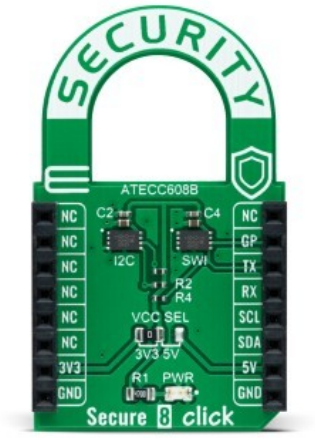
MIKROELEKTRONIKA D.O.O, Batajnički drum 23, 11000 Belgrade, Serbia
VAT: SR105917343 Registration No. 20490918
Phone: + 381 11 78 57 600 Fax: + 381 11 63 09 644 E-mail: office@mikroe.com
www.mikroe.com

Secure 8 Click



PID: MIKROE-5154

Secure 8 Click is a compact add-on board containing hardware-based key storage with a cryptographic accelerator to implement authentication and encryption protocol. This board features the ATECC608B, a member of the Microchip CryptoAuthentication™ family of high-security cryptographic devices with a wide array of defense mechanisms specifically designed to prevent logical attacks on the data transmitted between the device and the system. An integrated EEPROM can be used to store up to 16 keys, certificates, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. It also allows memory-section restrictions in several different ways. This version of the Secure Click board™ carries two versions of the ATECC608B, thus supporting the I2C and the Single Wire (SWI) interface, giving the user the ability to select the desired communication interface. This Click board™ is suitable for various security applications such as Network/IoT node endpoint security, secure boot, small message encryption, key generation for software download, and more.

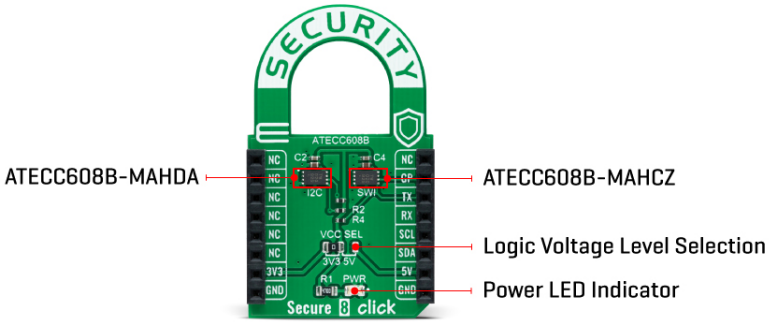
NOTE: This Click board™ comes with stacking headers which allow you to combine it with other Click boards™ more efficiently by using just one mikroBUS™ socket.

How does it work?

Secure 8 Click as its foundation uses the ATECC608B, a cryptographic coprocessor with secure hardware-based key storage from Microchip. The ATECC608B integrates the ECDH (Elliptic Curve Diffie Hellman) security protocol, an ultra-secure method to provide a key agreement for

MIKROELEKTRONIKA D.O.O, Batajnički drum 23, 11000 Belgrade, Serbia
VAT: SR105917343 Registration No. 20490918
Phone: + 381 11 78 57 600 Fax: + 381 11 63 09 644 E-mail: office@mikroe.com
www.mikroe.com

encryption/decryption along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication for the Internet of Things (IoT) market. It includes an EEPROM array that can store up to 16 keys, certificates, miscellaneous read/write, read-only or secret data, consumption logging, and security configurations. It also allows memory-section restrictions in several ways, with a locked configuration feature to prevent changes.



Each ATECC608B contains a unique 72-bit serial number stored in a standard serial EEPROM. Using the cryptographic protocols supported by the device, a host system can verify the signature of the serial number to prove that the serial number is authentic and not a copy. However, these can be easily copied with no way for the host to know if the serial number is authentic or a clone. Like all Microchip CryptoAuthentication products, the new ATECC608B employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures that eliminate potential backdoors linked to software weaknesses.

