CryptoAuth Pro Trust Platform User Guide

EV89U05A

Product Page Links

Introduction

The Microchip CryptoAuth Pro Trust Platform is an enhanced version of the CryptoAuth Trust Platform Board and is part of the CryptoAuthentication™ evaluation kit portfolio.

The CryptoAuth Pro Trust Platform kit extends the CryptoAuth Trust Platform with a more powerful Cortex M4 microcontroller, four on-board CryptoAuthentication devices, two mikroBUS™ sockets, and an on-board 10/100 Mbit Ethernet PHY. The board also contains the Microchip Technology PKoB4 debugger, which is compatible with MPLAB®X IDE. The application microcontroller has been configured to readily make use of many of the features provided on the board.

This user guide provides a physical overview of the connections, components and features associated with the CryptoAuth Pro Trust Platform development kit.

Figure 1. CryptoAuth Pro Trust Platform

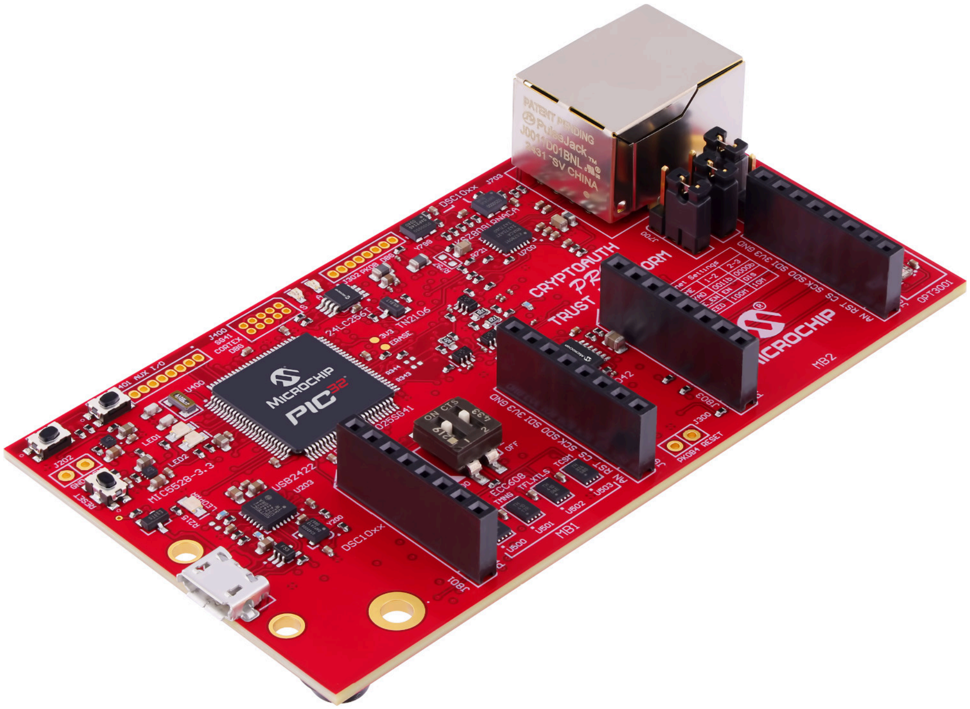
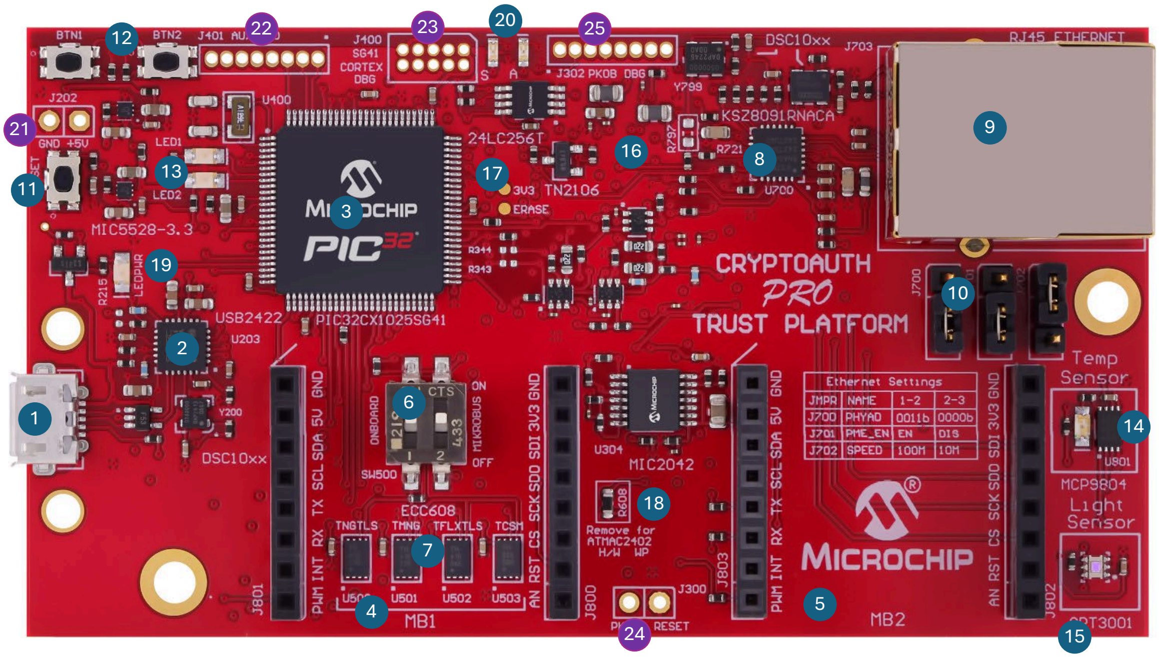


Table of Contents

1. Hardware Overview

The CryptoAuth Pro Trust Platform consists of a Microchip PIC32CX1025SG41 microcontroller configured as the main MCU. It comes pre-programmed with Microchip's Secure Computing Group (SCG) kit protocol. This protocol facilitates the communication between the CryptoAuthentication™ device(s) and the host MCU over the USB HID interface. Data transfers between the secure element(s) and the host MCU are indicated by the PKoB4 status LED.

