DM320118

CryptoAuth Trust Platform User's Guide

Introduction

The Microchip CryptoAuth Trust Platform is the newest addition to the CryptoAuthentication™ evaluation kits. This kit is used for exploring and developing solutions for the IoT space with a pre-provisioned ATECC608A Trust&GO, pre-configured TrustFLEX and fully customizable TrustCUSTOM products.

The Trust&GO and TrustFLEX products have been developed to allow for an easy way to add hardware security to IoT Cloud solutions. Using the kit with the Microchip development tools and provisioning systems allows for customers with low volume projects to easily and readily implement secure authentication into their application.

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

Figure 1. CryptoAuth Trust Platform

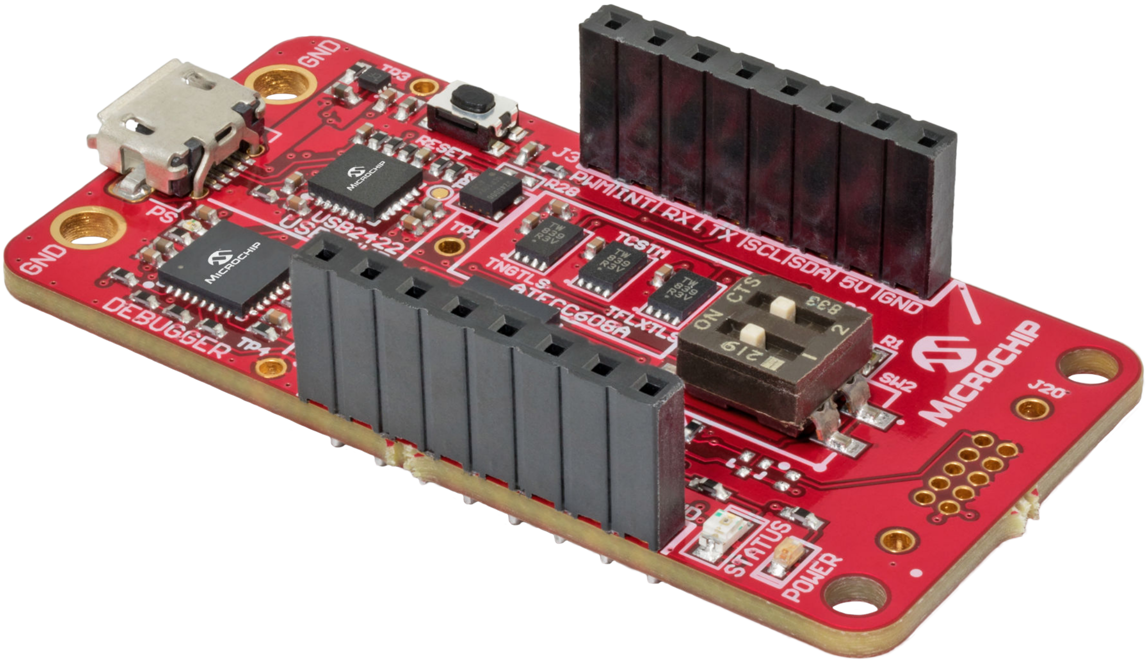


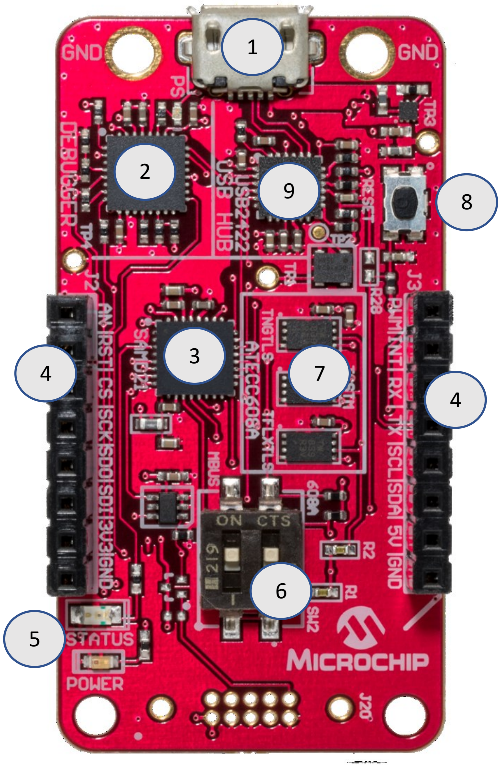
Table of Contents

1. Hardware Overview

The CryptoAuth Trust Platform consists of a Microchip SAM D21 microcontroller configured as the main MCU. It comes pre-programmed with Microchip`s Secure Products Group (SPG) kit protocol. This protocol facilitates the communication between the CryptoAuthentication devices and the host MCU over the USB HID interface. The data transfer between the secure elements and the host MCU is indicated by the Status LED.