This version of the Secure Click board™ carries two versions of the ATECC608B, thus supporting the standard I2C 2-Wire interface at speed up to 1Mbps (MAHDA) and the Single Wire (SWI) interface (MAHCZ), giving the user the ability to select the desired communication interface for various security applications. While using a Single-Wire interface (SWI), this Click board™ communicates with MCU using shorted UART (RX and TX) lines, which act as a single line with only one trace routed back to the ATECC608B (MAHCZ). Further, UART pins can be used only for SWI communication when this Click board™ is used on a system. When the Single-Wire interface is enabled, the remaining pin is available as a GPIO pin marked as GP and routed to the INT pin of the mikroBUS™ socket as an authenticated output/tamper input.

This Click board™ can operate with both 3.3V and 5V logic voltage levels selected via the VCC SEL jumper. This way, it is allowed for both 3.3V and 5V capable MCUs to use the communication lines properly.

Specifications

Type	Encryption
Applications	Can be used for various security applications such as Network/IoT node endpoint security, secure boot, small message encryption, key generation for software download, and more
On-board modules	ATECC608B - cryptographic coprocessor with

MIKROELEKTRONIKA D.O.O, Batajnički drum 23, 11000 Belgrade, Serbia
VAT: SR105917343 Registration No. 20490918
Phone: + 381 11 78 57 600 Fax: + 381 11 63 09 644 E-mail: office@mikroe.com
www.mikroe.com

	secure hardware-based key storage from Microchip
Key Features	Cryptographic co-processor with secure hardware-based key storage, hardware support for asymmetric sign, verify, key agreement, networking key management, secure boot support, two interface options, and more
Interface	I2C,SWI
Feature	No ClickID
Compatibility	mikroBUS™
Click board size	M (42.9 x 25.4 mm)
Input Voltage	3.3V or 5V

Pinout diagram

This table shows how the pinout on Secure 8 Click corresponds to the pinout on the mikroBUS™ socket (the latter shown in the two middle columns).

Notes	Pin	mikroBUS™				Pin	Notes
	NC	1	AN	PWM	16	NC	
	NC	2	RST	INT	15	**GP**	General Purpse
	NC	3	CS	RX	14	**TX**	SWI Line
	NC	4	SCK	TX	13	**RX**	SWI Line
	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

Onboard settings and indicators

Label	Name	Default	Description
LD1	PWR	-	Power LED Indicator
JP1	VCC SEL	Left	Logic Level Voltage Selection 3V3/5V: Left position 3V3, Right position 5V

Secure 8 Click electrical specifications

Description	Min	Typ	Max	Unit
Supply Voltage	3.3	-	5	V
Zones	-	-	16	-
Key Size	-	-	256	-
EEPROM Memory Size	-	-	10.5	Kb
Operating Temperature Range	-40	+25	+85	°C

Software Support

MIKROELEKTRONIKA D.O.O, Batajnički drum 23, 11000 Belgrade, Serbia
VAT: SR105917343 Registration No. 20490918
Phone: + 381 11 78 57 600 Fax: + 381 11 63 09 644 E-mail: office@mikroe.com
www.mikroe.com

MikroElektronika does not provide software support for this Click board™ in the form of libraries, functions, or example code at this moment. The software support is provided by the Microchip company, with Microchip CryptoAuthentication™ library.

CryptoAuthLib is a software support library for the ATSHA204A, ATSHA206A, ATECC108A, ATECC508A, ATECC608A and ATECC608B CryptoAuthentication™ devices written in C code. It is a portable, extensible, powerful, and easy-to-use library for working with the ATSHA and ATECC device families. We now deliver the CAL through a GitHub page, so you can remove the mention to the SLA agreement and link to the above webpage.

For Technical support questions, the customers can submit a support case to Microchip by following the procedure.

Resources

mikroBUS™

mikroSDK

Click board™ Catalog

Click boards™

Downloads

Secure 8 click schematic

ATECC608B datasheet

Secure 8 click 2D and 3D files