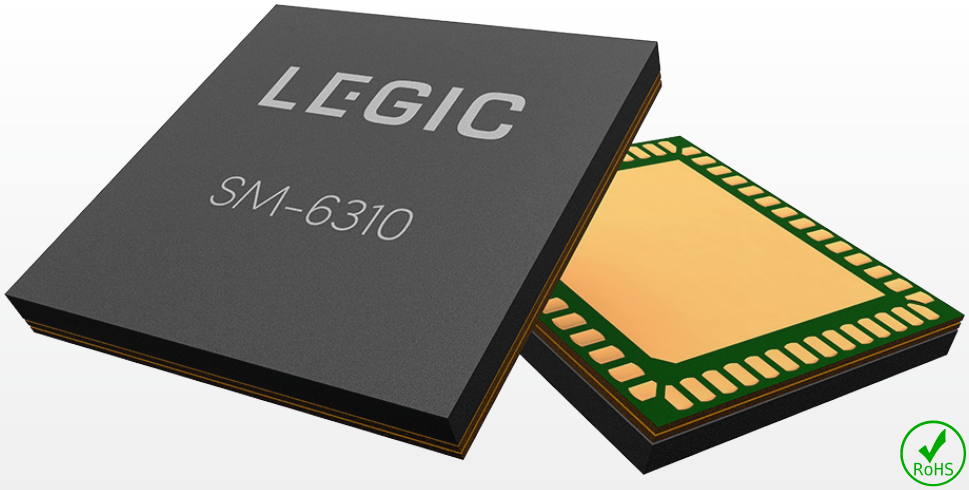
LEGIC

SM-6310 programmierbares Sicherheitsmodul

IoT Edge Prozessor mit RFID, Bluetooth® und Secure Element



Tatsächliche Grösse: 8 x 8 mm

- **ARM® Cortex® Core mit 128 KB programmierbarem Flash Speicher in CC EAL5+ Secure Element**
- **Unterstützt RFID, NFC und Bluetooth 5 für Anwendungen mit Smartphones, Smartcards, Fobs, Tags und Labeln**
- **Kompatibel mit LEGIC advant und neon, MIFARE*, HID iCLASS*, MTSC und Orbit**
- **Hohe Sicherheit dank AES-128/256 Verschlüsselung und Hardware Root of Trust**

Intelligente Sicherheit und kontaktlose Interaktion für vernetzte Infrastruktur und IoT-Geräte

Mit frei programmierbarem Anwendungscode und kryptografischen Schlüsseln in einem zertifizierten Secure Element ist das SM-6310 ideal für kompakte, kontaktlose Anwendungen mit geringem Stromverbrauch, welche sichere Konnektivität und Benutzerauthentifizierung via Smartcards oder Smartphone-Apps erfordern.

Vielseitiges Sicherheitsmodul

Das SM-6310 unterstützt alle relevanten Smartcard Technologien, Bluetooth und NFC. Mit frei programmierbarem Anwendungscode in einem CC EAL5+ zertifizierten Secure Element (SE) erlaubt das Modul die unkomplizierte Umsetzung von sicherheitskritischen Anwendungen.

Das SM-6310 eignet sich perfekt für kompakte Anwendungen mit geringem Stromverbrauch in den Bereichen Zugangskontrolle, Hospitality, Carsharing, öffentliche Verkehrsmittel, E-Payment, Smart City, IoT und mehr.

Sichere Umgebung für Anwendungen und Schlüssel

Das manipulationssichere SE ist ideal zum Speichern von sicherheitskritischem Code und kundenspezifischen Schlüsseln. Zur Verwendung mit LEGIC Orbit ist ein Transportschlüssel vorprogrammiert. Die verschlüsselte Kommunikation zwischen Gerät und Management System wird unterstützt.

Das 8 x 8 mm System-in-Package integriert zwei ARM-Prozessoren, Bluetooth, NFC, passive Komponenten und ein Secure Element.

Die LEGIC Sicherheitsplattform

Das SM-6310 ist ein wesentlicher Bestandteil der LEGIC Sicherheitsplattform, welche Smartcard-ICs, Verwaltungstools für Schlüssel und Berechtigungen sowie den Software-Service LEGIC Connect umfasst.

Dank dem vielseitigen und nahtlosen Zusammenspiel dieser Komponenten kann eine breite Palette von Anwendungen basierend auf Smartphones, Smartcards und anderen Geräten schnell und einfach realisiert werden.

