NXP, PUF 복제 방지 기능 탑재 보안칩 업계 최초 출시

인트린직 ID 社와 라이선스 계약 체결로 NXP 의 보안 기능 강화

2012 년 2 월 22 일 - NXP 반도체 (NASDAQ: NXPI)는 인트린직 ID(Intrinsic-ID) 社의 물리적 복제 방지 기능 (PUF: Physically Unclonable Function)을 탑재한 스마트카드와 보안칩을 업계 최초로 시장에 출시한다고 오늘 발표했다. 물리적 복제 방지 기능(PUF)은 모든 반도체 제품에 존재하는 고유의 '지문'을 이용해 암호 키를 보호함으로써 개별 반도체 칩의 데이터 도난을 방지하는 혁신적인 기술이다. 이 기술을 사용하면 보안칩의 복제가 사실상 불가능해 역설계 및 컴퓨터 데이터 침해 행위를 방지할 수 있다.

전세계적인 도시화, 문서의 디지털화, 금융 보안 강화, NFC 도입 증가 등으로 인해 보안용 칩의 도입이 그 어느 때보다 활발히 이루어지고 있으나, 동시에 보안칩의 기능을 저해하고 정보 침해 공격 또한 정교해지고 있다. 이를 해결하기 위해 NXP 는 인트린직 ID 의 PUF 기술을 자사의 보안 마이크로컨트롤러인 SmartMX2 에 탑재하여 보안성을 대폭 향상시켰고, NFC 모바일 결제, 전자티켓, 전자정부 및 사이버 보안 등의 애플리케이션을 강화했다.

인트린직 ID 의 CEO 핌 투일스(Pim Tuyls)는"데이터 복제, 조작 및 절도 방지를 위해 사용되는 비밀 키와 암호 키를 알아내려는 정교한 도구들과 기법들이 광범위하게 사용됨에 따라 스마트카드 보안에 대한 우려가 증대되고 있다" 고 말하고, "PUF 기술은 이러한 문제를 해소하기 위한 가장 이상적인 방법이며, 특히 NXP 의 시장 선도적 보안 IC 솔루션과 접목되었을 때 그 효과가 더욱 클 것으로 본다"고 밝혔다.

NXP 반도체 ID 사업부의 수석부사장 뤼디거 스트로(Ruediger Stroh)는"전세계적으로 NFC 탑재 휴대폰에서 스마트카드 또는 유사 기능을 사용하는 일이 폭증하고 있다" 고 말하고, "그러나 사용자들이 보안문제로 여전히 우려하고 있기 때문에 eID 카드, 금융거래 카드, NFC 스마트폰에서 최고 수준의 보안을 제공하는 것이 매우 중요하다. PUF 기술을 탑재한 SmartMX2 는 스마트 라이프 솔루션의 보안과 신뢰성을 향상시키므로 사용자의 걱정을 해소할 수 있을 뿐 아니라, 이를 통해 NXP 의 고객업체들은 중요한 경쟁 우위를 점할 수 있게 된다. 이런 점에서 PUF 분야의

명실상부한 선도업체인 인트린직 ID 와 라이선스 계약을 체결하게 되어 대단히 기쁘다"고 밝혔다.

SmartMX 와 PUF 기술

현재 인트린직 ID 의 PUF 기술은 NXP 의 SmartMX2 보안 칩의 차세대 제품군에 탑재되고 있다. SmartMX2 는 독일연방정보보안국(BSI)의 공동 기준 EAL 6+ 인증을 세계 최초로 획득한 보안 마이크로컨트롤러이다. SmartMX2 의 IntegralSecurity™ 아키텍처는 역설계, 반 침투형(semi-invasive) 공격 및 비 침투형(non-invasive) 공격으로부터 칩을 보호할 수 있는 100 개 이상의 보안 기능을 제공한다. 여기에 PUF 기술이 추가됨으로써 디지털 암호키가 기기에 항시 존재해야 할 필요가 없어지기 때문에 역설계 공격으로부터 칩을 보다 잘 보호할 수 있다.

PUF 는 SRAM 기술의 물리적 특징을 기반으로 한다. 시큐어 엘리멘트의 작동 시작 후 사용된 셀은 랜덤 방식으로 초기화되는데, 이렇게 비트가 0 과 1 사이를 왔다 갔다 하는 스타트업은 칩마다 다르게 나타난다. 이처럼 스타트업 후에 보이는 특징이 일종의 독특한 지문으로 작용하여 암호 키나 메모리를 보호하기 위한 열쇠로 사용될 수 있다.

전세계 ID 시장의 최대 공급업체인 NXP 는 비접촉식 기술과 보안 기술 부문에서 차지하고 있는 자사의 선도적 위치를 활용하여 완벽한 ID 솔루션을 제공한다. NXP 의 트러스티드 스마트 기술 솔루션(Trusted Smart Life Solutions)을 통해 전자정부, 금융, 모바일 거래, 승차권/항공권 등의 교통관련 전자발권, 접근 관리, 인프라스트럭처, 기기 인증, RFID 태깅 및 게임을 아우르는 광범위한 애플리케이션에 보안 및 비접촉 성능이 제공된다. NXP 는 전자여권 사업을 추진 중인 전세계 102 개국 중 86 개국 등 다양한 고객을 대상으로 20 억 여 개 이상의 SmartMX 칩을 출하했다.

오는 2 월 25 일부터 28 일까지 스페인 바르셀로나에서 개최되는 모바일 월드 콩그레스(Mobile World Congress)의 참가자들은 Hall 7, A111 에 위치한 NXP 부스를 방문해 트러스티드 모바일 스마트 라이프 솔루션(Trust Mobile Smart Life Solutions)을 경험할 수 있다. 동 행사 기간 동안 NXP 는 인트린직 ID 와 협력해, 인트린직 ID 의 세사미스 어워드(SESAMES Award)를 수상한 새터너스(SATURNUS) 보안 클라우드

애플리케이션을 통해 PUF 기술을 탑재한 SmartMX2 테스트 칩의 성능을 선보일 예정이다.

- SmartMX 기술 소개
- PUF 백서 (NXP)

인트린직 ID 회사 소개

인트린직 ID 는 보안 IP 코어와 애플리케이션의 세계적인 선도 업체로 '물리적 복제 방지 기능'이라고도 불리는 HIS(Hardware Intrinsic Security)™ 기술의 특허를 보유하고 있다. HIS 비밀 키는 칩의 고유한 성질에서 추출되는 일종의 '전자 지문'으로 모바일 기기, 임베디드 시스템 및 클라우드에 존재하는 민감한 개인 및 기업 데이터를 완벽히 보호하는 데 사용된다. 인트린직 ID 는 네덜란드 아인트호벤에 본사를 두고 있으며 미국 캘리포니아주 산호세와 일본 동경 및 한국 서울에 영업지사가 있다. www.intrinsic-id.com