

Digital Trust[®]



경량화 · 저전력 암호 알고리즘 모듈 및 인증서 기반 기기 인증 솔루션

Magic | IoT

Copyright © DreamSecurity Co., Ltd. All rights reserved.

Magic IoT는 유·무선 통신으로 연결되는 디바이스를 통해 사람과 사물, 사물과 사물 간의 정보가 교류되고 상호 소통이 가능하도록 하는 지능형 인프라 및 서비스의 핵심 보안 기술로 CPU 성능, 메모리 용량, 소비전력 등의 제약을 갖는 IoT 환경에 최적화된 경량화·저전력 암호 알고리즘 모듈 및 PKI 기반 인증서 발급을 통한 기기 인증 솔루션입니다.

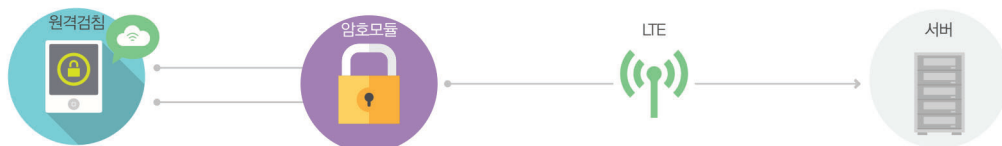
Magic IoT는 스마트홈, U-헬스케어, 커넥티드카, 스마트팩토리 등 다양한 산업분야에 적용되는 IoT 기기(센서, CCTV, 무선단말 등)에 인증서(Certificate)를 주입하여 기기의 무결성 및 접근 권한 기능을 제공합니다.

Digital Trust

Magic IoT(사물인터넷 환경 기반 보안 솔루션)

IoT 보안 : 경량화 · 저전력 암호 알고리즘 모듈 및 인증서 기반 기기 인증 솔루션

경량 암호화

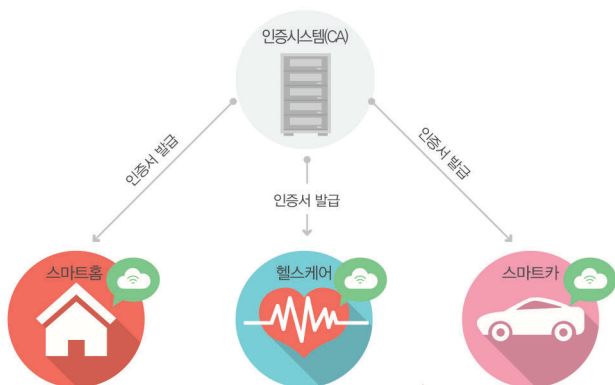


암호화	우수한 성능	다양한 환경 지원
<ul style="list-style-type: none"> 국가정보원 검증필 암호모듈 LEA 알고리즘 탑재 안전한 난수생성기를 통한 비밀키 및 키쌍 생성 표준 적합성에 의한 암호 알고리즘 구현 RSA Blinding 적용으로 Time attack 방지로 강력한 보안성 제공 	<ul style="list-style-type: none"> 연산 알고리즘 및 최적화된 알고리즘의 성능 보장 용량이 작은 휴대단말에도 적용된 알고리즘 집적화 다양한 플랫폼에서 최적화된 성능 제공 	<ul style="list-style-type: none"> Windows, Linux, Unix 등 서버 환경 지원 Windows, Mac OS, Linux Embedded (ARM, MIPS, TILERA) 지원 iOS, Android 지원 JDK 1.4 이상 지원

적용사례

- 한국전력공사 : 스마트그리드 서비스에서 국가정보원 검증필 암호모듈을 사용해야 하며, 원격검침용 SKT LTE 무선모뎀의 데이터 암호화를 위하여 IoT 보안 영역의 경량 암호화 적용

PKI기반의 기기 및 사물 인증



인증서 발급	IoT환경 최적화	기술 우수성
<ul style="list-style-type: none"> 기기 및 사물에 대한 인증서 발급 <ul style="list-style-type: none"> ※ 유 · 무선 인증서 발급 발급된 인증서를 기기 및 사물에 주입 HSM을 이용한 안전한 키 관리 	<ul style="list-style-type: none"> 진단기, 제어기 등 제한된 메모리 사용으로 CVC 인증서 포맷 활용 제한된 CPU 성능으로 최소한의 연산을 수행하는 RSA 공개키 알고리즘 사용 LEA 알고리즘 탑재 	<ul style="list-style-type: none"> Multithread 구현으로 최적의 프로세스 구현 객체지향적인 설계로 최신 PKI 표준적용을 위한 모듈별 확장 및 최적화 용이 유 · 무선 알고리즘 동시 지원

적용사례

- ○○자동차 : 차량 진단기와 고급 승용차에 기기 인증서를 발급하여 인가된 진단기와 차량에서만 정비 서비스 제공하며, 국내 최초 커넥티드카의 기기인증서 상용화