

Trust M Click



PID: MIKROE-4236

Trust M Click is trust anchor add-on board for advanced security combined with high performance for connected devices that address individual needs in the field of embedded authentication, brand protection and further security applications. Its based on SLS 32AIA010 [OPTIGA™ Trust M1](#) high-end security controller from [Infineon](#), that features advanced security controller with built-in tamper proof NVM for secure storage and Symmetric/Asymmetric crypto engines. The OPTIGA™ Trust M1 covers a broad range of use cases necessary for many types of applications that include Network node protection using Mutual Authentication such as TLS or DTLS, Protect the Authenticity, Integrity and Confidentiality of data and IP, Secure Communication and many more.

How does it work?

As embedded systems (e.g. IoT devices) are increasingly gaining the attention of attackers, Trust M Click offers the OPTIGA™ Trust M1 from Infineon as a turnkey security solution for industrial automation systems, smart homes, consumer devices and medical devices. This high-end security controller comes with full system integration support for easy and cost-effective deployment of high-end security for your assets.

Mikroe produces entire development toolchains for all major microcontroller architectures.

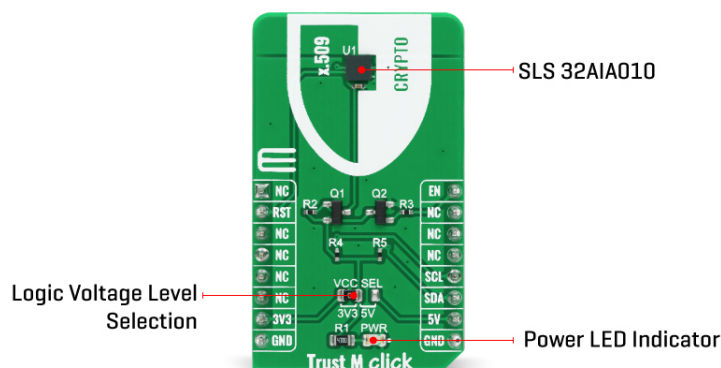
Committed to excellency, we are dedicated to helping engineers bring the project development up to speed and achieve outstanding results.



ISO 27001: 2013 certification of informational security management system.
 ISO 14001: 2015 certification of environmental management system.
 OHSAS 18001: 2008 certification of occupational health and safety management system.



ISO 9001: 2015 certification of quality management system (QMS).



Trust M Click comes with up to 10kB user memory that can be used to store X.509 certificates and data. OPTIGA™ Trust M1 is based on Common Criteria (CC) Certified EAL6+ (high) hardware enabling it to prevent physical attacks on the device itself and providing high assurance that the keys or arbitrary data stored cannot be accessed by an unauthorized entity.

All communication is done through I2C bus which supports a highspeed I2C communication interface of up to 1MHz (FM+). Trust M Click also features two FETs for disconnecting/connecting power to IC using EN pin on mikroBUS™ which allows it to go to hibernation.

During chip production, unique asymmetric keys (private and public) are generated. The public key is signed by customer specific CA and the resulting X.509 certificate issued is securely stored in the OPTIGA™ Trust M1. Special measures are taken to prevent the leakage and modification of private key material at the Common Criteria Certified production site.

All of this features available on Trust M Click makes it perfect solution for industrial automation systems, smart homes and consumer devices in broad range of use cases necessary to protect the authenticity, integrity and confidentiality in your device: mutual authentication, secured communication, data store protection, life-cycle management, secured updates, and also platform integrity protection.

Specifications

Type	Encryption
Applications	Industrial control and automation, Consumer electronics and Smart Home, Medical devices and more
On-board modules	SLS 32AIA010
Key Features	Symmetric/Asymmetric crypto engines to support ECC 256/384, RSA® 1024/2048 and SHA-256
Interface	GPIO, I2C
ClickID	No
Compatibility	mikroBUS™
Click board size	M (42.9 x 25.4 mm)

Mikroe produces entire development toolchains for all major microcontroller architectures.

Committed to excellency, we are dedicated to helping engineers bring the project development up to speed and achieve outstanding results.



ISO 27001: 2013 certification of informational security management system.
ISO 14001: 2015 certification of environmental management system.
OHSAS 18001: 2008 certification of occupational health and safety management system.



ISO 9001: 2015 certification of quality management system (QMS).

Input Voltage	3.3V or 5V
---------------	------------

Pinout diagram

This table shows how the pinout on Trust M 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	EN	Enable
Reset	RST	2	RST	INT	15	NC	
	NC	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
PWR	LD1	-	Power LED Indicator
VCC SEL	JP1	Left	Logic level voltage selection: left position 3V3, right position 5V

Software Support

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 our development partner on this project Infineon. Please visit the [Infineon Github repository](#) to get the full software support and Command Line Interface (CLI) for Optiga Trust M device.

Resources

[mikroBUS™](#)

[mikroSDK](#)

[Click board™ Catalog](#)

[Click boards™](#)

Downloads

[Trust M click 2D and 3D files](#)

[OPTIGA Trust M datasheet](#)

[Trust M click schematic](#)

Mikroe produces entire development toolchains for all major microcontroller architectures.

Committed to excellency, we are dedicated to helping engineers bring the project development up to speed and achieve outstanding results.



ISO 27001: 2013 certification of informational security management system.
ISO 14001: 2015 certification of environmental management system.
OHSAS 18001: 2008 certification of occupational health and safety management system.



ISO 9001: 2015 certification of quality management system (QMS).