Vorteile und Eigenschaften

- 128 KB Flash Speicher in Common Criteria EAL5+ zertifiziertem Secure Element (SE) für individuellen Anwendungscode
- Sichere Ablage für kundenspezifische kryptografische Schlüssel innerhalb des SE
- Firmware-Update Over-the-Air (FOTA) via Orbit VCP
- Unterstützt alle weltweit relevanten Smartcard-Standards
- Unterstützt die Verwendung in Kombination mit HID iCLASS SE® Processor oder NXP MIFARE® Secure Access Modules
- Unterstützt die Implementierung von ECP 2.0 durch Apple-Lizenznehmer
- Kryptografisch kontrollierte Übergabe der Hoheit über Gerätekonfiguration
- Unterstützt sichere Anbindung von Public oder Private Clouds mittels TLS
- Geringer Stromverbrauch; für den Batteriebetrieb geeignet
- Kommunikation via Bluetooth oder NFC-HCE mit dem LEGIC Mobile SDK (Android und iOS) für den Zugriff auf LEGIC neon Files oder für das Übermitteln von Informationen via LEGIC Trusted Service an das kundenseitige Management-System
- Parallele Suche nach Bluetooth- und RFID-Medien
- Schnelle Bluetooth Kommunikation durch erhöhte Paketgrösse (Bluetooth 4.2+)
- Betrieb mit asymmetrischen & symmetrischen NFC Antennen
- Kompatibel mit Master-Token System-Control (MTSC) und LEGIC Orbit
- Unterstützt ePayment-System LEGIC Cash
- Kompaktes System-in-Package mit den Abmessungen 8 x 8 x 1.1 mm, PQFN56

Evaluation und Entwicklung

Das Custom Code Development Kit DK-6310 unterstützt Sie bei der effizienten Programmierung und der Entwicklung von sicheren IoT- und Kontaktlos-Anwendungen.

Technische Daten

SM-6310 oder SM-6310*init* mit Firmware OS50			
Varianten	▪ SM-6310 mit Standardfunktionalität ▪ SM-6310*init* mit erweiterter Funktionalität: Initialisieren von LEGIC advant/prime Segmenten		
Microcontroller	▪ ARM 32-bit RISC Prozessor mit 50 MHz ▪ 128 KB Custom Code Flash Speicher in SE ▪ 5 KB RAM ▪ Hardwarebeschleunigte Funktionen Custom Code: · Verschlüsselung: AES-128/256 (ECB oder CBC Modus), Elliptische-Kurven-Kryptografie (NIST P-256 und P-384) · Persistenter Speicher für 6 ECC-Schlüsselpaare · Unterstützt Ephemeral Difie-Hellman (ECDHE) zur Aushandlung von Schlüsseln · Hashing: SHA1-160, SHA2-256/384 · Authentifizierung: CMAC		
Drahtgebundene Schnittstellen			
Host Schnittstelle	▪ UART mit 38'400, 115'200 Bd oder 1 MBd ▪ SPI slave, Modus 1 oder 3 ▪ I²C 400 kbit/s or 100 kbit/s		
8 GPIOs	▪ Nutzbar als Ein-/Ausgänge, I²C, SPI, 12-bit ADC		
Drahtlose Schnittstellen			
Bluetooth	▪ V5.0+ Bluetooth Low Energy ▪ Kommunikation mit LEGIC Mobile SDK ▪ Kommunikation mit Drittgeräten: · Central / Peripheral & Client / Server Rolle · Long Term Key (LTK) · Bluetooth Beaconing		
RFID / NFC	▪ ISO 14443 A + B, ISO 15693 ▪ LEGIC RF standard ▪ Inside Secure*, Sony Felica**, ST SR series		
Sicherheitsmerkmale			
Host Schnittstelle	▪ Authentifizierung und Verschlüsselung (optional)		
Secure Element	▪ Zertifiziert nach Common Criteria EAL5+ ▪ Sicherer Transportschlüssel für LEGIC Orbit		
RFID	▪ Master-Token System-Control ▪ NXP Schlüsselableitung ▪ AES-128/256 Bit, 3DES		
Mobile ID	▪ Applikationsspezifische Datenverschlüsselung (AES-128) mit Ende-zu-Ende-Sicherheit vom LEGIC Trusted Service zum SM-6310		
Kommunikation mit kundenseitigem Management System	▪ Datenverschlüsselung ▪ Projektspezifische AES-256 Schlüssel		
Betriebsbedingungen			
Betriebsspannung (Einzel-/Doppelspeisung)	Min	Typ	Max
RF-Teil	2.4 V	3.3 / 5.0 V	3.6 / 5.5 V
Digital-Teil	1.8 V	3.3 V	3.6 V
Stromverbrauch im Ruhemodus je nach Weckfunktion ***	▪ 0.8 µA beim Wecken via Input-Port ▪ 21.0 µA via Induktivitätsänderung (OIF) ▪ 4.5 µA via Kapazitätsänderung		
Betriebstemperatur	-40°C bis +85°C		

* Lese- / Schreibzugriff auf Smartcards mit NXP MIFARE® und verschlüsselter Inside Secure Technologie wie HID iCLASS®. NXP MIFARE® und HID iCLASS® sind Produkte und Warenmarken von Drittparteien, welche nicht im Besitz von LEGIC Identsystems AG sind und weder hergestellt noch vertrieben werden durch LEGIC.
** Verschlüsselung ist nicht integriert
*** Typischer Stromverbrauch bei Einzelspeisung

LEGIC Identsystems AG
Schweiz Telefon +41 44 933 64 64 info@legic.com www.legic.com