Figure 1-1. CryptoAuth Pro Trust Platform Top View Components

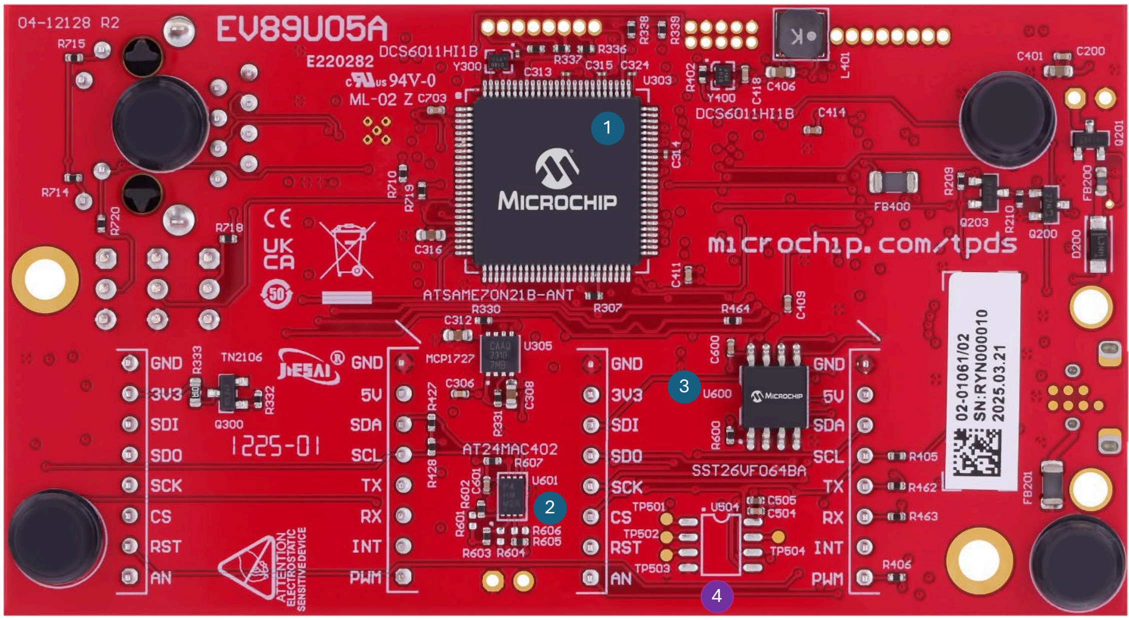


1. USB Connector
2. USB2422 Dual Port Hub
3. PIC32CX1025SG41 Host MCU
4. mikroBUS™ Header #1
5. mikroBUS Header #2
6. Dual SPST DIP Switch
7. ECC608 Secure Elements
8. KSZ8091RNACA 10/100 Mbit Ethernet PHY
9. 10/100 Ethernet Connector
10. Ethernet Selection Switches
11. Reset Button
12. User Defined Buttons
13. User-Defined LEDs
14. Temp Sensor
15. Light Sensor
16. Selection Resistor for External Ethernet Oscillator
17. PKoB4 Chip Erase Pads
18. AT24MAC402 Write-Protect Resistor
19. LED Power Indicator (Yellow)
20. PKoB4 Active (Green) and Status (Yellow) LEDS

Non-Populated Features

21. External Power Connector
22. 1x8, 50 mil Pitch Header for SG41 Optional I/Os
23. 2x5, 50 mil Pitch Cortex Header for SG41 Programming
24. PKoB4 Reset Jumper
25. 1x8, 50 mil Pitch Header for PKoB4 Debugger

Figure 1-2. CryptoAuth Pro Trust Platform Bottom View Components



1. PKoB4 On-Board Debugger
2. AT24MAC402 Serial EEPROM
3. SST26VF064B 64-Mbit Quad SPI Memory
4. Alternate SOIC Crypto Device Footprint (Unpopulated)

1.1. Kit Ordering Code and Components

Ordering Information

- **Kit Name:** CryptoAuth Pro Trust Platform Development Kit
- **Ordering Code:** EV89U05A
- **Availability:** The kit will be available from Microchip Direct and multiple distributors.
- **Website:** www.microchip.com/en-us/development-tool/EV89U05A

