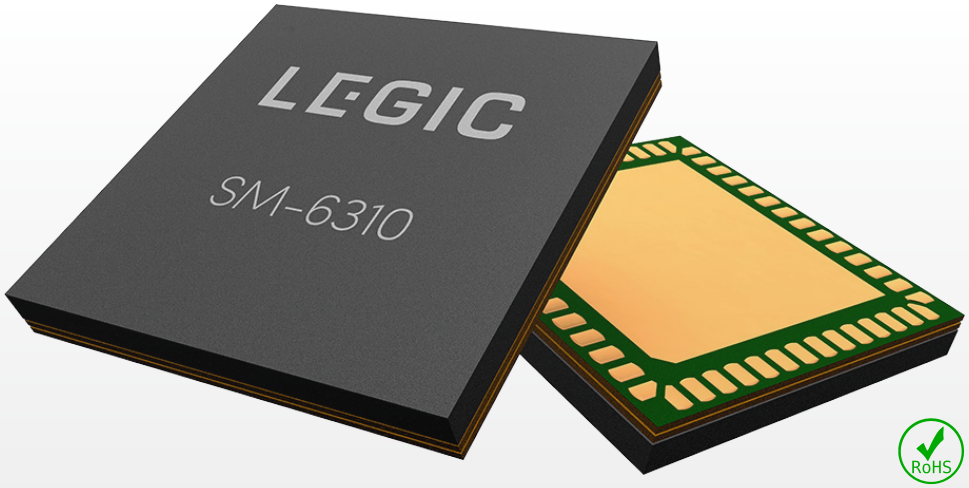
LEGIC

SM-6310 Programmable Security Module

IoT Edge Processor with RFID, Bluetooth® and Secure Element



Actual size: 8 x 8 mm

- **ARM® Cortex® Core with 128 KB programmable flash memory stored in CC EAL5+ Secure Element**
- **Supports RFID, NFC and Bluetooth 5 for smartphone, smartcard, fob, tag and label based applications**
- **Compatible with LEGIC advant, neon, NXP MIFARE*, HID iCLASS*, LEGIC MTSC and Connect**
- **High security based on AES-128/256 encryption, hardware Root of Trust**

Intelligent security and contactless interaction for connected infrastructure and IoT devices

With freely programmable application code and cryptographic keys in a certified Secure Element, the SM-6310 is ideal for compact, low-power, contactless applications requiring secure connectivity, user authentication and credential management. It supports smartcards and iOS / Android smartphone apps based on LEGIC Connect.

Multi-purpose security module

The SM-6310 supports all relevant smartcard technologies, Bluetooth Low Energy and NFC. With freely programmable application code running in a CC EAL5+ certified Secure Element (SE), the module enables easy design of security-critical applications.

The SM-6310 is perfect for low-power, compact applications in access control, hospitality, car-sharing, public transportation, e-payment, Smart City, IoT and more.

Secure application and key store

The tamper-proof hardware SE is ideal for storing security-critical code and customer-specific application keys. For use with LEGIC Orbit, a secure transport key is pre-programmed. Encrypted end-to-end communication with customer- and application-specific management systems is supported.

The 8 x 8 mm System-in-Package integrates two ARM processors, Bluetooth, NFC, passive components and SE chip.

The LEGIC security platform

The SM-6310 is an integral part of the LEGIC Security Platform which also includes smartcard ICs, key and authorization management tools and the software service LEGIC Connect consisting of the Trusted Service and Mobile SDK.

Thanks to the versatile and seamless interoperation of these components, a wide range of applications based on smartphones, smartcards and other devices can be realized quickly and easily.

