Secure 4 click

PID: MIKROE-2829

Weight: 24 g

Secure 4 click includes the ATECC608A, a secure CryptoAuthentication™ device from Microchip, which is equipped with an EEPROM array which can be used for storing of up to 16 keys, certificates, consumption logging, security configurations and other types of secure data. Access to the various sections of memory can be restricted in several different ways and then the configuration can be locked permanently, to prevent changes.

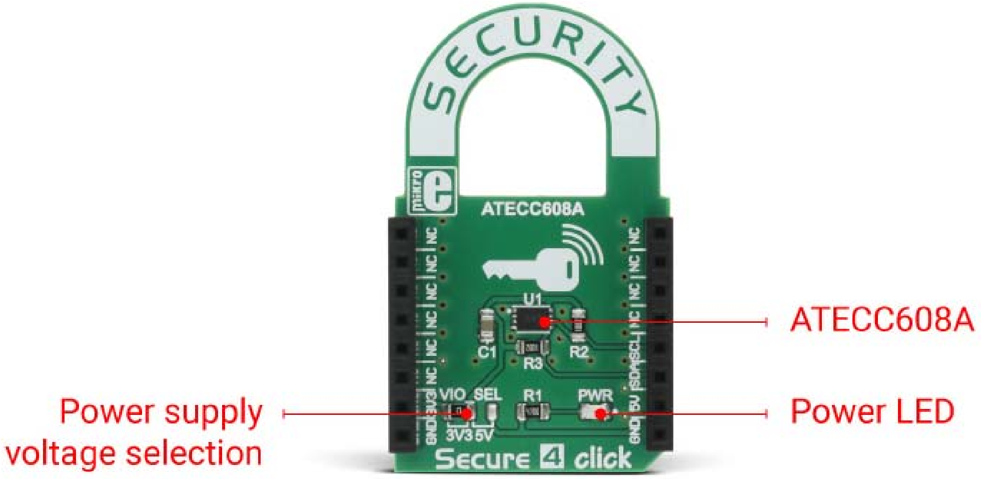
The ATECC608A equipped on this click board™, supports the I2C interface with a flexible command set, that allows use in various security applications, including Network/IoT Node Endpoint Security, Secure Boot, Small Message Encryption, Key Generation for Software Download, Ecosystem control, Anti Counterfeiting and similar.

NOTE: The click board™ comes with stacking headers which allow you to combine it with other click boards™ more easily by using just one mikroBUS™ socket.

How does the click work?

The ATECC608A implements a complete asymmetric key cryptographic signature solution, based on the Elliptic Curve Cryptography and the ECDSA signature protocol. It also implements AES-128, SHA256 and multiple SHA derivatives, such as HMSC(SHA), PRF (the key derivation function in TLS) and HKDF in hardware. It can also generate random private keys and random numbers, which can be used as a part of the crypto protocol.

Those asymmetric cryptographic operations are accelerated by the ATECC608A hardware and are calculated up from ten to thousand times faster than with the software running on standard microprocessors. This prevents the risk of key exposure, which is usually found in standard microprocessors.



The device is consuming very low current, especially while it is in the sleep mode. The chip itself uses less than 150nA, in that case. The voltage range which can be used to power up the Security 4 click, allows for it to work with both 3.3V and 5V capable MCUs.

The chip itself uses a minimal number of pins; only the I2C lines are routed to the mikroBUS™ along with the 3.3V and 5V rails. The device can work with any of these voltages. It can be selected by soldering a small SMD jumper to the correct position.

The I2C lines are pulled high by the two 4.7KΩ resistors, so no additional pull-up resistors are needed.

Specifications

Type	EEPROM
Applications	Used for storage of up to 16 keys, certificates, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations
On-board modules	Microchip ATECC608A IC which includes an EEPROM array
Key Features	Cryptographic Co-processor with secure hardware-based key storage for up to 16 keys, certificates or data. Hardware support for the asymmetric sign, verify, key agreement, unique 72-bit serial number, fast communication protocol (I2C/GPIO).
Interface	I2C
Input Voltage	3.3V or 5V
Click board size	M (42.9 x 25.4 mm)

Pinout diagram

This table shows how the pinout on **Secure 4 click** corresponds to the pinout on the mikroBUS™ socket (the latter shown in the two middle columns).

Notes	Pin	mikro™ BUS				Pin	Notes
	NC	1	AN	PWM	16	NC	
	NC	2	RST	INT	15	NC	
	NC	3	CS	RX	14	NC	
	NC	4	SCK	TX	13	NC	
	NC	5	MISO	SCL	12	**SCL**	I2C clock
	NC	6	MOSI	SDA	11	**SDA**	I2C data

Power supply	**+3.3V**	7	3.3V	5V	10	**+5V**	Power supply
Ground	**GND**	8	GND	GND	9	**GND**	Ground

Secure 4 click maximum ratings

Description	Min	Typ	Max	Unit
Serial clock frequency			1	MHz
Operating temperature	-40	350	+85	°C

Onboard settings and indicators

Label	Name	Default	Description
LD1	PWR LED	-	Power indication LED
JP1	VIO SEL.	LEFT	Power supply voltage selection, left position 3V3, right position 5V

Software support

We provide a library for the Secure 4 click on our LibStock page, as well as a demo application (example), developed using MikroElektronika compilers. The demo can run on all the main MikroElektronika development boards.

Library Description

This click uses CryptoAuthLib from Atmel, slightly modified to work with MikroElektronika compilers. CryptoAuthLib is designed to cover a wide variety of devices and functions, and it supports all the features of this click. Basic and commonly used functions are contained in atca_basic file, and are marked with atcab_ prefix.

Key functions

`ATCA_STATUS atcab_random(uint8_t *rand_out)` - Returns a random number

`ATCA_STATUS atcab_genkey( int slot, uint8_t *pubkey )` - Generates a key in a given slot

`ATCA_STATUS atcab_verify_extern (uint8_t *message, uint8_t *signature, uint8_t *pubkey, bool *verified)` - Verifies a signature using a public key

Examples Description

The example demonstrates various functions of the Secure 4 click. It first performs basic functions, that can be executed without permanently locking the device. Using the more advanced functions that are needed to lock the device irreversibly is also shown in the example, but commented out to prevent accidental locking of the device.
The code snippet shows the use of one of the functions that calculates SHA digest of a short message and compares it to the precalculated value.

```
memset (bufferOut, 0x00, 128);
    bufferIn [0] = 0x74;
    bufferIn [1] = 0xba;
    bufferIn [2] = 0x25;
    bufferIn [3] = 0x21;

    if (atcab_sha(4, bufferIn, bufferOut) == ATCA_SUCCESS)
    {
        LOG( "rnrn SHA Digest of 0x74BA2521:  " );
        outputHex (bufferOut, 32);
        LOG("rn Expected value of digest: ");
        LOG("B1 6A A5 6B E3 88 0D 18 CD 41 E6 83 84 CF 1E C8 C1 76 80 C4
5A");
        LOG(" 02 B1 57 5D C1 51 89 23 AE 8B 0E");

    }
    else  LOG( "rn Generating SHA digest of the message failed..." );

    delay_ms (1500);
```

The full application code, and ready to use projects can be found on our LibStock page.

Other MikroElektronika Libraries used in the example:

- MemManager
- Conversions
- C_String
- UART

Additional notes and information

Depending on the development board you are using, you may need USB UART click, USB UART 2 click or RS232 click to connect to your PC, for development systems with no UART to USB interface available on the board. The terminal available in all MikroElektronika compilers, or any other terminal application of your choice, can be used to read the message.