A5000 Plug&Trust Click

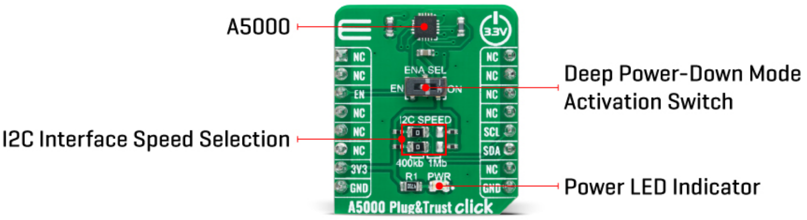
PID: MIKROE-5391

A5000 Plug&Trust Click is a compact add-on board representing a ready-to-use secure IoT authenticator. This board features the EdgeLock® A5000, a Secure Authenticator from NXP Semiconductors. The A5000 provides a root of trust at the IC level, giving an IoT authentication system state-of-the-art security capability. It allows for securely storing and provisioning credentials and performing cryptographic operations for security-critical communication and authentication functions. It has an independent Common Criteria EAL 6+ security certification up to OS level and supports ECC asymmetric cryptographic and AES/3DES symmetric algorithms. This Click board™ is suitable in IoT security use cases such as secure connection to public/private clouds, device-to-device authentication, or counterfeit protection.

A5000 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?

A5000 Plug&Trust Click, as its foundation, uses the A5000, a secure IoT authenticator based on Integral Security Architecture 3.0™ from NXP Semiconductors, providing secure and efficient protection for authentication and anti-counterfeit use cases. This Click board™ is designed to be part of an IoT system; works as an auxiliary security device attached to a host MCU. A Common Criteria EAL6+ certification proves the efficiency of the security measures. It is ideal for many authentication use cases without the need to write security code, and comes with ECC asymmetric cryptographic and AES/3DES symmetric algorithms support to protect the A5000 even against sophisticated non-invasive and invasive attack scenarios.



The A5000 operates autonomously based on an integrated Java Card operating system and a full-fledged authentication applet. The Authentication Applet features a generic file system that stores secure objects and associated privilege management. Direct memory access is possible only by the NXP Authentication applet's fixed functionalities. With that, the content from memory is fully isolated from the host system.

This Click board™ communicates with MCU using the standard I2C 2-Wire interface. The communication with the A5000 authenticator follows a command/response concept. It means that after sending the entire command to the authenticator, all data must be retrieved fully to allow sending of the following command. 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 A5000 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 A5000 is in normal operation mode.

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

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 counterfeit protection
On-board modules	A5000 - secure IoT authenticator from NXP Semiconductors
Key Features	Based on Integral Security Architecture 3.0™,

	secure and efficient protection for authentication and anti-counterfeit use cases, Common Criteria EAL6+ certification, ECC asymmetric cryptographic and AES/3DES symmetric algorithms support, Deep Power-Down Mode, and more
Interface	I2C
Feature	No ClickID
Compatibility	mikroBUS™
Click board size	S (28.6 x 25.4 mm)
Input Voltage	3.3V

Pinout diagram

This table shows how the pinout on A5000 Plug&Trust 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	
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	ENA SEL	Right	Deep Power-Down Mode Activation Switch EN/ON: Left position EN, Right position ON

A5000 Plug&Trust Click electrical specifications

Description	Min	Typ	Max	Unit
Supply Voltage	-	3.3	-	V
User Memory	-	-	8	kB
I2C Interface Speed	400	-	1000	kHz
Operating Temperature Range	-40	+25	+105	°C

Software Support

We provide a library for the A5000 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 A5000 Plug&Trust Click driver.

Key functions

- a5000plugntrust_apdu_write This function writes a @b frame_data to device.
- a5000plugntrust_apdu_read This function reads a @b frame_data from device.
- a5000plugntrust_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 A5000 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.

Other Mikroe Libraries used in the example:

- MikroSDK.Board
- MikroSDK.Log
- Click.A5000PlugnTrust

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

A5000 Plug&Trust click example on Libstock

A5000 Plug&Trust click 2D and 3D files

A5000 datasheet

A5000 Plug&Trust click schematic