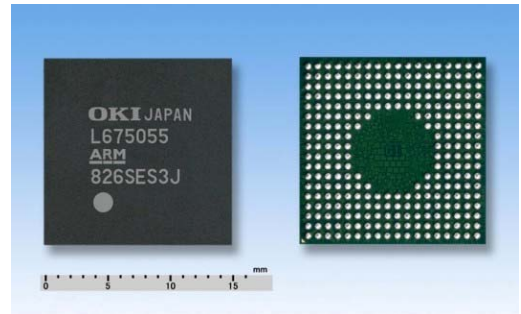


2009년 1월 20일

## 결제 단말기에 최적의 높은 보안성의 LSI, ML675055 를 개발 PCI-PED2.0의 실장을 지원하는 보안 기술을 탑재

오키세미컨덕터는 이번에 결제 단말기로부터 요구되는 보안 강도 평가 기준 PCI-PED 2.0<sup>(\*)1</sup>에 대응 가능한 높은 보안 기능을 실현한 독자 개발의 보안 IP 군과 최적의 주변 제어 기능을 원-칩에 집적시킨 'ML675055'를 개발하여 오늘부터 판매를 개시합니다.

오키세미컨덕터가 독자적으로 개발한 보안 IP 군은, 각종 공격<sup>(\*)2</sup>에 내성을 가져 암호화 및 암호 해독에 안전한 실행이 가능한 암호 엔진, 공격을 감시하는 각종 센서들과 악성 프로그램으로부터 암호 키 등의 중요한 데이터를 보호하는 메모리 보호 기능으로 구성됩니다. ML675055는 ARM7 기반의 32비트 고성능 CPU 코어에 8Kbyte의 캐시 메모리를 탑재, 80MHz의 동작이 가능한 시스템 LSI에 독자 개발한 보안 IP 군을 조합시키고 결제 단말에 필요한 각종 주변 기능들도 원-칩에 집적하고 있습니다. 본 LSI는 세계적으로도 권위 있는 PCI-PED 보안 평가 연구소인 독일의 'T-Systems'에 의해 보안 평가(Assessment)가 완료된 상태로써 PCI-PED 2.0의 기기 인증이 필요한 PED<sup>(\*)3</sup>, 신용카드 인증 단말(CAT) 등에 최적의 상품입니다.



### 【개발의 배경】

세계적으로 개인 정보 보호에 대한 관심이 높아지고 신용 카드 범죄의 고도화 및 복잡화에 따라, 기존의 IC 카드에 의한 트랜지션 보호뿐만 아니라, PED 등의 단말 장치 전체에 대한 높은 보안성이 요구되고 있습니다. 당사는 새로운 보안 규격에 대응하는 단말기 설계 시, 고객의 부담을 최대한 경감시키기 위해 보안에 관련되는 기능을 최대한으로 LSI 내부에 포함시키는 것을 목표로 보안 기술 개발에 임해왔습니다. 이에 따라 고도의 변형 억제성(Temper-resistant)<sup>(\*)4</sup>을 실현하는 보안 IP 군의 개발과 이 IP 군을 탑재한 LSI, ML675055의 판매에 이르렀습니다. 오키세미컨덕터는 앞으로도 이 IP 군을 탑재한 LSI 상품을 제안해나갈 것입니다.

### 【이 LSI 상품의 특징】

- 변형 억제성을 실현하는 신개발 보안 IP 군을 내장

전력 해석<sup>(\*5)</sup>의 내성을 가진 RSA<sup>(\*6)</sup>, DES/T-DES<sup>(\*7)</sup>, AES<sup>(\*8)</sup>, SHA1/SHA256<sup>(\*9)</sup>의 각 암호 엔진을 탑재하여 고속으로 안전하게 처리할 수 있습니다. 특히 RSA는 최대 2112 비트의 키를 이용한 암호, 암호 해독 연산이 가능합니다. 전압, 온도, 주파수 등 각종 센서들도 탑재하고 있어, 이들을 지속적으로 감시하여 변형 억제성을 실현하고 있습니다. 뿐만 아니라, 독자 개발에 의한 메모리 보호 기능을 제어하여 올바르지 못한 접속에 의한 공격을 검출합니다.

