스마트 디바이스용 칩(ARM7/9/11, UICC 등)에 최적화된 암호(ARIA, SEED, KCDSA 등)의 국가 인증 모듈 및 배포 체계 개발

2015년

총괄책임자 이 옥 연

국민대학교

사업추진 배경 및 필요성

❖ IT 기술 발전에 따른 다양한 융합 서비스 출현

- 스마트그리드, 스마트 워크, 전자정부, U-City, 홈 네트워크 등

❖ 스마트 IT 환경을 위한 스마트 디바이스 등장

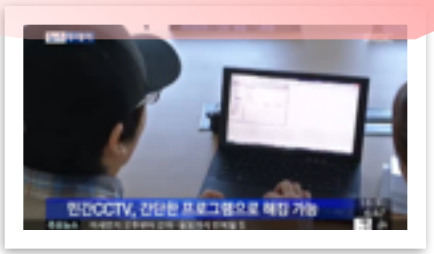
- 스마트 폰, 스마트카드, 전자여권, 스마트 미터, IP카메라 등
- 다양한 통신환경을 통해 편리한 서비스 제공

❖ 공격경로의 다양화 등 사이버 보안위협 증가

- 개인정보유출 등 보안사고 증가
- 원격의 스마트 디바이스에 대한 취약점 등 발생

“CCTV 몰래 훔쳐 보는 사이트 등장… 사생활 침해 논란”
|TBC 2013.01.22

“지능형 CCTV 두 얼굴 : 사생활 노출 보안은 취약”
MBC 2014.01.08



“강남 길거리 CCTV가…” 시민들 “경악”
중앙일보 2013.01.23

“해킹되는 방범용 CCTV”
SBS 2013.11.12

사업추진 배경 및 필요성

암호모듈 검증제도(KCMVP)

- 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증

[전자정부법 제 56조 및 시행령 69조]

제69조(전자문서의 보관 · 유통 관련 보안조치)
① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.
1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행

[지식경제부 고시 제2013-129호 – 지능형전력망 정보의 보호조치에 관한 지침]

제10조 (암호모듈)
① 지능형전력망 사업자는 지능형전력망 시스템에 사용되는 암호모듈로
국가사이버안전센터 IT보안인증사무국의 **검증필 암호모듈을 사용**하여야 한다.
② 지능형전력망 시스템에 사용되는 암호알고리즘은 보안강도 128 비트이상을 만족해야 한다.

- 국가·공공기관에 정보보호시스템 도입 시 암호모듈 검증제도에 의한 검증필 암호모듈을 탑재해야 함
- 암호기능이 포함된 정보보호시스템 [국가사이버안전센터 홈페이지 - 보안적합성 검증 개요]

제 품 군	CC 등급	검증필 암호모듈 탑재
메일 암호화 모듈 / **구간 암호화 모듈** PKI 제품 / SSO 제품 디스크·파일 암호화 제품 문서 암호화 제품(DRM)등 키보드 암호화 모듈 하드웨어 보안 토큰 **DB 암호화 제품** 기타 암호화 제품	**해당사항 없음**	**필 수**

사업추진 배경 및 필요성

용도 및 환경에 따른 KCMVP 암호모듈의 다양성

Platform

intel AMD ARM MIPS TECHNOLOGIES ● ● ●

×

OS

Linux Windows Mac OS iOS android hp UX AIX solaris ● ● ●

×

Algorithm

ARIA	SEED	SHA
HMAC	CMAC	RSAES
CTR_DRBG	EC-KCDSA	DH

● ● ●

KCMVP 검증대상 알고리즘 및 파라미터 조합 **총 82개**

×

Etc..

- 컴파일러 버전
- OS 버전
- 비검증대상 알고리즘 포함 여부
- H/W, F/W, S/W

● ● ●

=

사업추진 배경 및 필요성

다양한 스마트 디바이스 응용환경에 높은 보안성 제공

- 스마트 디바이스에서의 암호화를 수행함으로써 **End-to-End 터널링** 가능
  - 스마트 디바이스용 칩에 대한 최적화를 통해 암호화를 위한 성능 확보
  - **스마트 디바이스의 다양한 응용환경을 고려한 인터페이스 개발**
    ⇒ **응용환경 구축 및 융합에 대한 용이성** 제공

