



## NXP, 마이페어 울트라라이트 AES 발표... 비접촉 일회용 애플리케이션 보안 강화

- EAL3+ 보안 인증과 AES(고급 암호화 표준) 사용, 마이페어 울트라라이트 제품군 최고의 안전성 제공
- RFID 기반 비접촉식 티켓과 카드를 보다 안전하고 편리하게 발행할 수 있는 기술 제공
- 미국 국립표준기술연구소(NIST) 권장 키(key) 길이 준수 암호화 사용으로 뛰어난 인증 제공

2022년 2월 24일, 서울 - NXP 반도체가 오늘 일회성 비접촉 접근 애플리케이션에 최고 수준의 보안을 제공하는 마이페어 울트라라이트(MIFARE Ultralight) AES를 발표했다. 마이페어 울트라라이트 AES는 표준 AES 인증과 공통 기준(Common Criteria) EAL3+ 보안 인증을 사용한다.

사물간의 연결이 점차 확대되면서, 보안은 많은 제품의 핵심 기능으로 자리잡았다. 마이페어 울트라라이트 AES는 솔루션 제공업체가 비접촉식 티켓과 카드를 보다 안전하고 편리하게 발행할 수 있는 기술을 제공한다. 이는 RFID 기반 게스트 카드, 이벤트 티켓, 액세스 패스, 로열티 카드 및 대중 교통 티켓 등 다양한 티켓과 카드를 포함한다.

마이페어 울트라라이트 AES는 [미국 국립 표준 기술 연구소에서 권장하는 키\(key\) 길이](#)를 준수하는 암호화를 사용한다. 이는 잘못된 보안 인증 시도를 차단하는 옵션을 비롯해 뛰어난 인증 및 데이터 액세스 보안을 제공한다. 따라서 투숙객 보호, 객실 접근 보안, 스마트 시티의 안전한 교통 티켓 발권 등을 지원한다. 개발자는 마이페어 울트라라이트 제품군과 동일한 메모리 구조를 갖춘 새로운 IC를 활용해 제한된 사용 목적의 티켓팅 애플리케이션에서 빠르고 강력한 보안을 구현할 수 있다.

NXP의 마이페어 스마트 시티(Smart Cities) 부문 매니저 안드레 페르세일러(Andre Perchthaler)는 “우리는 호텔 키 카드부터 대중교통, 이벤트 티켓에 이르기까지 개발자가 안전한 비접촉식 접근을 대규모로 쉽게 구현하도록 한다. 서비스 제공업체는 AES와 같은 단일 표준 기반 암호화 방식을 활용해 사기 등을 방지하며, 통합 및 키 관리를 간소화할 수 있다. 마이페어 울트라라이트 AES를 통해 모든 마이페어 제품 포트폴리오는 일회성 뿐만 아니라 다중 애플리케이션에도 AES 인증을 제공한다. 또한, 액세스 인프라를 단순화하고 복잡성과 유지 관리 비용을 절감한다”라고 설명했다.

### 세부 사항:

- 128 비트 키 길이의 AES 인증과 잘못된 인증 시도를 제한하는 명령 카운터(Command Counter) 옵션으로 더욱 안전한 데이터 액세스
- 무결성 보호를 위해 CMAC 로 구성 가능한 보안 메시징 통신 모드
- 강화된 개인 정보 보호를 위해 임의 ID 지원 옵션을 제공하는 7 바이트 UID
- 공개 키(사전 프로그래밍)에 기반해 제품 검증을 허용하는 ECC 기반 원본 서명
- NXP 툴 지원으로 IC 의 출처를 확인하는 AES 기반 원본 검사
- ISO/IEC 14443 A -2 / -3 준수
- 144 바이트 EEPROM 사용자 메모리



더욱 자세한 정보는 [여기](#)에서 확인할 수 있다.

### **NXP 반도체 소개**

NXP®반도체(나스닥: NXPI)는 혁신을 통해 더욱 스마트하고 안전하며 지속 가능한 세상을 만들고 있다. NXP는 임베디드 애플리케이션용 보안 연결 솔루션의 선도 기업으로서, 자동차, 산업 및 IoT, 모바일, 통신 인프라 시장의 혁신을 주도하고 있다. NXP는 60년 이상의 전문성과 경험을 바탕으로, 전 세계 30개 이상의 국가에서 31,000명의 직원을 고용하고 있다. 2021년 매출은 미화 110억 6천만 불이다. 더 자세한 내용은 [www.nxp.com](http://www.nxp.com)에서 찾아볼 수 있다.