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

RNG 2 Click

PID: MIKROE-5915

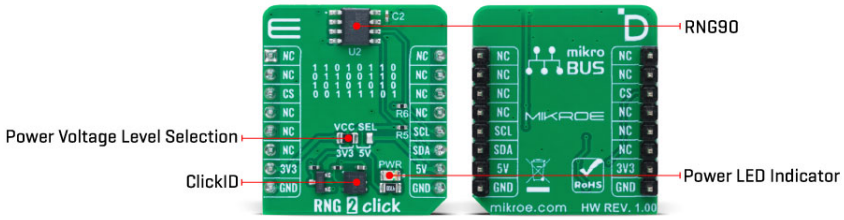
RNG 2 Click is a compact add-on board used for secure and certified random number generation in cryptographic systems. It is based on the RNG90 random number generator from Microchip, compliant with NIST SP 800-90A/B/C standards. The board generates 256-bit random numbers with a security strength of 128 bits, validated through a NIST-certified lab, and communicates via a standard I2C interface at up to 400kHz. It features a unique 72-bit serial number, advanced tamper detection, and operates on both 3.3V and 5V logic levels. RNG 2 Click is ideal for cryptographic applications, password generation, gaming systems, cryptocurrency hardware wallets, scientific research, and defense-grade security solutions.

For more information about **RNG 2 Click** visit the official product page.

How does it work?

RNG 2 Click is based on the RNG90, a secure Random Number Generator (RNG) from Microchip fully compliant with the NIST SP 800-90A/B/C standards. This Click board™ is designed to meet the stringent requirements of modern cryptographic systems, where the strength of generated random numbers directly influences the overall system security. True random number generation is critical in cryptographic applications such as key generation, digital signatures, password creation, nonce generation, random challenges, and initialization vectors. The RNG90 IC addresses these needs by producing a 256-bit random number with each Random command execution, offering a robust security strength of 128 bits. Independently validated for randomness through a NIST-certified laboratory, the RNG90 guarantees trustworthy operation in sensitive applications.

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



As part of Microchip's CryptoAuthentication™ product line, it integrates into systems demanding secure, ready-to-use randomness without requiring any additional configuration. RNG 2 Click communicates over a standard I2C interface operating at up to 400kHz, making it simple to integrate with a wide range of host MCUs. It also features a unique 72-bit serial number and advanced hardware-based security mechanisms such as an active shield for protection against invasive physical attacks, tamper detection for abnormal voltage conditions, and temperature-based tamper monitoring. With these features, RNG 2 Click is ideally suited for use in cryptographic systems, password management tools, gaming platforms, cryptocurrency hardware wallets, scientific experiments, and even aerospace and defense technologies, where secure and certified random number generation is a fundamental requirement.

This Click board™ can operate with either 3.3V or 5V logic voltage levels selected via the VCC SEL jumper. This way, both 3.3V and 5V capable MCUs can use the communication lines properly. Also, this Click board™ comes equipped with a library containing easy-to-use functions and an example code that can be used as a reference for further development.

Specifications

Type	Encryption
Applications	Ideal for cryptographic applications, password generation, gaming systems, cryptocurrency hardware wallets, scientific research, and defense-grade security solutions
On-board modules	RNG90 - secure Random Number Generator (RNG) from Microchip
Key Features	NIST SP 800-90A/B/C compliant, 256-bit random output with 128-bit security strength, unique 72-bit serial number, I2C interface up to 400kHz, active shield protection, voltage and temperature tamper detection, and more
Interface	I2C
Feature	ClickID
Compatibility	mikroBUS™
Click board size	S (28.6 x 25.4 mm)

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

Input Voltage	3.3V or 5V

Pinout diagram

This table shows how the pinout on RNG 2 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	
ID COMM	**CS**	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

Onboard settings and indicators

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

RNG 2 Click electrical specifications

Description	Min	Typ	Max	Unit
Supply Voltage	3.3	-	5	V
Random Number Output Size	-	256	-	bits
Security Strength	-	128	-	bits
Unique Serial Number Size	-	72	-	bits

Software Support

RNG 2 Click demo application is developed using the NECTO Studio, ensuring compatibility with mikroSDK's open-source libraries and tools. Designed for plug-and-play implementation and testing, the demo is fully compatible with all development, starter, and mikromedia boards featuring a mikroBUS™ socket.

Example Description

This example demonstrates the use of the RNG 2 Click board by periodically reading and logging random numbers generated by the device.

Key Functions

- rng2_cfg_setup This function initializes Click configuration structure to initial values.
- rng2_init This function initializes all necessary pins and peripherals used for this Click board.

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

- rng2_default_cfg This function executes a default configuration of RNG 2 Click board.
- rng2_read_random_num This function requests and reads a 32-byte random number from the RNG 2 Click board.

Application Init

Initializes the logger and the Click board driver, then applies the default configuration.

Application Task

Reads and displays a 32-byte random number from the device every second.

Application Output

This Click board can be interfaced and monitored in two ways:

- Application Output - Use the "Application Output" window in Debug mode for real-time data monitoring. Set it up properly by following this tutorial.
- UART Terminal - Monitor data via the UART Terminal using a USB to UART converter. For detailed instructions, check out this tutorial.

Additional Notes and Information

The complete application code and a ready-to-use project are available through the NECTO Studio Package Manager for direct installation in the NECTO Studio. The application code can also be found on the MIKROE GitHub account.

Resources

mikroBUS™

mikroSDK

Click board™ Catalog

Click boards™

ClickID

Downloads

RNG 2 click example package

RNG 2 click 2D and 3D files v100

RNG 2 click schematic v100

RNG90 datasheet