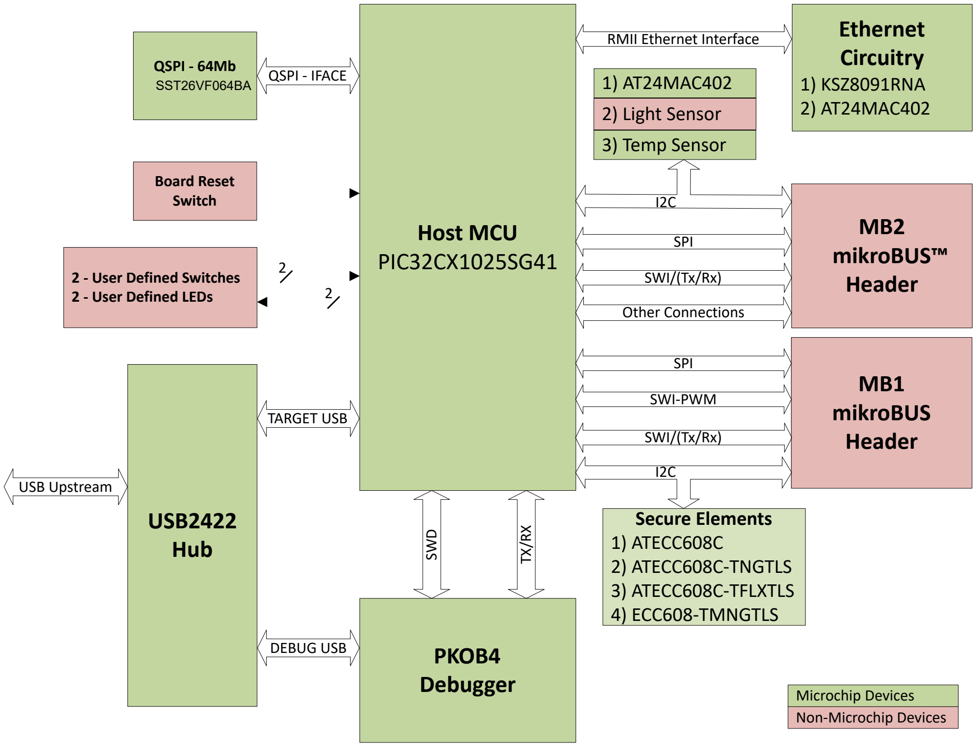
CryptoAuth Pro Trust Platform Kit Contents and Requirements

- Includes one CryptoAuth Pro Trust Platform board.
- A micro USB cable (not included) is required to operate the board.
- For wired connectivity, an ethernet cable (not included) is required. Customers can select a cable based on the performance requirements of the application. A CAT 5 cable will support up to 100 Mbps.

1.2. Functional Description

The block diagram below illustrates the major connections of the CryptoAuth Pro Trust Platform. For additional details, refer to the board schematics referenced in Hardware Documentation.

Figure 1-3. Block Diagram



1.2.1. Microcontroller

The PIC32CX1025SG41 microcontroller is an Arm® Cortex M4 based microcontroller. The version chosen for use on this board is in a 100-Pin TQFP package. Depending on the actual application, other packages are available, including a 64-Pin TQFP, 128-Pin TQFP and a 100-Pin BGA. The microcontroller is connected to and can control all the major features on the board. These connections will be detailed in individual sections.

1.2.2. Crypto Devices

Four Microchip CryptoAuthentication™ devices are included on the CryptoAuth Pro Trust Platform. Each device has a unique I^{2}C address and can coexist on the same I^{2}C bus. This particular bus is shared only with the I^{2}C connections of the mikroBUS™ MB1 connector. The MB1 mikroBUS connector allows other cryptographic devices to be connected to the board.

On the backside of the board is an optional SOIC footprint that can be used with other I^{2}C CryptoAuthentication or CryptoAutomotive™ devices. Devices mounted to this footprint will be connected to the same I^{2}C interface as the crypto devices mounted on the board.

Important: Ensure that any device mounted to the optional footprint has a unique I^{2}C address, distinct from those of the devices directly mounted on the board.

Table 1-1. On-Board CryptoAuthentication™ devices.

Device	Default 7-bit I^{2}C Address	I^{2}C R/W Address Byte Values	
		Write	Read
ATECC608C-TCSM	`0x60`	`0xC0`	`0xC1`
ATECC608C-TNGTLS	`0x35`	`0x6A`	`0x6B`
ATECC608C-TFLXTLS	`0x36`	`0x6C`	`0x6D`
ECC608-TMNGTLS	`0x38`	`0x70`	`0x71`

Microcontroller Interface

The CryptoAuthentication devices are connected to the microcontroller only through the I^{2}C bus. There are no other signals that can be connected. The devices are powered with 3.3V. Each of the I^{2}C signals has a 10k pull-up resistor.

- Signal Connections: PA23(SCL), PA22(SDA)
  - PA22(SDA) - Sercom #3. Pin Mux Configuration: IOSET1-PAD0
  - PA23(SCL) - Sercom #3. Pin Mux Configuration: IOSET1-PAD1
- Special Considerations: Set Dip Switch S500 to select the on-board connection and optionally disable the mikroBUS connections. Note that both switches can be enabled, provided that no device has a duplicate I^{2}C address. The kit protocol software will currently only detect up to eight devices on the I^{2}C bus.

Related Links

Additional On-Board Crypto Device

1.2.3. mikroBUS™ MB1 Connector

The mikroBUS MB1 connector is intended primarily to work with Microchip Technology CryptoAuthentication™ and CryptoAutomotive™ device families. The connector provides interfaces to I^{2}C, SPI, SWI and SWI-PWM interfaces used by the various devices in those families. There is a wide range of dedicated mikroBUS boards with CryptoAuthentication devices that can be connected to this interface, as well as multiple socket-based boards. The socket-based boards can be used with various devices and are especially useful when you wish to configure a device prior to installing it on a board.

Microcontroller Interface

Table 1-2. MB1 Connector

SG41 Connections			MB1 Connector		SG41 Connections		
Sercom #	IOSET	Pin #	J801	J800	Pin #	IOSET	Sercom #
—	—	—	GND	GND	—	—	—
—	—	—	5.0V	3.3V	—	—	—
Sercom #3	IOSET1-PAD0	PA22	SDA	SDI	PB12	IOSET1-PAD0	Sercom #4
Sercom #3	IOSET1-PAD1	PA23	SCL	SDO	PB15	IOSET1-PAD3	Sercom #4
Sercom #5	IOSET6-PAD3	PB01	TX	SCK	PB13	IOSET1-PAD1	Sercom #4
Sercom #5	IOSET6-PAD0	PB02	RX	CS	PB14	IOSET1-PAD2	Sercom #4
—	EXTINT[0]	PC00	INT	RST	PB06	—	—
—	—	PB09	PWM[1]	AN	PA05[2]	—	—

Notes: Configuration Options: The PWM and AN signals are defined as digital GPIOs for the default application but can be configured to support the intended mikroBUS functionality. See the PIC32CX1025SG41 data sheet for more information.

