이용할 수 있게 하는 이동단말에 대한 사용 제한을 함.	이동국의 프로세서는 서빙 기지국과 핸드오버 네고시에이션 공정을 실행해, 무선 송수신기 모듈에 의해, 인증 키 (AK) 컨텍스트를 생성하고, 적어도 하나의 트래픽 암호화 키 (TEK)를 타깃 기지국에 파생하며, AK 컨텍스트는 타깃 기지국과 공유하는 복수의 키	공정편차에 기반한 보안 시스템은 반도체 공정의 편차로 인한 소자 간의 전기적 특성 차이를 활용하여 비밀키를 생성하는 비밀키 생성부 및 상기 비밀키를 이용하여 소정의 데이터에 대한 암호 연산을 수행하여 변경된 데이터를 생성함.	복수의 태스크보다 적은 수의 키 데이터와 각 태스크를 식별하기 위한 태스크 ID와 값이 감소하는 일 없이 계속 증가하도록 구성된 단조 증가 카운터로부터의 각 태스크의 생성 시의 출력값을 이용하고, 각 태스크에 독특한 열쇠 스트림을 생성하고, 생성

		로 구성되고, 타겟 BS로 전송되는 정보를 암호화 해, TEK 는 타겟 BS 와 공유되는 비밀 키로, 트래픽 데이터를 암호화 함.		한 당해 키 스트림을 이용하고, 각 태스크용 메모리 공간내의 보호 영역에 기억되는 데이터를 암호화함.
관련도 분석	Y	Y	A	A
	* 관련도 : X - 관련높음, Y - 관련있음, A - 관련은 없으나 참고할 자료 * X, Y - 주요참증에 해당, A - 참고참증에 해당			
조사결과	○ 대상 기술과 관련하여 보유하고 있는 권리의 구성이 적절하게 구성되어 있음 ○ 그러나, 본 기술에 관한 4건의 특허가 모두 최종 등록여부 판단을 받기 전의 출원상태이므로, 권리구성의 적절성, 권리의 범위의 타당성 및 권리의 안정성 등에 관한 판단을 유보하기로 함.			

3. 사업성 및 시장성 분석

1. 사업화 제품화

○본 기술은 기존의 PC나 노트북용 보안칩(TPM)과는 달리 모바일 단말에 직접 적용 가능한 기술로써, MTM을 기반으로 수행되는 스마트 단말용 보안 기술의 형태로 사업화 및 제품화가 가능함.

- 스마트 단말의 확산과 함께 스마트폰을 이용한 모바일 서비스 이용도 급격히 증가하는 추세임
- 따라서 MTM을 이용하여 단말 플랫폼 및 서비스의 안전성을 확보하기 위한 보안 기술은 꼭 필요함
- 특히, IoT 시장이 확대됨에 따라 디바이스의 보안 위협을 방지하기 위한 기술 수요가 증대할 것으로 예상됨

○ 제품 경쟁성

	대상 기술 (MTM기반 보안기술)	경쟁 기술 (TrustZone기반 보안 기술)
기술 개요 및 특징	- HW 보안 칩을 기반으로 한 별도의 안전한 실행환경 제공	- TrustZone을 기반으로 한 안전한 실행 환경 제공
기술의 장점	- 물리적으로 분리된 안전한 저장공간 및 보안 실행 영역 제공(물리적 해킹방지 기능 제공) - TrustZone에 비해 큰 사이즈의 저장공간과 다양한 보안기능 제공 - 기존의 단말에서 제공되는 외부인터페이스(microSD, USB)를 이용하여 적용 능(기존 단말의 HW 수정 불필요) - 특정 벤더에 대해 의존하지 않고, 보안 칩 적용에 대한 독립성 제공	- AP(Application Processor) 칩에 내장된 ARM TrustZone을 이용하므로 추가적인 HW 보안 모듈 장착 불필요
기술의 단점	- 별도의 HW 보안 칩 장착을 위한 인터페이스 필요(비용 증가 발생)	- 제한된 리소스로 인해 아주 작은 실행공간만이 제공됨(따라서, 제한된 보안 기능만 제공)

		- ARM TrustZone이 내장된 AP를 사용하는 디바이스에만 적용 가능. 즉, ARM사의 프로세서에 대한 종속성 가짐

2. 사업화 방법 및 성공요인

○

3. 국내외 시장전망

1) 국내외 시장 규모 및 동향

○ 국내외 시장 규모

- 국내 IT 시장 규모는 2014년 391조원으로 세계 IT시장 4,552조원의 8.6%이지만, 국내 정보보안 시장 규모는 2014년 6조원으로 세계시장(209조원)의 2.9 %수준임(출처: 정보보호산업 전망(KISA, 2014), 2014 국내 정보보호산업 실태조사(KISIA, 2014)

