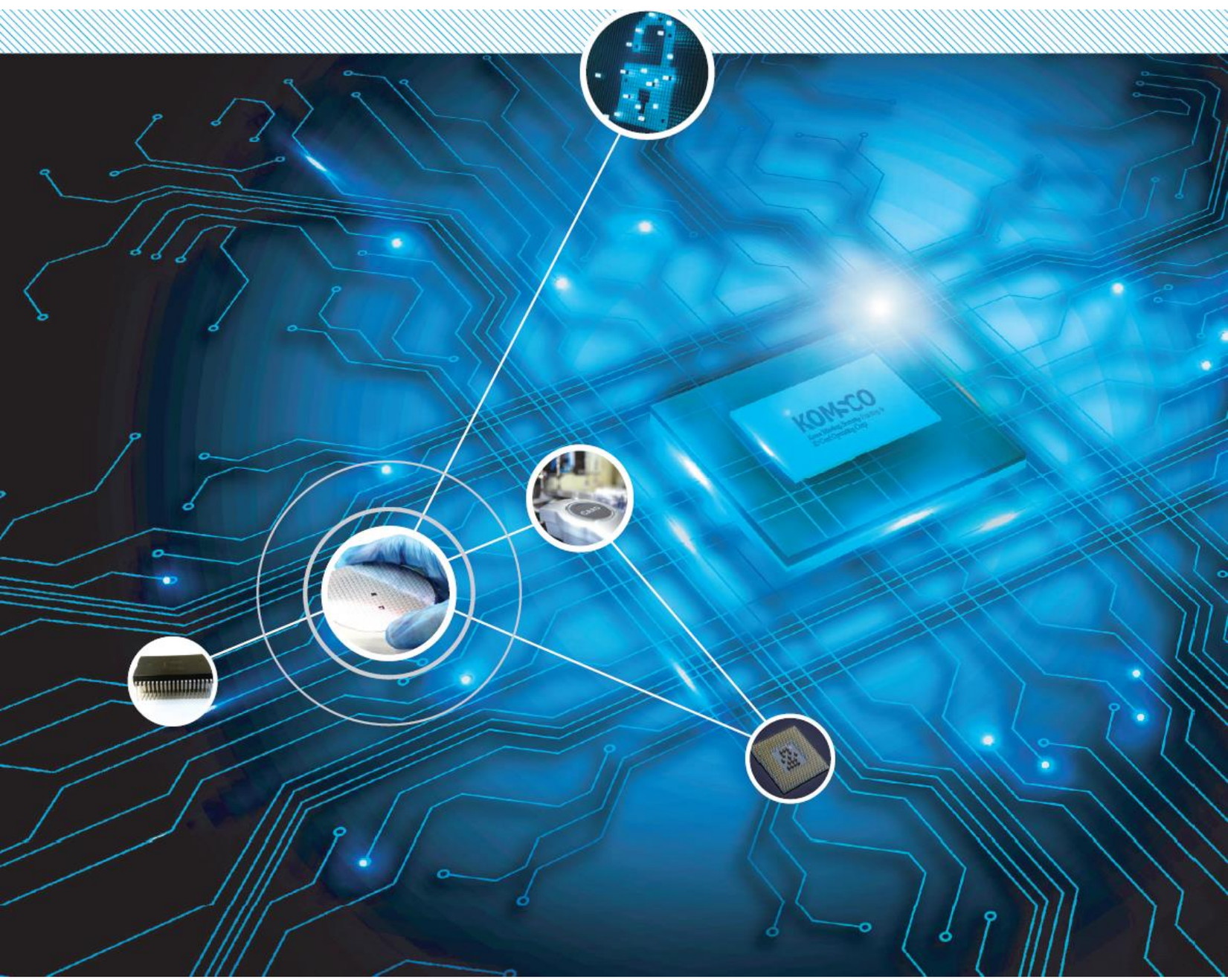
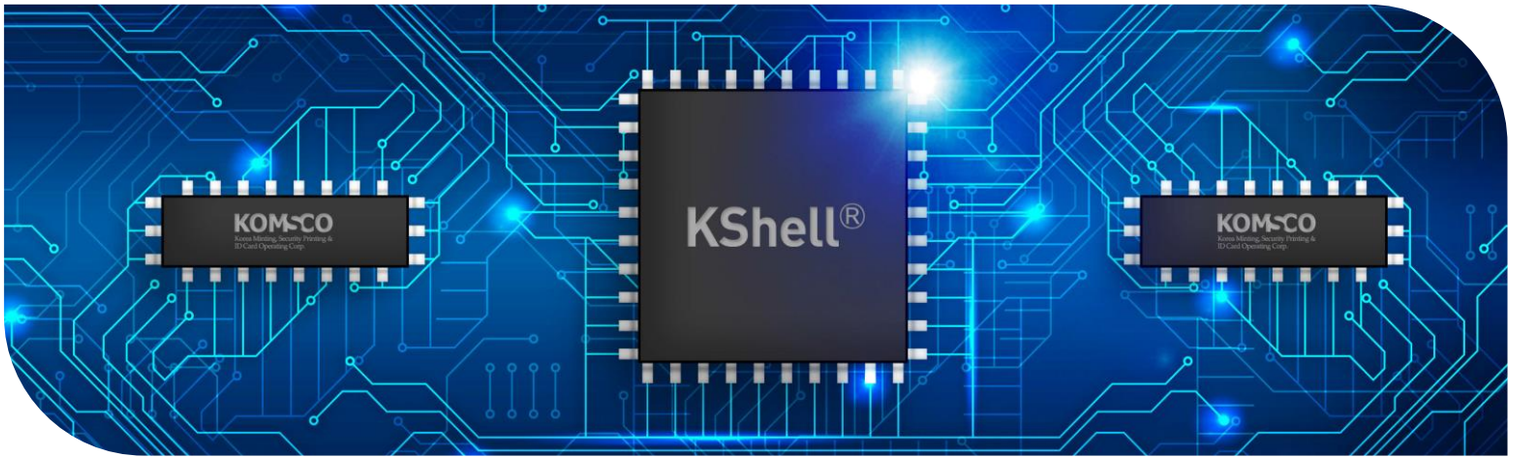
KOMSCO
Korea Minting, Security Printing &
ID Card Operating Corp.