Benefits and features

- 128 KB of flash memory in Common Criteria EAL5+ certified Secure Element (SE) for storing application code
- Secure storage of customer-specific encryption keys in SE
- Firmware update Over-the-Air (FOTA) via Orbit VCP
- Supports all globally relevant smartcard technologies
- Supports applications with HID iCLASS SE® Processor or NXP MIFARE® Secure Access Modules
- Supports Apple licensees implementing ECP 2.0
- Cryptographically controlled transfer of power over device configuration
- Support of secure TLS connection to public or private clouds
- Low power during sleep, idle and RF activity, optimal for battery operation
- Bluetooth or NFC-HCE communication to LEGIC Mobile SDK (Android & iOS) to access LEGIC neon files, or send messages via LEGIC Trusted Service to customer's management system
- Parallel Bluetooth and RFID search accelerates interactions
- Fast Bluetooth speed via increased data packet size (Bluetooth 4.2+)
- Supports symmetrical and asymmetrical NFC antennas
- Supported by LEGIC's Master-Token System-Control (MTSC) and LEGIC's key and authorization management solution LEGIC Orbit
- Supports closed-loop e-payment feature LEGIC Cash
- Compact System-in-Package PQFN56, 8 x 8 x 1.1 mm

Evaluation and Design

The Custom Code Development Kit DK-6310 supports you in the efficient programming and design of secure IoT and contactless applications based on the SM-6310 Security Module.

Technical data

SM-6310 or SM-6310*init* with firmware OS50			
Variants	▪ SM-6310 with standard functionality ▪ SM-6310*init* with extended functionality: Initialization of LEGIC advant and prime segments		
Microcontroller	▪ ARM 32-bit RISC processor with 50 MHz clock ▪ 128 KB Custom Code flash memory in SE ▪ 5 KB RAM ▪ Hardware accelerated functions for Custom Code: · Crypto algorithms: AES-128/256 (ECB or CBC modes), Elliptic-curve (NIST P-256 and P-384) · Persistent storage for 6 ECC key pairs · Supports Ephemeral Diffie-Hellmann (ECDHE) key exchange · Hashing: SHA1-160, SHA2-256/384 · Message authentication via CMAC		
Wired interfaces			
Host interface	▪ UART with 38,400 or 115,200 baud or 1 Mbaud ▪ SPI slave mode 1 or mode 3 ▪ I²C 400 kbit/s or 100 kbit/s		
8 GPIOs	▪ Definable as inputs, outputs, I²C, SPI, 12-bit ADC		
Wireless interfaces			
Bluetooth	▪ V5.0+ Bluetooth Low Energy ▪ Communication to apps with LEGIC Mobile SDK ▪ Communication to third-party Bluetooth devices: · Central / peripheral & client / server role · Long Term Key (LTK) · Bluetooth beaconing		
RFID / NFC	▪ ISO 14443 A + B ▪ ISO 15693 ▪ LEGIC RF standard ▪ Inside Secure*, Sony Felica**, ST SR series ▪ Supports Apple licensees implementing ECP 2.0 for reading NFC credentials in Apple Wallet		
Security features			
Host interface	▪ Authentication and encryption (optional)		
Secure element	▪ Common Criteria EAL5+ certified ▪ Secure transport key for LEGIC Orbit		
RFID	▪ Master-Token System-Control ▪ NXP key diversification ▪ AES-128/256 Bit, 3DES		
Mobile ID	▪ Data encryption with end-to-end security from LEGIC Trusted Service to SM-6310 ▪ Application-specific AES-128 Bit keys		
Messaging to customer's management system	▪ Data encryption ▪ Project-specific AES-256 Bit key		
Operating conditions			
Operating voltage (single / double supply)	Min	Typ	Max
RF part	2.4 V	3.3 / 5.0 V	3.6 / 5.5 V
Digital part	1.8 V	3.3 V	3.6 V
Sleep mode current consumption depending on wake-up function ***	▪ 0.8 µA if wake-up by change on input port ▪ 21.0 µA by inductive sensing (OIF), e.g. RFID card ▪ 4.5 µA by capacitive sensing		
Operating temperature	-40°C to +85°C		

* Read / write access to smartcards based on NXP MIFARE® and cyphered Inside Secure technology such as HID iCLASS®. NXP MIFARE® and HID iCLASS® are products and trademarks by a third party and not owned, manufactured or sold by LEGIC Identsystems AG.
** Encoding is not integrated
*** Typical current consumption in "single supply" configuration

LEGIC Identsystems Ltd
Switzerland Phone +41 44 933 64 64 info@legic.com www.legic.com