- 세계IT 시장 대비 국내 IT 산업 생산규모

– 세계 정보보호시장 대비 국내 현환 및 전망

○ 국내외 시장 동향

– 정보보호산업 매출액은 2010년 4,669,600백만원에서 연평균 13.0% 씩 성장하는 등 지속적으로 성장하고 있으며, 2014년 국내 정보보호산업 매출액은 총 7,602,219백만원으로 2013년 대비 7.1% 증가함

– 정보보호산업은 타산업과 비교하여, 보안사고의 발생 이전에는 필요성이나 중요성을 인지못하고, 항상 보안사고 이후에 보안대책에 대한 필요성을 언급하고 있음.

– 이는 아직까지 정보보호 산업이 다른 산업에 비해 경기변동에 따른 탄력성은 작다고 할 수 있음.

– 하지만, IT 융합과 사물인터넷 확산에 따라 융합보안 산업이 미래 유망산업으로 대두 되고 있고, 사이버 공간에서의 보안사고가 물리적인 보안사고로 이어질수도 있기에, 점점도 정보보호 산업은 중요하고 발전가능한 미래 산업이 될 것으로 예상됨

– 국내의 경우 애플의 아이폰이 출시된 이후 본격적인 스마트 단말 시대를 열어 국내 스마트폰 가입자는 2013년 8월 현재 3,600만명을 넘겼으며, 지속적으로 증가하고 있음

✓ 스마트폰 보급률 73%로 세계 1위 등극(프랑스 시장조사기관 입소스,'13.7)

– 스마트 단말의 확산과 함께 스마트폰을 이용한 모바일 서비스 이용도 급격히 증가하는 추세임

✓ 스마트폰 기반 모바일뱅킹 이용 금액이 2012년 4분기 1일 평균 1조 719

억원 기록

✓ 전자정부서비스의 경우 2012년 5월 기준 '민원24' 등 모바일 앱 393종, '대한민국정부' 등 모바일 웹 327종이 서비스 중에 있음

- 정부 부처의 경우 스마트 단말을 이용하기에 앞서 안전을 확보하기 위하여 국가정보원의 '국가·공공기관 업무용 스마트폰 보안규격'('10.5), 금융감독원의 '금융권 스마트워크 정보보호 가이드라인'('11.6) 제정
  - ✓ 스마트폰의 업무 활용 시 정보보호를 위한 DO와 DON'T를 규정
  - ✓ AS-IS가 아닌 TO-BE 관점의 규정으로서 추가적으로 개발하여야 할 보안 기능이 많이 포함되어 있음
- 모바일 산업의 활성화를 위하여 행정안전부는 모바일 전자정부 서비스를 위한 공통 기반 구축'사업을 2011년에 착수하는 등 공공부문의 선제 도입을 통한 수요창출, 민간 시장 성장 기반 마련, 핵심 모바일 보안 R&D를 통한 기술력 강화 등을 추진 중임
- 방송통신위원회에서는 스마트폰 등 폭발적인 모바일 인터넷 이용 확산에 따른 잠재적 위협에 선제적으로 대비하기 위해 2010년 12월 '스마트 모바일 시큐리티 종합계획'을 수립하여 2015년까지 안전한 모바일 인터넷 환경 조성을 위해 노력하고 있음
- 국가정보원은 공공부문의 모바일 업무를 위해 2013년 6월 모바일 보안규격 CC 인증 기준인 '스마트폰 보안관리 제품 보안요구사항'을 최종 확정함
- SK인포섹은 모바일 보안 솔루션을 출시
  - ✓ 어플리케이션 레벨의 보안 기능 제공
  - ✓ 기업용 모바일 오피스 연동 및 모바일 보안 관제 솔루션 제공
  - ✓ Mobile Security Processor 개발 중
- SK플래닛은 금융보안연구원과 신뢰플랫폼 기반 전자금융서비스 보안 기술 업무협약 체결(2011.10.4.)
  - ✓ 신뢰플랫폼 기반의 전자금융 응용서비스 개발
  - ✓ 신뢰플랫폼 및 전자금융서비스 보안성 테스트
  - ✓ 국·내외 모바일 전자금융서비스 분야 정보 공유
- 기업에서 스마트폰과 같은 모바일 기기를 업무에 활용하기 위해, 기기에 대한 완벽한 통제 방안이 최우선적으로 요구되므로, 모바일 기기의 라이프 사이클 전반에 걸쳐 총체적인 관리를 제공하는 MDM이 급부상하고 있음, 또한 MDM 시장이 성장을 지속하는 가운데 모바일 보안 CC 규격 발표('13.6)로