1. The PWM signal can be configured as PWM signal as TC4.
2. The AN signal can be configured as either ADC0/AIN[5] analog input or AC/AIN[1] analog comparator input.

Operational Notes:

- I^{2}C Operation Notes:
  - The I^{2}C bus connects to the four on-board secure elements and the optional secure element footprint.
  - Additional secure elements can be added to the bus through the mikroBUS connector.
  - Dip switch S500 can be used to select only the on-board secure elements, the external mikroBUS I^{2}C interface, or both. This switch only impacts I^{2}C connectivity.
- SPI Operation Notes:
  - The SPI interface has been defined to work with Microchip CryptoAutomotive devices that support an SPI interface. These currently include the TA100 and the TA101 devices.
- UART Operation Notes:
  - The UART interface is intended for use with the Microchip CryptoAuthentication devices that support an SWI interface. These devices include the ATECC608x and ATSHA204A family of devices.
  - The UART signals Rx/Tx swap as they pass through the mikroBUS extension board.
- The PWM signal is used to support the SWI-PWM interface of Microchip CryptoAuthentication devices. These devices currently include SHA104, SHA106, ECC204, ECC206 and TA010.
- The microcontroller pins selected for the INT, RST and AN signals support the functionality intended by the mikroBUS specification. These signals can be used for alternate GPIO functionality as required and are not currently used by any CryptoAuthentication devices.

Related Links

mikroBUS and Click Add-On Boards

1.2.4. mikroBUS™ MB2 Connector

The mikroBUS MB2 connector is set up as a generic mikroBUS header. The devices can be used with mikroBUS extension boards that have SPI, I^{2}C, Serial Port I/O, as well as some generic GPIO signals. The MB2 connector signaling is entirely separate from that of the MB1 connector.

Expected uses of the port includes digital sensors, analog sensors, WiFi modules and other devices.

Microcontroller Interface

Table 1-3. MB2 Connector

SG41 Connections			MB2 Connector		SG41 Connections		
Sercom #	IOSET	Pin #	J803	J802	Pin #	IOSET	Sercom #
—	—	—	GND	GND	—	—	—
—	—	—	5.0V	3.3V	—	—	—
Sercom #2	IOSET4-PAD0	PB25	SDA	SDI	PC12	IOSET1-PAD0	Sercom #7
Sercom #2	IOSET4-PAD1	PB24	SCL	SDO	PC15	IOSET1-PAD3	Sercom #7
Sercom #6	IOSET1-PAD0	PC16	TX	SCK	PC13	IOSET1-PAD1	Sercom #7
Sercom #6	IOSET1-PAD1	PC17	RX	CS	PC14	IOSET1-PAD2	Sercom #7
—	EXTINT[6]	PA06	INT	RST	PA07	—	—

Table 1-3. MB2 Connector (continued)

SG41 Connections			MB2 Connector		SG41 Connections		
Sercom #	IOSET	Pin #	J803	J802	Pin #	IOSET	Sercom #
—	TC[4]	PB08	PWM	AN	PA04	AIN[0]/AIN[4]	—

Notes: Configuration Options: The PWM and AN signals are defined as digital GPIOs for the default application but can be configured to support the intended mikroBUS functionality. See the PIC32CX1025SG41 data sheet for more information.

1. The PWM signal can be configured as PWM signal TC4.
2. The AN signal can be configured as either ADC0/AIN[4] analog input or AC/AIN[0] analog comparator input.

Operational Notes:

- The on-board temperature sensor (MCP9804), light sensor (OTP3001) and AT24MAC402 serial EEPROM share the I^2C bus.
- The UART signals Rx/Tx swap as they pass through the mikroBUS extension board.
- The microcontroller pins selected for the INT, RST, PWM and AN signals support the functionality intended by the mikroBUS specification. These signals can be used for alternate GPIO functionality as required.

Related Links

On-Board Sensors
WINCS02 mikroBUS board
mikroBUS and Click Add-On Boards

1.2.5. User-Defined LEDs and Push Buttons

To facilitate the development of applications, two user-defined LEDs and two user-defined push buttons have been added to the CryptoAuth Pro Trust Platform development board. The LEDs (LED1, LED2) can be used to indicate status associated with some application code, and the push buttons (BTN1, BTN2) can be used to initiate actions associated with the code.

Table 1-4. User Defined LEDs and Push Buttons

Item	Pin #	Pin Name	Configuration	Actions:
LED1	7	PA02	Output	LED ON: PA02 = LOW LED OFF: PA02 = HIGH
LED2	8	PA03	Output	LED ON: PA03 = LOW LED OFF: PA03 = HIGH
BTN1	5	PC02	Input	Detect LOW: Button Pressed Detect HIGH: Button Not Pressed
BTN2	4	PC01	Input	Detect LOW: Button Pressed Detect HIGH: Button Not Pressed

Remember: The GPIO signals connected to the push buttons must enable the internal pull-up resistor on the GPIO pin to fully ensure the signal is not floating when the button is not pressed.

1.2.6. On-Board Sensors

The CryptoAuth Pro Trust Platform contains a temperature sensor and a light sensor. Each of the sensors can communicate using a shared I^2C bus.

Temperature Sensor

The MCP9804 is a Microchip temperature sensor that can measure temperatures in the range of -40℃ to +125℃. The device has multiple features that can be set, including the resolution accuracy and high and low temperature thresholds. The I^{2}C address of the device has three selectable address pins. For this design, all have been defaulted to low. The default 7-bit I^{2}C address of the device is 0x18.

