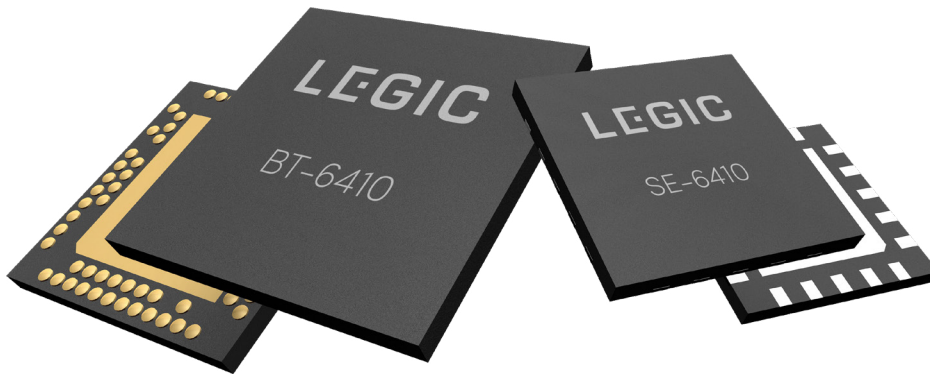


SC-6410 Programmable Security Chipset

Secure Chipset with Bluetooth® and Secure Element



- ✓ ARM® Cortex® Core with 128 KB programmable flash memory stored in CC EAL5+ Secure Element
- ✓ For applications with smartphones and tablets requiring secure Bluetooth® Low Energy connectivity
- ✓ Compatible with LEGIC Connect, LEGIC neon credentials and LEGIC Orbit key and configuration management
- ✓ High security based on AES-128/256 encryption, hardware Root of Trust



Actual size: Secure Element 4 x 4 mm / Bluetooth chip 7 x 7 mm

User authentication, remote interaction, secure configuration and data retrieval for infrastructure and IoT devices

With freely programmable application code and cryptographic keys stored in a certified Secure Element, the SC-6410 is ideal for compact, low-power, wireless applications requiring secure connectivity, user identification and credential data processing. It supports iOS / Android smartphone apps based on LEGIC Connect.

Multi-purpose security chipset

The SC-6410 supports Bluetooth Low Energy and has freely programmable application code running in a CC EAL5+ certified Secure Element (SE). The chipset enables easy design of security critical applications.

The SC-6410 is perfect for physical and logical access via Bluetooth mobile credentials, secure device commissioning, preventive maintenance, device tracking and data retrieval requiring secure communication with mobile devices and back-end systems.

Secure application and key store

The tamper-proof hardware SE includes a crypto engine and is ideal for storing security-critical code and customer-specific application keys. For use with LEGIC Orbit, a secure AES-256 transport key is pre-programmed. For PKI applications, there is a Device Manufacturer Certificate as root of trust.

The Custom Code feature enables the use of state-of-the-art crypto algorithms for writing own application-specific program code to run in the SE.

The LEGIC Security Platform

The SC-6410 is an integral part of the LEGIC Security Platform which includes high availability trusted services, security chips, smartcard and mobile credentials, as well as key and authorization management solutions.

Together with the SC-6410, the platform supports demanding IoT and access control applications requiring secure configuration, monitoring and control of critical devices, as well as user identification and credential data processing.

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) online or offline via Orbit VCP
- Device Manufacturer Certificate is pre-programmed in SE to verify component authenticity
- Enabling secure connections to public or private clouds with TLS
- Low power; optimal for battery operation
- Bluetooth communication to LEGIC Mobile SDK (Android & iOS) to access LEGIC neon files, or send messages via LEGIC Trusted Service to customer's management system
- Fast Bluetooth speed via increased data packet size (Bluetooth 5.1)
- Compatible with LEGIC Orbit key and configuration management solution to enable device configuration with end-to-end encryption and never-visible cryptographic application keys
- External 32.768 kHz crystal enables power saving operation and Real Time Counter for date and time
- Compact two-chip solution with 7 x 7 mm and 4 x 4 mm size

Technical data

SC-6410 with firmware OS60			
Wired interfaces			
Host interface		<ul style="list-style-type: none"> ▪ USB 2.0 12 Mbit/s ▪ UART with 38,400 or 115,200 baud or 1 Mbd ▪ SPI slave mode 1 or mode 3 ▪ I²C 400 kbit/s or 100 kbit/s 	
20 GPIOs		<ul style="list-style-type: none"> ▪ Definable as inputs, outputs, I²C, SPI, 12-bit ADC 	
Wireless interfaces			
Bluetooth		<ul style="list-style-type: none"> ▪ V5.1 Bluetooth Low Energy ▪ Bluetooth wake-up ▪ Communication to apps with LEGIC Mobile SDK ▪ Communication to third-party Bluetooth devices: <ul style="list-style-type: none"> • Central or peripheral role • Client or server role • Long Term Key (LTK) • Filter for device selection • Bluetooth beaconing 	
Security features			
Host interface		<ul style="list-style-type: none"> ▪ Authentication and encryption (optional) 	
Secure Element		<ul style="list-style-type: none"> ▪ Common Criteria EAL5+ certified ▪ Secure AES-256 transport key for LEGIC Orbit ▪ Device Manufacturer Certificate (DMC) as a base for PKI applications 	
Mobile credentialing		<ul style="list-style-type: none"> ▪ Data encryption based on AES-128 ensures end-to-end security from LEGIC Trusted Service to SC-6410 ▪ Application-specific AES-128 Bit keys 	
Messaging to customer's management system		<ul style="list-style-type: none"> ▪ Data encryption ▪ Project-specific AES-256 Bit key 	
Custom Code in SE-6410			
Available microcontroller resources		<ul style="list-style-type: none"> ▪ Secure ARM 32-bit RISC processor with 50 MHz clock ▪ 128 KB Custom Code flash memory in SE ▪ 250 KB Custom Code Data Flash in Download area of SE ▪ 5 KB secure RAM 	
Available functions for Custom Code (beyond OS60 command set)		<ul style="list-style-type: none"> ▪ Hardware-accelerated functions for Custom Code: <ul style="list-style-type: none"> • Crypto algorithms: AES-128/256 (ECB or CBC modes), Elliptic-curve (NIST P-256 and P-384), Brainpool 256/384 bits according to RFC-5639 • Persistent storage for 6 ECC key pairs • Supports Ephemeral Diffie-Hellmann (ECDHE) key exchange • Hashing: SHA1-160, SHA2-256/384 • Message authentication via CMAC 	
Operating conditions			
Operating voltage	Min	Typ	Max
	1.75 V	3.0 V	3.6 V
Sleep mode current consumption depending on wake-up function	<ul style="list-style-type: none"> ▪ 15.6 µA (13.0 µA with external 32.768 kHz crystal) by Bluetooth using 1 s advertizing interval ▪ 3.7 µA by internal timer ▪ 0.8 µA by input change on GPIO 		
Operating temperature	-40°C to +105°C		