공공시장의 수요도 확대될 전망

- ✓ SK인포섹, 지란지교소프트, 루멘소프트, 핸디소프트, 라온시큐어 등 국내 보안업체들의 MDM 사업 매출이 크게 향상됨

- 미국 NIST는 'Mobile Security and Forensics' 프로젝트를 통해 다중 인증, 암호화, 동적 보안정책 컨트롤 등을 포함하여 스마트 단말 보안에 대한 연구 진행 중임
- 미국은 정부 내 모바일 기기 사용시 NIST FIPS 140-2 기반의 데이터 보안 기능을 요구
- EU FP7 SEPIA 프로젝트에서 Infineon, Brightsight, ARM, G&D의 참여로 모바일 및 임베디드 플랫폼 상에서의 보안을 강화하고 개인정보를 보호할 수 있는 기반 기술을 연구 중, 이외 PASSIVE, TECOM 등의 관련 프로젝트가 진행되고 있음
- 일본은 2011년 6월 현재 90개 이상의 기관과 기업이 모여 '일본 스마트폰 보안 포럼(JSSEC, Japan Smartphone Security Forum)을 구성하였으며, 분석, 기술, 보급 등 3개의 WG을 두고 활동 중임
- Google, MS, Apple 등 모바일 운영체제 공급업체들은 지속적인 보안, 관리 기능을 추가하여 공급하고 있음
  - ✓ 애플은 그동안 19개 개발사에게만 허용하였던 MDM API를 2011년 10월 공개 방식으로 전환하여 조직 내 구성원들에게 모바일 단말 관리 기능을 도입하고자 하는 모든 Enterprise Program 가입 고객이 사용할 수 있도록 함
  - ✓ 구글은 안드로이드 어플리케이션을 제작할 수 있는 SDK API의 업데이트시 보안 관리 기능을 계속 추가하고 있음
  - ✓ 후발주자인 MS의 Windows Phone 7은 타 스마트 단말용 OS에서 보안 위협을 불러 일으켰던 테더링, 멀티태스킹 등을 지원하지 않고 외장 메모리도 지원하지 않는 등 취약점이 노출될 수 있는 가능성을 많이 차단하였으나, 사용의 편의성 등을 이유로 개선될 경우 애플이나 구글과 같은 문제들을 갖게 될 것임
- 다수의 기업이 성장이 전망되는 MDM 시장에 뛰어들면서 치열한 시장 경쟁을 펼치고 있음
  - ✓ 전세계적으로 MDM 시장의 강자인 사이베이스를 비롯한 모바일아이언, 젠프라이즈 등이 국내 시장에 진출해 활동 중임

✓ 글로벌 보안 기업인 시만텍, 맥아피 등도 보안에서의 강점을 앞세워 MDM시장에 뛰어들고 있는 상황임

- 국내에 비하여 다양한 스마트폰 단말 보안 기술이 개발되고 있으나 아직은 초기 단계이며, 안전한 스마트 단말 서비스 환경을 보장하기 위한 보안 인프라에 대한 개발은 이루어지고 있지않음
  - ✓ 국외 스마트 단말 보안 기술은 악성코드 차단을 위한 백신 기술뿐만 아니라, 디바이스 보호, 개인데이터보호, 네트워크 접속 제어 기술 등을 포함하여 개발되고 있음

