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

SE051 Plug&Trust Click

PID: MIKROE-5392

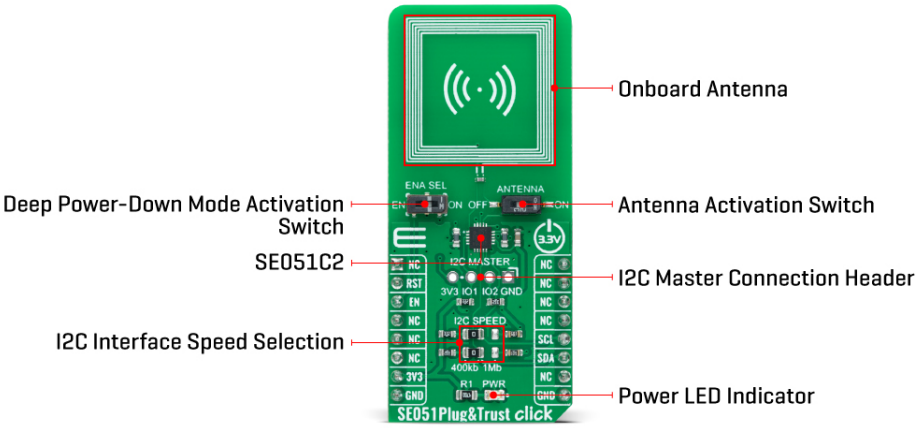
SE051 Plug&Trust Click is a compact add-on board representing a ready-to-use IoT security solution. This board features the SE051C2, an updatable extension of the EdgeLock™ SE050 from NXP Semiconductor, which delivers proven security certified to CC EAL 6+, with AVA_VAN.5up to the OS level. Designed for the latest IoT security requirements, it allows securely storing and provisioning credentials performing cryptographic operations, giving edge-to-cloud security capability right out of the box. It also provides upgrade functionality of the IoT applet while preserving on-device credentials, alongside reconfiguration possibility. This Click board™ is versatile in IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, attestation and proof of device origin, and many more.

SE051 Plug&Trust Click is supported by a mikroSDK compliant library, which includes functions that simplify software development. This Click board™ comes as a fully tested product, ready to be used on a system equipped with the mikroBUS™ socket.

How does it work?

SE051 Plug&Trust Click, as its foundation, uses the SE051C2, a ready-to-use IoT secure element solution from NXP Semiconductor, providing a root of trust at the IC level and giving an IoT system state-of-the-art, edge-to-cloud security capability right out of the box. It has an independent Common Criteria EAL 6+ security certification up to OS level and supports both RSA & ECC asymmetric cryptographic algorithms with high key length and future-proof ECC curves. Designed for the latest IoT security requirements, it allows for securely storing, provisioning credentials, and performing cryptographic operations for security-critical communication and control functions.

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



The SE051C2 represents a turnkey solution with a Java Card operating system and an updatable pre-installed applet optimized for IoT security use cases. Alongside the updatable IoT applet, it also possesses SEMS Lite as well as a PERSO applet that provides upgradability of the IoT applet while preserving on-device credentials and the possibility to reconfigure the SE051 device. The SEMS Lite represents a capability based on a subset of GlobalPlatform's Secure Element Management Service (SEMS), optimized for IoT use cases.

This Click board™ communicates with MCU using the standard I2C 2-Wire interface. Besides the mandatory connection to the host controller, this Click board™ can optionally be connected to a sensor node or similar element through separate I2C interface pins on the 1x4 male header labeled I2C Master. In this case, the SE051C2 device is the Controller device, and the sensor node represents the Target. This board also allows the user to select the appropriate I2C communication speed by onboard SMD jumpers labeled as I2C SPEED to a proper position marked as 400Kb and 1Mb. Note that all the jumpers must be lined to the same side, or else the Click board™ may become unresponsive.

Besides, the SE051C2 provides a special power-saving mode offering maximum power saving. The way of activation of this mode is realized with the onboard switch marked as ENA SEL. In this way, Power-Saving Mode can be activated via the EN pin, routed to the CS pin of the mikroBUS™ socket, primarily by placing the switch to the EN position and then pulling the EN pin to a logic zero level. By placing the switch in the second position marked as ON, the SE051C2 is in normal operation mode. The RST pin has no functionality in I2C Mode. It can only be used as an external reset source if the ISO7816 interface is enabled (not enabled in generic SE051 configurations).

