General Description

The SIB8112 a Single chip of Bio-Crypto device offers a highly secure access control system. It integrates a 32-bit microprocessor with two 8k byte cache, one 512k byte flash memory, large system SRAM and powerful I/O to provide a high performance biometric security system which is built in a proven finger print extraction algorithm (winner of International Fingerprint Verification Competition 2000) and Public Key Infrastructure (PKI) function.

Features

- Powerful I/O interface : UARTs, I2C (Master/ Slave), SPI, Wireless interface and 26 General Purpose I/O control
- Enrolment/ De-enrolment and Authentication can be performed through UART or wireless interface
- Once owner is enrolled, other users of the same device can only be enrolled with owner's approval
- Ownership is transferable if granted by current owner
- Provide 512K byte of built in flash memory for fingerprint template storage and application programming
- No reading of the confidential area in flash memory is allowed
- RSA key pair are generated internally, only public key is allowed to be read externally, private key is always resided in the silicon
- Built-in AES algorithm for data encryption
- Provide maximum security as the biometric matching is performed in the silicon
- Provide a set of protocol through UART for external MCU to control the crypto function, biometric verification and I/O logic function
- Support most of the fingerprint sensor in the market, like Fujitsu and Atura sensor, etc. Allow plug in for new sensor type
- Power management for maximizing battery life of mobile devices

Applications

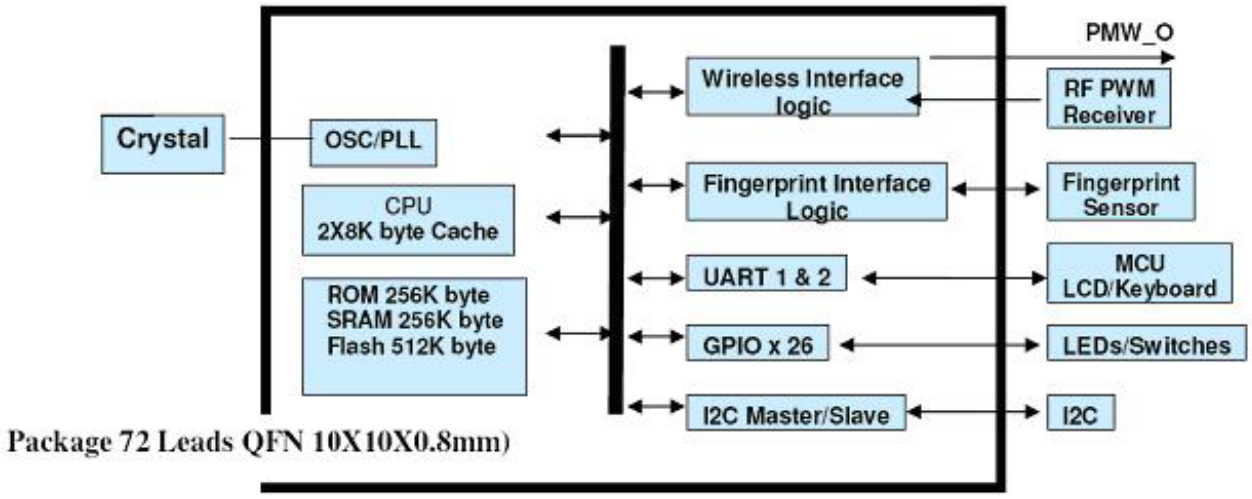
- General locking device
- Car security
- Desktop computer access
- Private/secret key deployment
- Access control and monitoring
- Phone, keyboard, door, safe access
- Toy, electronic pets
- Replace keypad password

Functions

The three basic functions:

- **Basic Stand Alone**: Capable to enroll (Read an finger print image from sensor), De-Enroll (Search and remove the related finger print data) and authenticate (Read the finger print image and match with the stored template)
- **Internal MCU emulation**: Allow to utilize the internal MCU emulation to interface with the external devices
- **External MCU**: capable to interface with external MCU to communicate the finger print authentication result

Block Diagram



Finger Print Verification Specification

Finger print template size	360 byte / fingerprint template
Maximum finger print templates	250
False Acceptance rate (FAR)	< 1 in 10000
False Rejection rate (FRR)	< 1 in 1000
Verification time (100 templates)	< 1 sec

DC Parameters

Parameter	Ratings	Unit
Operating Temperature Range (T_{opr})	-40 to +85	^{o}C
Storage Temperature Range	-55 to +125	^{o}C
Lead Temperature Range (soldering, 10 seconds)	+260	^{o}C
Maximum Supply Voltage, V_{IO}	+3.6	V
Maximum Input Voltage, V_{INT}	+2.75	V
Note: The absolute maximum ratings are rated values, which must not be exceeded during operations, even for an instant. Any one of the ratings must not be exceeded. If any absolute maximum rating is exceeded, a device may break down or its performance may be degraded, causing it to catch fire or explode resulting in injury to the user. Thus when designing products which include this device, ensure that no absolute maximum rating value will ever be exceeded.		

Sales Offices

Singapore

BlueChips Technology Pte Ltd

No. 18 Boon Lay Way
TradeHub 21 #09-94/95
Singapore 609966

Tel : +65 6501 0511
Fax: +65 6501 0515

Email: info@bluechipstech.com

Hong Kong

BlueChips Technology (HK) Ltd

Unit 1101-1103, 11/F, Yardley Comm. Bldg.,
3 Connaught Road West, Sheung Wan,
Hong Kong

Tel: 852 2776 7968
Fax: 852 2776 8997

Email: info@bluechipstech.com

Malaysia

BCT Technology Bhd (HQ)

Lot G4, Incubator 3
Technology Park Malaysia
Bukit Jalil, 57000 Kuala Lumpur
Malaysia

Tel: 603 - 8996 8088
Fax: 603 - 8996 8087

Email: info@bluechipstech.com