2) 시장의 구조, 경쟁강도 및 진입장벽

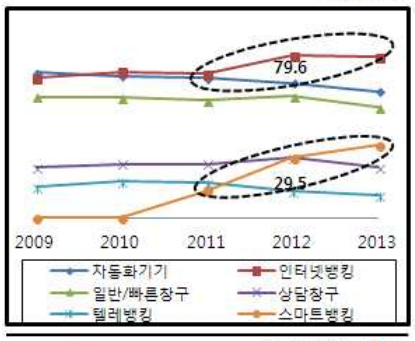
○ 시장의 구조

- 정보보호산업은 “창과 방패”처럼, 끝없이 진화하는 보안위협에 대응하여 지속적인 R&D가 필요한 분야
- 따라서, 보안사고 발생 시 개인, 사회, 국가 등 전 영역에 영향을 주는 등 파급력이 매우 큰 특성을 가짐
- 최근 전 산업의 IT화로 대부분의 산업에 보안기술 적용이 요구되고 있으며, 평상시에는 중요성을 인식 못하지만 사고 발생 시에는 높은 수준의 품질을 요구하게 되는 특징을 가짐
- 정보보호산업은 성장발전 가능성이 높은 신성장 산업이며, 국가의 안위를 지켜주는 방위산업이다. 즉, 개인의 안전과 재산을 지켜주는 보안산업이면서 크게는 각종 테러와 보이지 않는 전쟁(사이버테러 및 정보화 전쟁)으로부터 국가의 안위를 지켜주는 방위 산업
- 또한, 정보보호산업은 차세대 고부가가치 미래지향 산업으로 최근 국내 IT 산업이 스마트 모바일 기기 시장뿐만 아니라 IoT(사물인터넷) 및 클라우드 컴퓨팅 등 큰 변화가 있는 만큼, 이에 대한 정보보안 및 무선 통신망의 안전성 강화와 IT 산업을 기반으로 한 미래 생활에 정보보호 산업 기술이 포함되어 이용되고 있음
- 2013년 국내 인터넷 및 모바일뱅킹 이용건수는 5,429만건, 이용금액은 33조 6,6867억으로 전체 금융거래 중 전자금융 업무처리비중은 87.8%에 육박하는 등 비대면거래 비중이 꾸준히 증가하는 추세

- 사용성이 편리한 스마트 단말이 보급됨에 따라, 일반 PC와 동등 수준의 사용 환경이 제공되는 모바일 지급결제 (Mobile Payment) 등 모바일 전자금융 시장의 급격한 성장 예상
- 2011년1월14일 금융사의 '스마트워크' 지침 마련 계획의 발표와 같이 스마트폰·태블릿PC 보급이 늘면서 금융회사들이 스마트워크 도입을 고려하고 있는 상황

전달 채널별 금융 이용행태

(단위 : %)



자료 : 나이스 알앤씨

인터넷뱅킹 중 스마트폰뱅킹 비중 추이

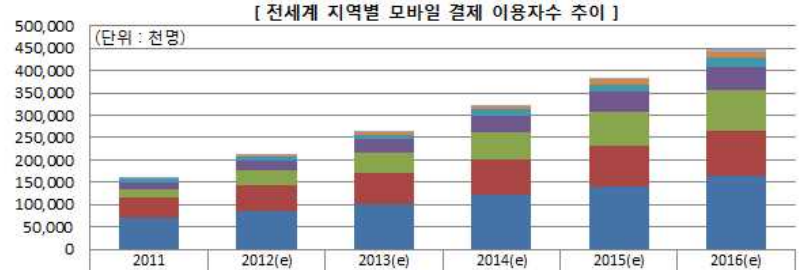
(단위 : % / 일평균 기준)

구 분	2010	2011	2012	2013
이용건수	2.7	15.1	28.0	39.2
이용금액	0.2	1.3	2.6	4.1

자료 : 한국은행

- 스마트폰의 보급률이 높아지면서 모바일 결제 시장도 급성장하고 있음. Gartner는 2012년 모바일 결제 시장 규모를 1,715억 달러로 추정, 2013년에는 이용자 수도 2억 6,600여만명으로 늘어날 것으로 전망, 이러한 추이라면 2016년에는 결제금액 6,170억달러, 이용자 수 4억 4,800만명이 될 것으로 전망

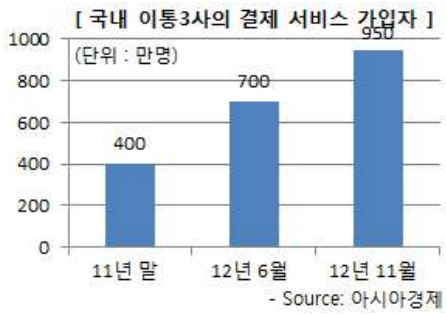
[전세계 지역별 모바일 결제 이용자수 추이]



	2011	2012(e)	2013(e)	2014(e)	2015(e)	2016(e)
중동	935	1,527	2,326	3,440	4,710	6,019
동유럽	2,226	3,882	5,694	7,729	9,935	12,447
남미	7,058	8,456	10,479	13,373	17,268	22,314
서유럽	15,974	22,784	29,734	36,886	44,144	51,514
미국	19,111	32,788	45,518	60,853	75,514	90,653
아프리카	45,539	57,751	69,694	80,530	91,034	101,336
아태지역	69,622	85,031	102,064	120,822	141,364	163,642