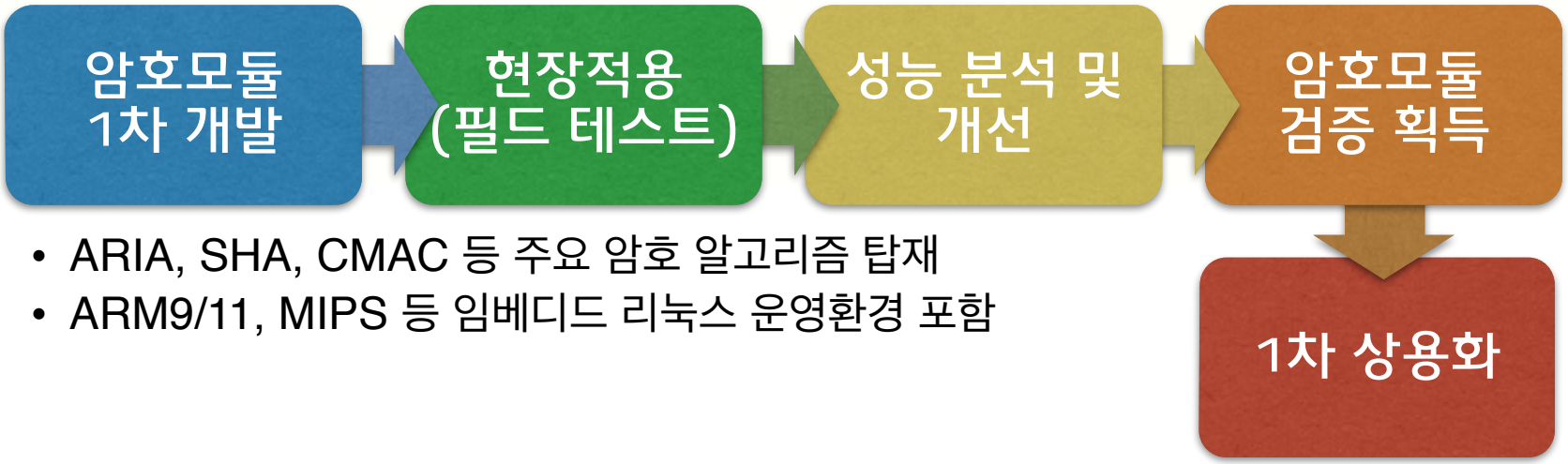
국가·공공시장에 대한 진입장벽 해소

- 암호모듈 기술이전을 통한 중소기업 정보보호제품의 **국가·공공기관 도입** 지원
  - 다양한 스마트 디바이스에 대한 개별 기업의 암호모듈 검증 소요비용 방지
- 빠르게 진화하는 IT 시장에 적절한 암호모듈 개발 기술 확보
- 기업에 대한 암호기술 자문 지원
  - 국가기관과 기업간의 암호 전문지식 및 제도 이해 격차 해소
  - 다양한 정보보호제품의 개발 촉진

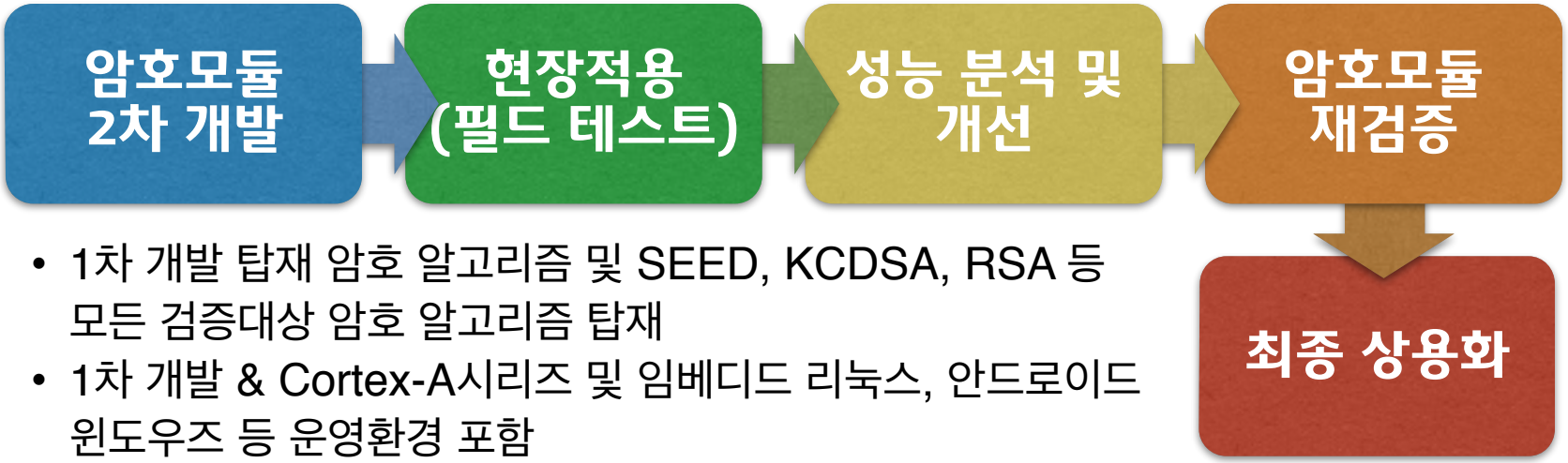
국내 암호모듈 검증제도의 발전 및 암호시장 활성화

- 검증필 암호모듈의 다양화를 통한 국가 경쟁력 확보
  - 다양한 형태(하드웨어/소프트웨어/펌웨어 등) 및 환경(운영체제 등)에 대한 암호모듈 개발 및 검증필 획득
- 정보보안 핵심기술로서의 암호 기술 위상 제고
  - 암호 기술의 연구 결과물의 재조명 및 **실용성 극대화**