The device also supports an external threshold alert signal that will trip when the temperature is outside of the low or high temperature thresholds. These out-of-range conditions can be programmed into the MCP9804 via the I^{2}C port. Additionally, the polarity of this signal can be configured as one of the device's features. For further details, please refer to the MCP9804 data sheet.

Microcontroller Interface:

- ***I^{2}C Signal Connections:*** PB24(SCL), PB25(SDA)
  - PB25(SDA) - Sercom #2. Pin Mux Configuration: IOSET2-PAD0
  - PB24(SCL) - Sercom #2. Pin Mux Configuration: IOSET2-PAD1
- ***Other Connections:***
  - Signal Connections: PC05(Alert), PC06(LED-Enable)
    - PC05 (Alert) - Must be configured as an input.
    - PC06 (LED Temperature Alert Indicator) - Must be configured as an output and must initially be driven high or left floating so that the LED will be off. The microcontroller can drive PC06 low when the PC05 alert signal indicates an out-of-range condition.
- ***Special Considerations:*** The on-board light sensor, MB2 mikroBUS header and AT24MAC402 share the I^{2}C port with the temperature sensor.

Light Sensor

The OPT3001 is a light sensor with an I^{2}C interface. The device can operate between -40℃ and +85℃. It can measure light in the range of .01 to 83k lux using a 23-bit ADC.

The I^{2}C address of the device has one selectable address pin. For this design, it has been defaulted to low. The default 7-bit I^{2}C address of the device is 0x44.

Microcontroller Interface:

- ***I^{2}C Signal Connections:*** PB24(SCL), PB25(SDA)
  - PB25(SDA) - Sercom #2. Pin Mux Configuration: IOSET2-PAD0
  - PB24(SCL) - Sercom #2. Pin Mux Configuration: IOSET2-PAD1
- ***Other Connections:***
  - The INT signal is not connected to the microcontroller.
- ***Special Considerations:*** The on-board temp sensor, MB2 mikroBUS header and AT24MAC402 share the I^{2}C port with the light sensor.

Related Links

mikroBUS MB2 Connector
Ethernet Functionality

1.2.7. Ethernet Functionality

The CryptoAuth Pro Trust Platform supports 10BASE-T/100BASE-T Ethernet functionality. The PIC32CX1025SG41 provides the Media Access Controller (MAC) functionality, and the KSZ8091RNA Ethernet Transceiver provides the physical layer interface. The board utilizes the Reduced Media-Independent Interface (RMII).

Microcontroller Interface

Table 1-5. Ethernet Connectivity

SG41 Connections	KSZ8091RNACA				SG41 Connections
Pin #	Pin #	Pin Name	Pin Name	Pin #	Pin #
1.2V Decoupling	1	VDD_1V2	$\overline{\text{RST}}$	24	PA16
3.3V Analog Supply	2	VDDA_3V3	SPEED	23	J702
PA22	3	RXP	GND	22	GND
PA23	4	RXM	TXD1	21	PA19
PB01	5	TXM	TXD0	20	PA18
PB02	6	TXP	TXEN	19	PA17
PC00	7	XO	INTRP	18	PC21
PB09	8	XI	PME_EN	17	J701
External Resistor	9	REXT	REF_CLK	16	PA14
PA21(IOSET4)	10	MDIO	PHYAD	15	J700
PA20	11	MDC	VDDIO	14	3.3V
PA12	12	RXD1	RXD0	13	PA13

Ethernet Feature Selection

The board is set up with three selection jumpers that control features of the Ethernet PHY, provided the PHY has been configured to make use of one or more of these features.

Table 1-6. Ethernet PHY Jumpers

Jumper #	Function	Jumper Position	
J700	PHY Physical Address	2-3 (Default)	PhyAdd = 00000b
		1-2	PhyAdd = 00011b
J701	Wake-on LAN Enable	2-3 (Default)	Disabled
		1-2	Enabled
J702	Auto Negotiation and Speed Mode	1-2 (Default)	Enable Auto Negotiation and set speed to 100 Mbps
		2-3	Disable Auto Negotiation and set speed to 10 Mbps

MAC Address

The board comes mounted with an AT24MAC402 serial EEPROM pre-progammed with a MAC address. The MAC address is stored in the serial EEPROM and can only be read. The serial EEPROM can also be used to store other data beyond the MAC Address. If so desired, the main memory array can be write-protected.

The Serial EEPROM has three different I^{2}C addresses that allow access to different parts of the memory array. The addresses shown below are the default addresses for the EV89U05A development board. Addresses can be modified by the way resistors R601 through R606 are populated. Note that modifications of these resistors adjust all three of the addresses. See the AT24MAC402 data sheet for more details.

Table 1-7. AT24MAC402 I^{2}C Addresses

I^{2}C Address (7-Bit)	Function	Access Type	Comments
0x56	General Purpose Memory Array Address	R/W	Setup up for Read/Write Access. Can be write-protected through the removal of resistor R608.
0x5E	MAC Address	R	Can only be read. Cannot be overwritten.
0x36	WP Register Address	R/W	Used to check the write protection status of the memory.

1.2.8. QSPI Memory Functionality

The CryptoAuth Pro Trust Platform contains a single 64-Mbit QSPI flash memory device that can be used by the PIC32CX1025SG41 for storing and executing code. The PIC32CX1025SG41 allows Execute-In-Place (XIP) directly from the memory.