Also, the SE051 Plug&Trust Click has an onboard antenna, providing a wireless interface (ISO14443) to an external device like a smartphone, connected via a switch labeled as ANTENNA with SE051C2 allowing the activation of the antenna itself by setting it to the appropriate ON or OFF position.

This Click board™ can be operated only with a 3.3V logic voltage level. The board must perform appropriate logic voltage level conversion before using MCUs with different logic levels. However, the Click board™ comes equipped with a library containing functions and an example code that can be used, as a reference, for further development.

Specifications

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

Type	Encryption,IoT security
Applications	Can be used in IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, attestation and proof of device origin, and more
On-board modules	SE051C2 - ready-to-use IoT secure element solution from NXP Semiconductor
Key Features	Updatable extension of the EdgeLock™ SE050, Common Criteria EAL6+ certification, pre-installed IoT applet, SEMS Lite future-proof security, maximum flexibility, optional I2C Master to support new IoT security use cases, ISO14443 interface, Deep Power-Down Mode, and more
Interface	I2C
Feature	No ClickID
Compatibility	mikroBUS™
Click board size	L (57.15 x 25.4 mm)
Input Voltage	3.3V

Pinout diagram

This table shows how the pinout on SE051 Plug&Trust 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	
ISO7816 Reset	**RST**	2	RST	INT	15	NC	
Deep Power-Down Mode	**EN**	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	NC	
Ground	**GND**	8	GND	GND	9	**GND**	Ground

Onboard settings and indicators

Label	Name	Default	Description
LD1	PWR	-	Power LED Indicator
JP1-JP2	I2C SPEED	Left	I2C Speed Selection 400Kb/1Mb: Left position 400Kb, Right position 1Mb
SW1	ANTENNA	Left	Antenna Activation Switch OFF/ON: Left position OFF, Right

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

			position ON
SW2	ENA SEL	Right	Deep Power-Down Mode Activation Switch EN/ON: Left position EN, Right position ON
J1	I2C MASTER	Unpopulated	I2C Master Connection Header

SE051 Plug&Trust Click electrical specifications

Description	Min	Typ	Max	Unit
Supply Voltage	-	3.3	-	V
Antenna Operating Frequency	-	13.56	-	MHz
User Memory	46	-	104	kB
I2C Interface Speed	400	-	1000	kHz
Operating Temperature Range	-40	+25	+105	°C

Software Support

We provide a library for the SE051 Plug & Trust Click as well as a demo application (example), developed using MikroElektronika compilers. The demo can run on all the main MikroElektronika development boards.

Package can be downloaded/installed directly from NECTO Studio Package Manager(recommended way), downloaded from our LibStock™ or found on Mikroe github account.

Library Description

This library contains API for SE051 Plug & Trust Click driver.

Key functions

- se051plugntrust_apdu_write This function writes a @b frame_data to device.
- se051plugntrust_apdu_read This function reads a @b frame_data from device.
- se051plugntrust_apdu_transfer This function writes a @b frame_data and then reads return data from device and stores it in @b frame_data.

Example Description

This application is showcasing basic functionality of SE051 Plug&Trust Click board™. It gets identify data from device, selects card manager and applet. Then checks free memory, reads all objects and deletes not reserved ones. After that showcases a few of functionality: Generating random data, Creating, reading and deleting binary objects, Creating AES symmetrical key and cipher with it; In the end it is showcasing funcionality in the endless loop.

The full application code, and ready to use projects can be installed directly from NECTO Studio Package Manager(recommended way), downloaded from our LibStock™ or found on Mikroe github account.

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

Other Mikroe Libraries used in the example:

- MikroSDK.Board
- MikroSDK.Log
- Click.SE051PlugnTrust

Additional notes and informations

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. UART terminal is available in all MikroElektronika compilers.

mikroSDK

This Click board™ is supported with mikroSDK - MikroElektronika Software Development Kit. To ensure proper operation of mikroSDK compliant Click board™ demo applications, mikroSDK should be downloaded from the LibStock and installed for the compiler you are using.

For more information about mikroSDK, visit the official page.

Resources

mikroBUS™

mikroSDK

Click board™ Catalog

Click boards™

Downloads

SE051 Plug&Trust click example on Libstock

SE051 datasheet

SE051 Plug&Trust click 2D and 3D files

SE051 Plug&Trust click schematic

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Mikroe:

MIKROE-5392