- Source : Gartner

– 국내 시장도 전체 시장 규모를 예측한 공식력 있는 보고서는 없지만 관련 기업들의 자료들을 보면 빠른 성장이 진행 중



○ 기업간 경쟁강도

– 최근 휴대폰과 개인 정보관리 등을 통합한 스마트단말이 시장에서 자리를 잡아가고 있으나, 지금까지의 단말가상화 기술은 신뢰성과 성능 측면에서 부족한 점이 많음
  ✓ 대표적으로 VirtualLogix의 VLX, VMware의 MVP, OK-Labs의 모바일 가상화 기술이 있으며, 모두 가상화 모듈 기반 기술임
– 보안 칩 기술 기반의 보안성 및 호환성 기술의 표준을 제정하는 Global Platform은 모바일 환경에서의 신뢰 실행 환경(TEE, Trusted Execution Environment)를 위해 Device Committee에서 TEE Client API 및 TEE Internal API 등의 표준을 제정하고 있음
– 임베디드 단말용 IP 업체인 ARM은 하드웨어 기반의 가상화 보안 기능인 TrustZone 기능을 ARM11 이상 모든 칩에 기본 제공하고 있으며, Qualcomm, TI(Texas Instrument), Samsung System LSI 등 ARM IP를 사용하는 대부분의 Chip Vendor에서 TrustZone 기술을 탑재하고 있음
  ✓ G&D는 Qualcomm과, Trusted Logic은 TI와 협력하여 새로운 비즈니스 모델 창출을 위해 노력중이며, 특히 Trusted Logic은 TI의 OMAP chip에 자사의 솔루션(Trusted Foundation)을 적용하여 유럽시장에 출시함
– STM과 Gemalto는 새로운 파트너쉽을 체결하고 모바일 애플리케이션용으로 설계된 고보안 'secure element ST33' 칩셋, Gemalto의 보안 운영체제,

모바일 단말 소프트웨어, TSM(Trusted Service Management), 보안 개인화 서비스 등을 포함한 다양한 패키지 솔루션 개발을 추진중임

- 한국은행 산하 금융정보화 추진 협의회를 중심으로 금융결제원을 포함한 금융기관 등 45개 기관이 참여하여 microSD 내에 금융정보를 저장할 수 있는 SE(Secure Element)를 내장하여 금융서비스를 지원할 수 있는 휴대용 메모리 카드인 금융 microSD에 대한 표준을 제정하고 시범사업을 추진중임
- 삼성전자에서는 2013년 개인용과 업무용 영역을 분리한 모바일 보안 솔루션인 Knox를 발표함. 삼성 Knox는 Container를 통해 응용 레벨의 도메인 분리를 제공하고 있으며, 파일 시스템에 대한 접근제어를 통해 응용 및 데이터 영역 분리를 제공함
- SK C&C, 삼성전자, SK 인포섹이 공동개발한 모바일 보안솔루션인 엠쉴드는 3G, Wi-Fi 등 스마트 단말 환경에서 보안위협을 탐지하고 차단하며 단말기 도난과 분실 시 원격관리(MDM)가 가능한 모바일 통합 보안솔루션을 제공함
- SK텔레콤의 스마트 시큐리티(Smart Security)는 SK텔레콤이 자체 개발한 단말제어 솔루션인 SSM(Smartdevice Security Management)을 기반으로 안철수연구소, McAfee, Juniper Networks 등과 제휴를 통해 모바일 보안솔루션을 제공함
- 주니퍼의 모바일용 보안 솔루션인 Junos Pulse와 Junos Pulse Mobile Security Suite 솔루션은 모바일 단말에 안티바이러스, 개인 방화벽 기능, 분실, 도난 시 원격 제어, 데이터 백업 및 복구 기능 등을 제공함

○ 진입장벽

- 대상 기술이 적용된 제품의 시장 진입 또는 매출성장에 있어 제도적 요인, 즉 승인, 허가 사항은 없음.

4. 사업화 성공 가이드

1) 사업화 후보기업 요건

○ 통신사업자

○ 보안기술사업자

○ 관련 장비/부품 기업 등

2) 사업화 투자비용

○ 사업화 후보기업의 적극적인 개발 의지만 확보된다면 상용화 추가 개발 (1년미만 개발) 완료후 사업화 가능

3) 법적 검토사항

○ 기술이전 및 실시권 계약 범위 / 라이센싱 및 공동연구 범위 협의

○ 수익성 배분 협의 등

4) 희망 파트너쉽

① 기술이전 (○) ② 라이센싱 (○) ③ 공동연구 ( )

④ 기술출자 ( ) ⑤ 기타 ( )