Microcontroller Interface

Table 1-8. SST26VF064B Microcontroller Connections

SG41 Connections	SSTV26VF064B				SG41 Connections
Pin Name	Pin #	Pin Name	Pin Name	Pin #	Pin Number
PB11	1	CE#	V_{DD}	8	3.3V
PA09	2	SIO1	SIO3	7	PA11
PA10	3	SIO2	SCK	6	PB10
GND	4	V_{SS}	SIO0	5	PA08

1.3. Optional Features

Several optional features are available on the CryptoAuth Pro Trust Platform but require hardware modifications. These optional features are described in the following subsections.

1.3.1. External Debugger Connections to the SG41

The PKoB4 on-board debugger will typically be all that is needed to program the PIC32CX1025SG41 microcontroller. If, for some reason, there is a desire to use an external debugger/programmer, there is an option to do this by populating some additional features of the board and following the procedure below.

Hardware Requirements

1. Cortex Header: 2x5 50 mil pitch
   - Manufacturer: Amphenol FCI
   - Part Number: 20021111-00010T4LF
2. PKoB4 Reset Header: 1x2 100 mil pitch
   - Manufacturer: Samtec Inc.
   - Part Number: TSW-102-07-G-S
3. Jumper Cap: 100 mil pitch
   - Manufacturer: FCI
   - Part Number: 63429-202LF
4. In-Circuit Debuggers:
   - Preferred: PICkit™ 5 or PICkit 4
   - Alternative: ICD 5 Debugger/Programmer
5. Adpater Kit: AC102015 ICD / PICkit Adapter Kit

NOTICE For items 1, 2 and 3, the ordering information provided serves as an example of devices that may be utilized. Alternative options are available.

External Debugger Connections to the SG41

1. Populate J400, the 10-pin Cortex header.

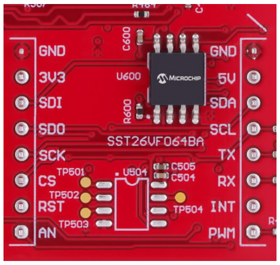
Restriction: This header needs to be an unshrouded connector due to limited space on the board.

2. Populate J300, the PKoB4 Reset header. Ensure that the PKoB4 is in Reset mode to enable programming via the debugger.
3. Place a jumper cap on the J300 header.
4. Attach the PICKit debugger tool to the Cortex header, ensuring alignment with the pin 1 indicator.
5. Connect the adapter kit to the USB debugger tool.
6. Connect the adapter board to the EV89U05A using the 2x5 50 mil pitch cable.
7. Connect the USB cable to the EV89U05A to supply power to the board.
8. Attach a micro USB cable to the debugger.
9. Launch either MPLAB® X IDE or MPLAB X IPE to program the board.

1.3.2. Additional On-Board Crypto Device

An optional SOIC footprint is located on the backside of the board, allowing for the installation of an additional CryptoAuthentication™ or CryptoAutomotive™ device. This footprint can be utilized to support the development of specialized applications, integrate newer secure elements or implement customer-specific provisioned versions.

Figure 1-4. Optional SOIC-8 Footprint



Supported Devices

The following devices can be soldered onto the board: ATSHA204A, ATECC608x (all versions), TA10x, ECC204, SHA104, SHA105 and TA010. Although other legacy devices may be compatible, only devices recommended for new designs are listed here.

Requirements:

- The device must be in an 8-pin SOIC package.
- The device must use the I^{2}C Interface (SWI and SPI are not supported).
- The device must have an I^{2}C address unique from the four ATECC608C devices also mounted on the board.

Tip: For devices that support additional signals or GPIOs, these are accessible via test pads TP501 through TP504. Users have the flexibility to determine how these signals are connected to the board.

Related Links

Crypto Devices

mikroBUS and Click Add-On Boards

1.3.3. Additional GPIOs

Optional GPIOs of the PIC32CX1025SG41 microcontroller that have not been used elsewhere in the design have been brought out to an 8-pin, 50 mil pitch header (J401). This header is unpopulated but can be mounted by the user. The available signals can be used as GPIOs, interrupt signals, analog inputs, peripheral touch control (PTC) inputs, or timing control. The following details list the possible usage option for each of the signals. See the PIC32CX1025SG41 data sheet for more detailed information.

Connector: 1x8 50 mil pitch **Manufacturer:** Sullins **Part #:** LPPB081NFFN-RC

Table 1-9. J401 Signal Connections

Connector Pin #	Pin Number	Pin Name	Usage Options
1	96	PB31	GPIO, EXTINT[15], Timing Control
2	97	PB00	GPIO, EXTINT[0],ADC0-AIN[12], PTC-X30/Y30, Timing Control
3	100	PB03	GPIO, EXTINT[3],ADC0-AIN[15], PTC-X21/Y21, Timing Control
4	6	PC03	GPIO, EXTINT[3],ADC1-AIN[5]
5	9	PB04	GPIO, EXTINT[4],ADC1-AIN[6], PTC- X22/Y22
6	10	PB05	GPIO, EXTINT[5], ADC1-AIN[7], PTC X23,Y23
7	14	PB07	GPIO, EXTINT[7], ADC1-AIN[9], PTC X23,Y23
8	23	PC07	GPIO, EXTINT[9]

1.4. Hardware Documentation

Additional documentation for the kit can be found on the Microchip website for the EV89U05A.

