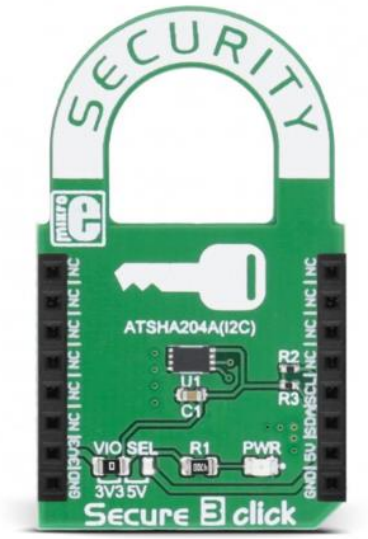
Secure 3 click

PID: MIKROE-2761

Secure 3 click carries the ATSHA204A, a cryptographic coprocessor with secure hardware-based key storage from Microchip. The click is designed to run on either 3.3V or 5V power supply. Secure 3 click communicates with the target microcontroller over an I2C interface.

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



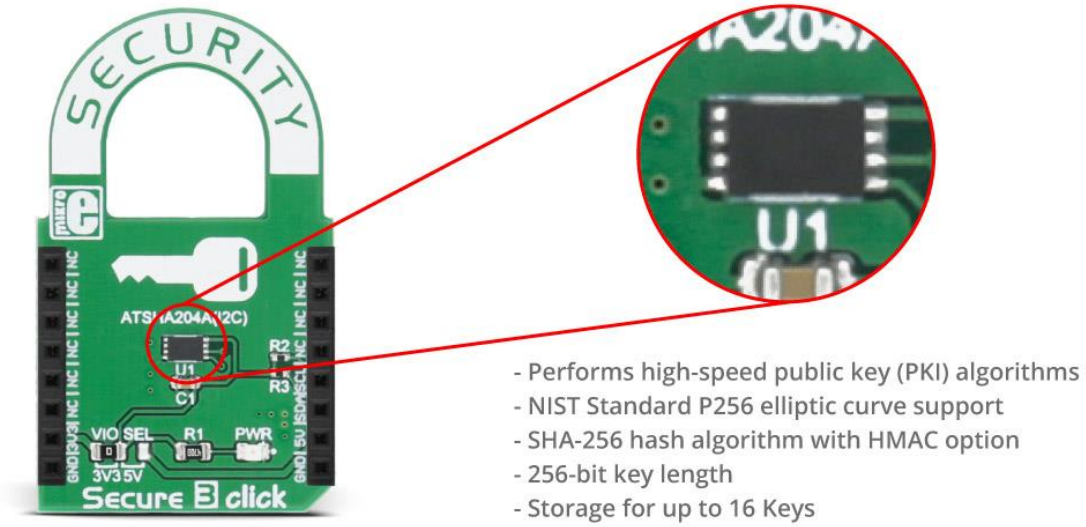
Secure 3 click carries the ATSHA204A, a cryptographic coprocessor with secure hardware-based key storage from Microchip. The click is designed to run on either 3.3V or 5V power supply. Secure 3 click communicates with the target microcontroller over an I2C interface.
It is ideal to use for:

- Secure download and boot - authentication and protect code in-transit
- Ecosystem control - ensure only OEM/licensed nodes and accessories work
- Anti-cloning - prevent building with identical BOM or stolen code
- Message security - authentication, message integrity, and confidentiality of network nodes (IoT)

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

ATSHA204A features

The ATSHA204A is a member of the Microchip Crypto Authentication™ family of high-security hardware authentication devices, which uses Secure Hash Algorithm (SHA-256) with 256-bit key length, message authentication code (MAC) and hash-based message authentication code (HMAC) options. It has a flexible command set that allows use in many applications.



The ATSHA204A device includes an Electrically Erasable Programmable Read-Only Memory (EEPROM) array that can be used for key storage, miscellaneous read/write data, read-only, secret data, consumption logging, and security configuration. Access to the various sections of memory can be restricted in a variety of ways, and the configuration can then be locked to prevent changes.

Specifications

Type	EEPROM
On-board modules	ATSHA204A - a cryptographic coprocessor with secure hardware-based key storage
Key Features	superior SHA-256 hash algorithm with 256-bit key length, message authentication code (MAC) and hash-based message authentication code (HMAC) options, storage for up to sixteen keys
Key Benefits	cost-effective symmetric authentication solution
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 3 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	NC	
	NC	3	CS	TX	14	NC	
	NC	4	SCK	RX	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

Jumpers and settings

Designator	Name	Default Position	Default Option	Description
JP1	VIO SEL.	Left	3V3	Power Supply Voltage Selection 3V3/5V, left position 3V3, right position 5V