New Directions for IoT Security

KShell®

HSM based Secure Element for IoT/M2M environment





What is Secure Element(SE)?

보안모듈(SE : Secure Element)은 신뢰할 수 있는 인증기관이 제시한 규칙과 보안 요구사항에 따라 암호 통신, 응용프로그램 및 중요 정보, 암호화 데이터 등을 안전하게 관리/저장할 수 있는 하드웨어(일반적으로 단일 칩) 형태의 위변조 방지 솔루션입니다. 보안모듈은 최근 신용카드 및 모바일 장치의 보안 강화를 위해 채택되고 있는 높은 수준의 보안 기술입니다.

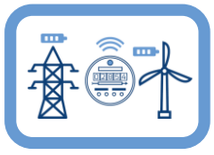
Application Areas

지능형 전력망 암호화
전력공급망 데이터 보안
도전(盜電) 감지 시스템 보안

스마트그리드

- 전기,가스,온도제어
- 스마트 미터링
- 대기전력 수요관리

적용 가능 장치 :
스마트미터링 장비
전력 공급 스위치
RTU(Remote Terminal Unit)



스마트 홈

- 스마트 홈 기기제어
- 도난 방지 시스템
- 공조 시스템 제어

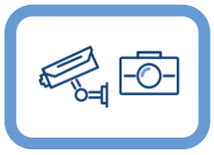
적용 가능 장치 :
스마트플러그,스마트전구
전기 사용량 측정 센서
홈 게이트웨이
온도제어 시스템

KShell®
한국조폐공사
보안모듈 솔루션

공공 IoT 장비

- CCTV/영상 녹화 장치
- 신원 인증 기술(FIDO)
- 시설 보안(출입통제)

적용 가능 장치 :
CCTV
출입통제 시스템
기타 보안장치



헬스케어

- 헬스케어 / 원격진료
- 생체신호 모니터링
- 지능형 의료 시스템

적용 가능 장치 :
웨어러블 헬스케어 장치
스마트 의료장비

커넥티드 카

자동차 블랙박스
스마트 카 커뮤니케이션 보안
커넥티드 카 보안관리

의료정보 접근권한 관리
통합 의료정보 보안
원격 진료 데이터 보안

KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.

KShell®
KOMSCO Secure Element

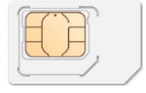
KShell® Family

What is KShell?

KShell®은 한국조폐공사의 보안모듈 브랜드입니다.

KShell® 은 CC(공통평가기준), KCMVP(한국형 암호모듈검증)등 국내외의 엄격한 보안성 인증을 통과하였으며, 강력한 암호화 알고리즘이 탑재되어 암호화 키의 발급 및 보관, 사물인터넷(IoT/M2M) 기기에 대한 **암호통신, 전자봉인, 데이터 암호화 기능**을 수행할 수 있습니다. 다양한 폼팩터와 인터페이스를 제공하므로 제품의 종류나 형태와 관계없이 필요에 따라 다양한 장치에 적용이 가능합니다.