This includes:

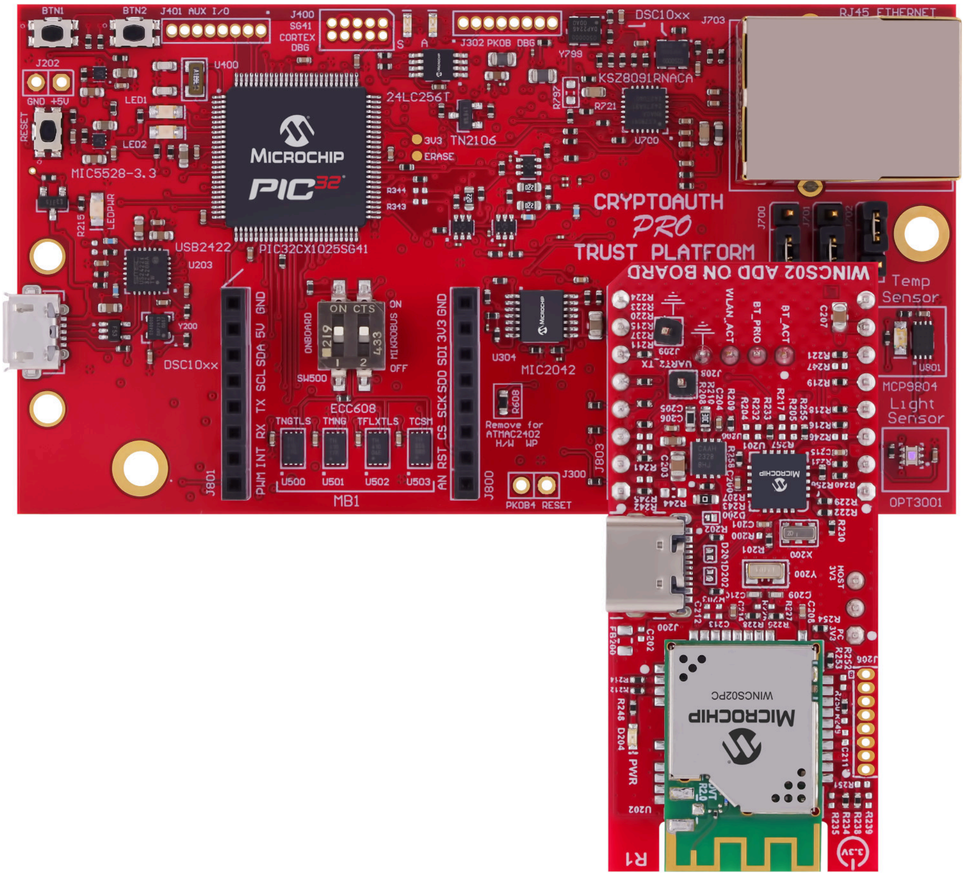
1. Board Design Documentation, including Schematics and 3D Views
2. Gerber Files
3. CryptoAuth Pro Trust Platform User Guide (EV89U05A)
4. Trust Platform Design Suite Tools

2. WINCS02 mikroBUS™ board

To connect to WiFi with the EV89U05A kit, it is recommended to integrate the Microchip WINCS02 mikroBUS™ compatible board with the CryptoAuth Pro Trust Platform. The WINCS02 board contains the Microchip WINCS02PC module, which supports IEEE® 802.11 b/g/n protocols. The board connects to the CryptoAuth Pro Trust Platform board via the mikroBUS extension headers and communicates with the microcontroller through the SPI interface. It is recommended that the MB2 extension header be used for the WINCS02 connection; however, the MB1 header can be used if necessary. Microchip's examples are designed to utilize the MB2 extension header. The WINCS02 can be reset via the reset signal on the mikroBUS board, which is connected to the host microcontroller. Additionally, the WINCS02 supports an interrupt signal connected to the microcontroller.

Specific TPDS use cases have been developed to support the development of applications operating with the Kudelski SaaS IoT infrastructure and tools. Power for the WINCS02 board is supplied through the mikroBUS extension header MB2, and the power to the overall system only requires the USB power connector. A view of the CryptoAuth Pro Trust Platform board with the WINCS02 mikroBUS board connected to MB2 is shown below.

Figure 2-1. CryptoAuth Pro Trust Platform + WINCS02 mikroBUS™ Board



WINCS02 Information

- **Board Name:** WINCS02 Add-On Board
- **Ordering Code:** EV68G27A

- **Availability:** The EV68G27A is available on Microchip Direct
- **WINCS02 Resources:**
  - WINCS02 Add-on-Board Website
  - WINCS02IC and WINCS02 Module Data Sheet
  - WINCS02 Application Developer’s Guide

3. mikroBUS™ and Click Add-On Boards

The mikroBUS™ connector has emerged as a de facto industry-standard add-on board form factor. The CryptoAuth Pro Trust Platform board has a single mikroBUS host connector. Having this capability dramatically expands the usefulness of this board for developing and prototyping new applications. The following tables list boards developed by Microchip Technology or MikroElektronika with support from Microchip Technology.

Table 3-1. Microchip mikroBUS™ Add-On Boards

Board Name	Devices Supported	Description
ATECC608_TRUST DT100104[1]	ATECC608C-TNGTLS ATECC608C-TFLXTLS ATECC608C-MAHDA ECC608-TMNGTLS	The ECC608-TMNGTLS Trust board provides additional sample units for development work. Designed as an alternative to socketed boards, this board allows for individual device selection using the on-board DIP switches.
TA010 CRYPTOAUTO EV74C12A	TA010-MAHDA	The TA010 CryptoAuto board supports TA010 devices with I^2C and SWI interfaces, as well as TA100 Host devices.
ECC204 CRYPTOAUTH EV92R58A	ECC204	The ECC204 CryptoAuto board supports ECC204 devices with I^2C and SWI interfaces, as well as TA100 Host devices.
VQFN-24 EV39Y17A	TA100 and TA101	The VQFN-24 Socket board supports both I^2C and SPI interfaces, as well as all GPIOs.
SOIC-08 AC164167	TA100 and TA101	The TA100-08 is an 8-pin SOIC socketed solution designed for configuring and provisioning CryptoAuto devices. These devices can be mounted on early prototype or production boards.
Contact 3 EV27Y72A	RBH parts	The 3-Lead Contact board is a 3-Lead RBH socketed solution designed for configuring and provisioning CryptoAuth devices. These devices can be mounted on early prototype or production boards.
VSFN socket EV98D91A	SHA106, ECC206	The uVSFN 2-Lead Contact board is a socketed solution specifically designed for configuring and provisioning the SHA106. It allows these devices to be mounted on early prototype or production boards.
WINCS02 WiFi Module EV68G27A	WINCS02IC, ATECC608C-TNGTLS	A WiFi module designed to connect to the MB2 header of the CryptoAuth Pro Trust Platform, adding WiFi capability to this development board.

