



## NXP LPC55S16 MCU, PSA 레벨 2 및 SESIP 레벨 2 인증 획득

**2020년 11월 19일** – NXP 반도체는 PSA 인증(PSA Certified) 제도와 IoT 플랫폼을 위한 글로벌 플랫폼 보안 평가 제도(SESIP) 모두에서 LPC55S16 MCU 제품이 레벨 2 인증을 획득했다고 발표했다. PSA 인증 제도는 Arm이 공동 개발했으며, SESIP는 임베디드 프로세서에 대한 보안 보호 프로파일을 이용한다. IoT 및 산업용 엣지 애플리케이션이 빠르게 확장됨에 따라 기기 보안과 데이터 보호가 무엇보다 중요해졌다. 이러한 가운데 해당 인증은 NXP의 설계에 의한 보안(security-by-design) 방식을 검증하고 NXP 지원 엣지 장치에 대한 OEM과 소비자의 신뢰를 더욱 강화한다.

NXP EdgeVerse™ 컴퓨팅 및 보안 포트폴리오에 속한 LPC55S16 MCU는 Arm® Cortex®-M33 코어를 기반으로 하는 범용 LPC5500 MCU 시리즈 중 하나이다. 이 시리즈는 40nm NVM 프로세스 기술, 고급 보안 및 혼합 신호 기능을 활용해 성능 효율성을 제공한다.

SESIP와 PSA 인증의 테스트 및 검증은 세계 유수의 독립 보안 평가 연구소인 브라이트사이트(BrightSight)가 실시했다.

LPC55S16 MCU가 보안 견고성을 검증하는 종합 보증 프레임워크에 기반한 PSA 인증 레벨 2를 달성함으로써, 장치 제조업체들은 추가적인 보안 테스트를 줄이고 신제품 출시 속도를 향상할 수 있게 됐다. PSA 루트 오브 트러스트(PSA-RoT) 보안 클레임에 대한 25일 기한의 실험실 평가를 통해, 확장 가능한 소프트웨어 공격에 대한 디바이스의 보호 능력도 입증했다.

SESIP 2를 달성하기 위해 LPC55S16 MCU는 브라이트사이트에서 발행한 소스 코드 분석 및 침투 테스트를 거쳤으며, 다른 독립 인증 기관의 검증을 받았다. SESIP 인증은 제품의 보안 클레임이 테스트 및 검증을 받았음을 보증하고, LPC55S16 MCU의 기본 공격 가능성에 대한 저항성을 입증한다. SESIP는 고객이 최종 애플리케이션에 대한 인증 과정에서 LPC55S16 MCU 검증 결과를 재사용하는 것을 허용한다.

LPC55S16 MCU의 통합 보안 기능은 다음과 같다.

- 주변 장치를 안전하게 격리하여 중요한 구성 요소에 대한 공격 위험을 줄이는 기능을 통해 시스템 전반의 소프트웨어 보호를 가능하게 하는 Arm TrustZone® 기술
- AES-256 가속기로 기밀성을 보장하고, 보안 해시 알고리즘(SHA2) 가속기로 보안 통신 및 보안 부팅의 무결성 제공



- 온칩 플래시의 실시간 암호화 및 암호 해독이 가능한 PRINCE 모듈로 데이터를 안전하게 저장하고 소프트웨어 지적 재산권(IP)의 자산 보호
- CASPER 암호화 코프로세서를 통한 다양한 비대칭 암호 알고리즘의 하드웨어 가속화로 보안 연결 설정
- 전용 온칩 SRAM을 사용해 보안 스토리지를 위한 고유한 장치 루트 키(64~4096비트)를 구축하는 물리적 복제 방지 기능(PUF)
- 식별을 위한 128비트 고유 장치 일련 번호(UUID)
- 진정한 난수 생성기(TRNG)
- 코드 감시를 통해 펌웨어 실행 흐름에 대한 무결성 검사
- 보안 디버깅을 위한 디버그 인증 프로토콜

### EdgeLock™ 인증

LPC55S16 MCU는 EdgeLock 인증 프로그램의 일부다. 업계 표준을 충족하도록 설계된 EdgeLock 인증 프로그램에 속한 NXP 제품 및 서비스는 제품 개념에서 출시에 이르기까지 검증된 보안 개발 프로세스 및 평가 기준을 준수해 고객이 보안 과제에 대해 신뢰할 수 있는 솔루션을 제공받을 수 있게 한다.

### 제품 소개

LPC55S16 MCU에 대한 자세한 내용은 링크에서 확인할 수 있다.

EdgeLock 보장, PSA 인증 및 글로벌플랫폼 SESIP에 대한 자세한 내용은 각 홈페이지에서 확인할 수 있다.

### NXP 반도체 소개

NXP® 반도체(나스닥: NXPI)는 더욱 편리하고 안전하며 더 나은 삶을 위한 첨단 솔루션을 개발하여, 안전하게 연결되는 스마트 월드를 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 29,000명의 직원을 고용하고 있다. 2019년 매출은 미화 88억 8천만 불이다. NXP 관련 뉴스는 [www.nxp.com](http://www.nxp.com)에서 찾아볼 수 있으며, NXP 반도체 블로그 (<http://blog.naver.com/nxpkor>) 에서도 NXP 관련 정보를 확인할 수 있다.