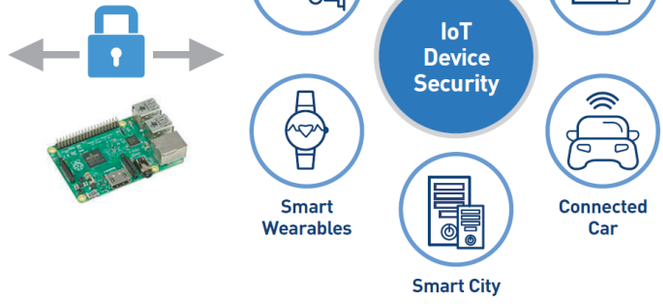
Form Factor Types

구분	기본형태	기기 내장형	탈착 가능형	
		SMD 타입	SIM/USIM 타입	Micro SD 타입
폼팩터				
응용분야	국가신분증, 여권 스마트카드 등	스마트미터링, 통신모듈, 군용장비 보안 등	스마트미터링, 스마트폰, 태블릿PC 등	주유기, CCTV, 스마트 디바이스 등

Usage

KShell® 42 (KCMVP,CC 인증 제품)

KShell® 31 (CC 인증 제품)



KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.

KShell®
KOMSCO Secure Element

Product Portfolio

KShell은 사용된 칩의 종류에 따라 2종의 제품, 3종의 폼팩터로 구분되어 있습니다.
제품별로 지원 가능한 기능과 인터페이스, 성능에는 약간의 차이가 있습니다.

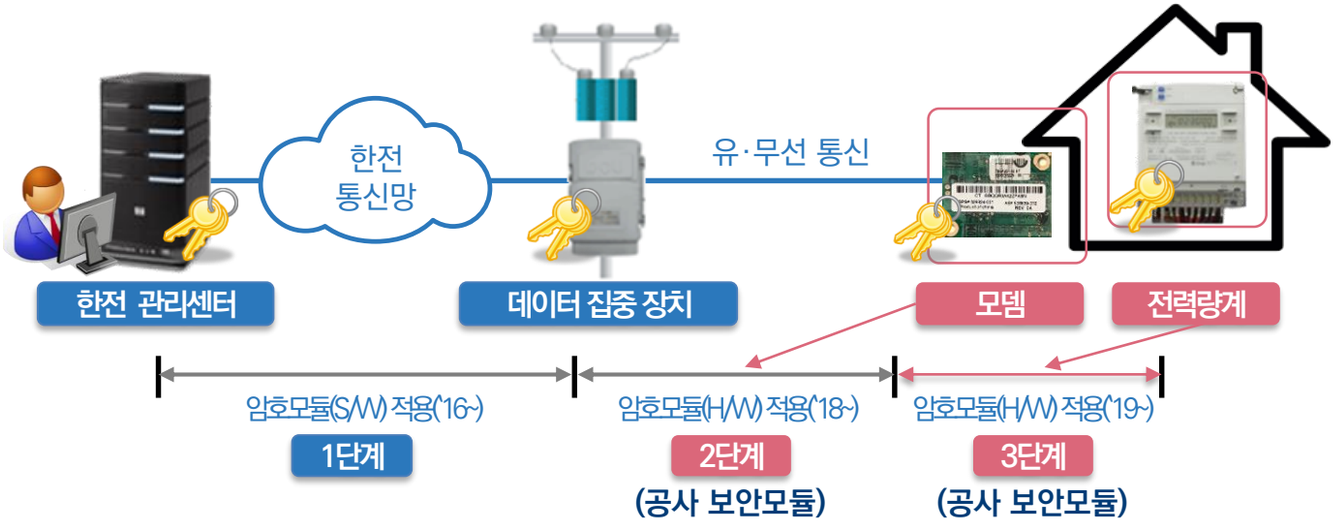
제품	제품 특징	
	KShell® 31	KShell® 42
칩	• SLE78CLFX/CAFX4000PM (Infineon, FLASH)	• SLM97CUINFX1M00PE (Infineon, FLASH)
보안 인증	• Chip : CC EAL 6+ • COS : CC EAL 5+	• Chip : CC EAL 5+ • COS : KCMVP
메모리	• FLASH : 404Kbytes	• FLASH : 1Mbytes
외부 인터페이스 (I/F)	• SD • SPI Contact T=0/T=1, up to 223Kbps (부품 간 인터페이스 : ISO7816)	• ISO7816 (Contact T=0/T=1, up to 223Kbps) • SPI (up to 4Mbps) • I^2C (up to 100Kbps)
폼팩터	• SD (Micro)	• SIM (Mini / Micro) • SMD (VQFN32) • SD (Micro)
플랫폼	• JavaCard v2.2.2 • VISA GlobalPlatform v2.1.1 • VGP Configuration 3(DAP, DM)	• JavaCard v3.0.4 • VISA GlobalPlatform v2.1.1 • VGP Configuration 1
암호엔진	• SEED, ARIA • SHA (up to 512bit) • RSA (up to 2048bit) • ECC (up to 512bit) • AES, DES/TDES via co-Processor	• ARIA 128/192/256bit • SHA 256bit, HMAC 256bit • ECC 256bit • CTR_DRBG(ARIA 128bit) • AES 128/192/256bit • TDES 128/192bit
기타	• Operating Temperature : −25℃ ~ 85℃ • Data Storage : 8GB	• Operating Temperature : −40℃ ~ 105℃ (M2M industrial extended endurance)

KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.