Note:

1. Previous versions of the board used ATECC608A/B devices and did not support the ECC608-TMNGTLS.

Table 3-2. MikroElektronika Click Add-On Boards

Board Name	Devices Supported	Description
WiFi 7 Click	ATWINC1510	WiFi module that utilizes the ATWINC510. The board supports IEEE® 802.11 b/g/n protocols and communicates over the SPI interface.
Secure 4 Click[1]	ATECC608A	Features a generic ATECC608A secure element with an I^2C interface. This device is an earlier version of the ATECC608B/C TrustCustom devices.
Secure Click[1]	ATECC508A	Includes a generic ATECC508A secure element with an I^2C interface.
Secure 3 Click	ATSHA204A	Contains a generic ATSHA204A secure element with an I^2C interface. The device has a cryptographic coprocessor with symmetric secure hardware-based key storage.
Secure 6 Click	ATSHA204A	Offers a generic ATSHA204A secure element with a SWI interface. The device has a cryptographic coprocessor with symmetric secure hardware-based key storage.
Secure UDFN Click	All Microchip CryptoAuthentication™ devices	An 8-pin UDFN socketed solution designed for configuring and provisioning CryptoAuth devices. It can be used for mounting on early prototype or production boards.

Table 3-2. MikroElektronika Click Add-On Boards (continued)

Board Name	Devices Supported	Description
Secure SOIC Click	All Microchip CryptoAuthentication devices	An 8-pin SOIC socketed solution designed for configuring and provisioning CryptoAuth devices. It can be used for mounting on early prototype or production boards.
mikroBUS Shuttle[(2)]	Click expansion boards	A compact add-on board designed to expand the mikroBUS to accommodate multiple mikroBUS connectors.
Shuttle Click[(2)]	Click expansion boards	A socket expansion board that provides an elegant solution for stacking up to four Click boards.

Notes:

1. Not recommended for new designs.
2. Generic boards developed by MikroElektronika that can expand the number of mikroBUS extension boards.

4. Software Requirements

The CryptoAuth Pro Trust Platform can be used in a variety of ways, including:

1. As a development tool in conjunction with Microchip's Trust Platform Design Suite of use case tools.
2. As a development and demonstration platform for Microchip predefined applications.
3. As a development platform for custom applications using Microchip's Python®-based tools or C-based tools.

A range of software tools is available to support work with the CryptoAuth Pro Trust Platform.

4.1. Software Application Development

The following tools are useful for developing or modifying applications.

Trust Platform Design Suite

The Microchip Trust Platform Design Suite of use case tools is based on Jupyter Notebooks and Python programs, allowing developers to quickly define and develop applications for the Trust Platform products.

The Microchip Trust Platform Design Suite provides the ability to interoperate with the on-board CryptoAuthentication™ devices or CryptoAuthentication devices attached through the mikroBUS™ header. The tool provides an easy way to select from available device options and generate the required configuration files needed for provisioning. Additionally, the tool can be used to develop applications utilizing the CryptoAuth Pro Trust Platform.

MPLAB® X IDE

MPLAB X is an Integrated Development Environment (IDE) that works on Windows®, macOS® and Linux® environments. The tools can be used to develop new embedded applications using the on-board PIC32CX1025SG41 microcontroller. The tool will automatically make use of the on-board PKoB4 debugger to program the PIC32CX1025SG41 microcontroller. The debugger can also be used to provide debug information back from the host microcontroller to a terminal window through a COM port.

CryptoAuthLib

CryptoAuthLib was developed to simplify the use of Microchip's CryptoAuthentication devices. It features a Hardware Abstraction Layer (HAL) to facilitate easy extension to other microcontrollers. Both C and Python versions of the library are available. The Python version of the library is maintained by Microchip and is available through the PythonPackage Index website (pypi.org). The most recent version of CryptoAuthLib is available on Microchip's GitHub site.

- CryptoAuthLib – Python
- CryptoAuthLib – GitHub

4.2. Firmware Upgrade

New firmware for the CryptoAuth Pro Trust Platform may be available periodically, offering new features or enhancements. In addition, specific applications developed by Microchip may be made available for use with this development board. The latest version of the firmware and information about other applications can be found on the EV89U05A product page.

The MPLAB® X IPE (Integrated Programming Environment) can be used to upgrade the firmware of the CryptoAuth Pro Trust Platform development kit. The firmware of the PIC32CX1025SG41 will be upgraded through the PKoB4 on-board debugger.

NOTICE Upgrading to the latest version of the tools is recommended. Older versions may not recognize the PKoB4 debugger or newer kits released after the manufacture of these boards.

5. Document Revision History

Revision A (May 2025)

- Initial release of this user guide.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

ISBN: 979-8-3371-1245-9

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Product Page Links

24LC256, AT24MAC402, ATECC608C, ATECC608C-TFLXTLS, ATECC608C-TNGTLS, ATSAME70N21, DSC1001, DSC6000B, ECC608-TMNGTLS, KSZ8091, MCP1727, MCP9804, MIC2042, MIC5528, PIC32CX1025SG41100, SST26VF064BA, TN2106, USB2422, VMK3