사업추진 전략 및 과정



- ARIA, SHA, CMAC 등 주요 암호 알고리즘 탑재
- ARM9/11, MIPS 등 임베디드 리눅스 운영환경 포함



- 1차 개발 탑재 암호 알고리즘 및 SEED, KCDSA, RSA 등 모든 검증대상 암호 알고리즘 탑재
- 1차 개발 & Cortex-A시리즈 및 임베디드 리눅스, 안드로이드 윈도우즈 등 운영환경 포함

주요 개발 결과 및 실적

개발완료 암호 알고리즘

- KCMVP 검증대상 암호 알고리즘 탑재

분류	기능		알고리즘	세부 내용
암호 알고리즘	블록암호		ARIA	- 키 길이 : 128, 192, 256 비트
			SEED	- 키 길이 : 128 비트
	블록암호 운영모드	기밀성	ECB, CBC, CTR	- 블록암호 : ARIA, SEED
		기밀성/인증	CCM, GCM	- 블록암호 : ARIA, SEED
	난수발생기		CTR_DRBG	- 블록암호 : ARIA, SEED
	공개키 암호		RSAES	- 공개키 길이 : 2048, 3072 비트
	키설정		DH	- 공개키, 개인키 길이 : 2048, 3072 비트
			ECDH	- B-233/283, K-233/283, P-224/256
인증 알고리즘	해시함수		SHA2	- 출력 길이 : 224, 256, 384, 512 비트
	메시지 인증 코드	해시기반	HMAC	- 해시함수 : SHA-224/256/384/512
		블록기반	CMAC	- 블록암호 : ARIA, SEED
			GMAC	- 블록암호 : ARIA, SEED
	전자서명		RSA-PSS	- 공개키 길이 : 2048, 3072 비트
			KCDSA	- 공개키, 개인키 길이 : 2048, 3072 비트
			ECDSA	- B-233/283, K-233/283, P-224/256
			EC-KCDSA	- B-233/283, K-233/283, P-224/256

4차년도 개발 목표 및 실적

프로세서 병렬처리 기술(SIMD 등)을 이용한 블록암호 고속화 기술 연구 완료

- SIMD(Single Instruction Multiple Data)
- 명령어 하나로 여러 데이터를 처리하는 기술
- S-box가 없고 간단한 연산(Addition, Rotation, Xor 등)으로 구성된 LEA는 SIMD로 구현이 적합

[SIMD 연산과정 도식화]

- Cortex-A9에서 LEA 참조코드(국보연 제공)에 비해
  약 1.5 ~ 2배의 성능 향상

4차년도 개발 목표 및 실적

경량 고속 블록암호 LEA 구현 경진대회 최우수상 수상

- 주최 : 국가보안기술연구소, 주관 : 한국암호포럼, 한국정보보호학회, 후원 : 미래창조과학부

사업화

사업화 사례

Surveillance

- 지자체 방범, 교통 카메라 무선전송
- 쓰레기 투척감시 카메라 영상 전송
- 버스장착 카메라로 주▪정차 위반 단속
- 시위현장 영상 실시간 무선전송
- 항만 감시 카메라 무선 전송

Smart Power

- EHP 수용가와 전력거래소 간
- 변전소와 전력 감시 센서 간
- 전기차 충전기와 관리서버 간

WSN Wireless Sensor Network

- 해상부표와 지상국 간 무선전송
- 기상 센서 및 영상정보 무선전송

Military

- 군 주요시설 온▪습도 센서 무선전송
- 훈련장 이동차량의 영상 및 데이터 무선 전송
- **** 이동감시 무선 영상전송

ITS

- UTIS RSE망 보안 전송
- 교통정보 영상정보 무선 전송

Remote Control

- 정수장, 가압장의 원격관리
- 배수지, 펌프장의 원격관리

결 론


검증필
암호모듈의 다양화로
정보보안
핵심기술로서의
암호 기술 위상
제고
다양한
응용환경을 고려한
인터페이스
제공
KCMVP
검증필
암호모듈
다양한
스마트 디바이스
응용환경에
높은 보안성
제공
중소기업의
국가, 공공기관
정보보호제품 도입을
위한 인프라 마련

Thank You