Key Business Reference

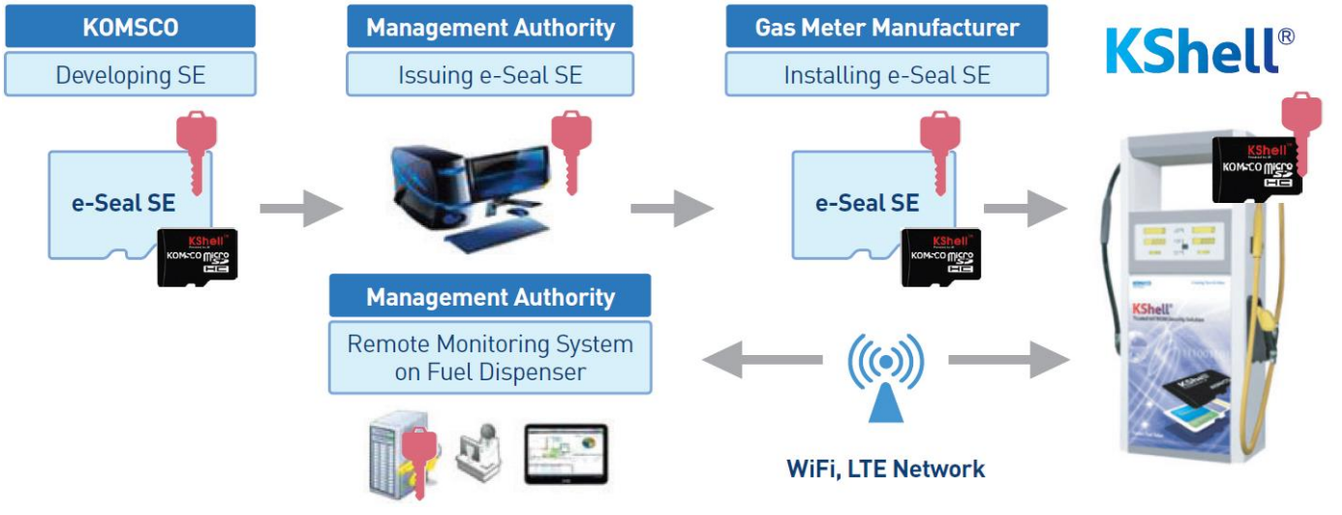
1 KShell42 - 한국전력공사 지능형전력망을 위한 보안모듈 솔루션

한국조폐공사는 한국전력공사 지능형전력망 인프라에 포함되는 보안모뎀, 전력량계 등의 원격 계량 정보 등 통신 데이터의 안전한 전송을 위해 DLMS/COSEM security, DTLS/TLS/EAP-TLS, 전자봉인(Secure booting, FW Integrity) 기능을 수행하는 보안모듈을 공급하고 있습니다. 공사의 보안모듈 **KShell42**에는 산업용 칩이 적용되어 추위, 더위 등 극한 상황에서도 높은 안정성을 보장합니다.



2 KShell31 - 주유기 조작방지를 위한 전자봉인용 보안모듈 솔루션

한국조폐공사는 2015년부터 한국기계전기전자시험연구원(KTC)에 주유기 보드에 탑재된 주유 SW의 불법 조작을 탐지할 수 있는 전자봉인용 보안모듈 **KShell31**을 공급하고 있습니다. **KShell**이 소프트웨어의 불법 조작을 탐지하면 주유기는 관리센터로 알림을 전송합니다. 주유기 보안모듈은 '18년 6월부터 신규 주유기에 의무 적용되었습니다.



KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.

Connecting Trust, Creating Value

KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.

KOMSCO (Korea Minting, Security Printing & ID Card Operating Corp.)
ID BUSINESS DEPARTMENT

80-67 Gwahak-ro, Yuseong-gu, Daejeon, 34132, South Korea
www.komsco.com

Business Department
Tel. 82-42-870-1291
E-mail. hslee@komsco.com

Technical Support Department
Tel. 82-42-820-1591
E-mail. jkyang@komsco.com