- 32 비트 CPU 코어, ARM7TDMI 를 기반으로 하여, 80MHz 의 고속 동작 CPU 코어로서 업계 표준인 ARM7TDMI 를 채용하고 있으며, 8Kbyte 의 캐시 메모리를 탑재하여 80MHz 의 고속 동작이 가능합니다.
- 안전한 외부 메모리 인터페이스에 의한 확장성  
독자적인 암호 기구를 탑재한 외부 메모리 인터페이스를 제공합니다. 고객의 어플리케이션 프로그램, 데이터의 대용량화에 대응이 가능합니다.
- PCI-PED2.0 에 대한 제 3 자 평가(Assessment)의 실시  
실장하고 있는 각종 보안 기능은, PCI-PED 인증 연구소로서 세계적인 권위의 독일 'T-System'에서 안전성을 평가하고 있습니다. 고객이 채용할 때의 평가 작업을 경감시키는 동시에 공정한 평가 데이터에 의한 안도감을 제공합니다.
- 평가 보고서에 기초한 단말 설계 지침의 제공  
평가에 의해 얻어진 평가 결과에 기초하여, 고객의 보안 실장의 지침이 되는 정보를 어플리케이션 노트로서 제공합니다.
- 원-칩으로 단말 기능을 실현할 수 있는 풍부한 주변장치  
Full-Speed(12Mbps)로 동작하는 USB 2.0 표준의 호스트/디바이스를 탑재하여 개별 인터페이스에 의한 동시 사용이 가능합니다. 또한 4 장의 IC 카드나 SIM 카드에 대응되는 컨트롤러, 대용량 저장을 실현하는 NAND 플래시 컨트롤러, 인증 정보를 표시하기 위한 LCD 컨트롤러, UART 나 I2C, SPI 등의 직렬 컨트롤러를 집적하여 풍부한 주변 기능을 원-칩으로 실현합니다.

#### 【판매 계획】

- 상품명 : ML675055
- 샘플 : 출하 접수 가능
- 양산 출하 시기 : 2009 년 1 월
- 소프트웨어 개발 툴(SDK) : 출하 접수 가능

#### 【ML675055 의 주요 사양】

- 보안 IP 군 : 각종 암호 엔진 탑재  
RSA(CRT<sup>(\*10)</sup>)를 이용하지 않는 최대 2112 비트의 암호, 암호 해독 키), DES/T-DES, AES, SHA1/256  
암호 키에 대한 전력 분석(DPA/SPA) 내성  
센서 내장에 의한 공격 감시  
독자 개발의 메모리 보호 기구 탑재
- IC 카드 컨트롤러 : ISO7816 표준, 4ch 탑재  
EMV(4.0) 프로토콜 대응

- 직렬 인터페이스 : USB2.0 표준 호스트 인터페이스(Full-Speed)  
USB2.0 표준 디바이스 인터페이스(Full-Speed)  
UART 4ch, I2C 2ch, SPI 2ch 탑재
- 대용량 저장 대응 : NAND 플래시 컨트롤러 내장
- 표시 제어 : QVGA 흑백 액정 컨트롤러 내장(VRAM 내장)
- CPU 코어, 주파수 : ARM7TDMI(+ 8Kbyte Cache), 80MHz
- 내장 RAM : 최대 32Kbyte 탑재
- 외부 메모리 인터페이스 : FLASH, ROM, SDRAM, 각종 I/O 제어 가능  
(메모리 디바이스는 암호에 의해 보호됩니다)
- 범용 I/O 단자 : 최대 148 비트 사용 가능
- 기타 주변 기능 : 각종 타이머, A/D 컨버터 탑재
- 패키지 : 272 핀 LFBGA (15mm□)

**【ML675055 소프트웨어 개발 키트(SDK)】**

ML675055 소프트웨어 개발 키트(SDK)는, ML675055 을 이용한 IC 카드 단말, 결제 단말 등의 어플리케이션의 안전한 시스템 개발을 지원하기 위한 소프트웨어 개발 키트입니다. 이 상품은 ML675055 을 탑재한 CPU 보드, CPU 보드와 조합시켜 사용하는 베이스 보드, ML675055 의 각종 기능을 확인할 수 있는 샘플 소프트웨어, 개발을 위한 각종 유틸리티 툴로 구성되어 있습니다. 자세한 사항은 직접 문의해 주십시오.



**ML675055 CPU Board**

**【용어 해설】**

- (\*1) PCI-PED2.0 : 신용 카드 결제에 필요한 PIN(비밀 번호)를 입력하는 기구에 대한 물리적이고 이론적인 보안 요건을 규정한 국제 규격  
현재는 버전 2 가 최신 규격이다.
- (\*2) 각종 공격 : 물리 공격(DFA, 악성 프로그램의 실행, 이상 환경에서의 오동작 발생 등), 사이드 채널 공격(전력 해석 등)을 의미한다.  
DFA(Differential Fault Analysis)란, 암호 처리 실행 중에 LSI 에 이상 상태(전압, 온도 등)을 인가하거나 클럭 단자에 임펄스를 인가(글리치)하는 등에 의해, 고장 동작(계산 오류)을 발생시켜 정상 동작과 고장 동작인 때의 출력 차이로부터 암호 키를 추정하는 공격을 의미한다.
- (\*3) PED : PIN Entry Device 의 약자. 비밀 번호 입력 장치
- (\*4) 변형 억제성 : 물리적 또는 이론적으로 LSI 내부의 정보가 읽혀지는 것에 대한 내성
- (\*5) 전력 해석 : LSI 가 그 처리를 실행하고 있을 때의 칩의 소비 전력이 처리 정보의 이론치와 상관 관계가 있다는 점에 착안하여, 소비 전력을 관찰하는 것으로 암호 키를 추정하는 방법. 암호 처리가 실행 중인 소비 전류 파형의 변화를 직접 해석하여 암호 키를 추정하는 방법(SPA : Simple Power Analysis)과 다수의 소비 전류 파형들에 대해 통계적 처리를

실행하여 암호 키를 추정하는 방법(DPA : Differential Power Analysis)이 알려져 있다.

- (\*6) RSA : 비대칭 암호 알고리즘 중 한가지. 공개 키 암호로 사용되는 알고리즘. RSA 는 사양을 결정한 3명(Rivest, Shamir, Adleman)의 이니셜이다.
- (\*7) DES/T-DES : 대칭 암호 알고리즘 중 한가지. DES : Data Encryption Standard, T-DES : Triple DES
- (\*8) AES : 대칭 암호 알고리즘 중 한가지. AES : Advanced Encryption Standard.
- (\*9) SHA1/SHA256 : 대칭 암호 알고리즘 중 한가지. SHA : Secure Hash Algorithm 는 한 군에 관련된 해쉬 함수. 생성하는 해쉬 값의 비트 수에 따라 다양한 종류가 알려져 있다. SHA1 은 160 비트, SHA256 은 256 비트의 해쉬 값을 각각 생성한다.
- (\*10) CRT : Chinese Remainder Theorem(중국 잉여 정리(수리 해법))  
중국의 산술서 '손자 산경'에 유래하는 정수의 잉여에 관한 정리.  
이 정리를 이용하여 RSA 암호 연산의 암호 키를 확장시키는 것이 가능하나, 그 확장 과정에서 암호 키에 대한 공격을 받기 쉬운 방법으로 알려져 있다.

※ 기타, 본문에 기재되어 있는 회사명, 제품명은 일반적으로 각사의 상표 또는 등록 상표입니다.