The trust platform consists of three secure elements: ATECC608A-TNGTLS (Trust&GO), ATECC608A-TFLXTLS Prototype (TrustFLEX) and ATECC608A-MAHDA (TrustCUSTOM). Each of the secure elements has a different I^2C address that enables its communication with the host MCU, which eliminates the line contention issue.

Figure 1-1. CryptoAuth Trust Platform Board Components



1. USB Connector
2. nEDBG On-board Debugger
3. ATSAMD21E18A Host MCU
4. mikroBUS™ Headers
5. Power and Status LEDs
6. Dual SPST DIP Switch
7. ATECC608A Secure Elements
8. Reset Switch
9. USB2422 Dual Port Hub

1.1 Kit Ordering Code and Components

Ordering Information
Kit Name: CryptoAuth Trust Platform Development Kit

Ordering Code: DM320118

Availability: The kit will be available from Microchip Direct and multiple distributors.

CryptoAuth Trust Platform Kit Contents and Requirements
The CryptoAuth Trust Platform Kit contains:

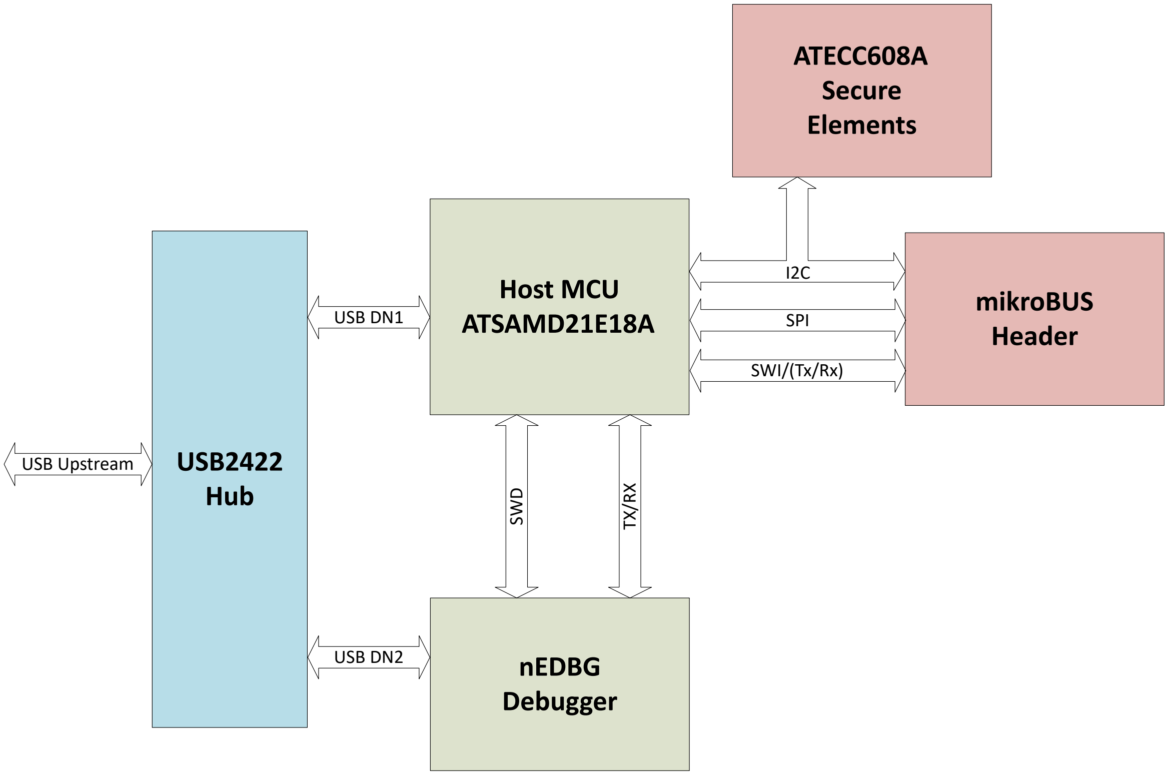
- CryptoAuth Trust Platform board

A micro USB cable (not included) is required to operate the board.

1.2 Functional Description

The block diagram in Figure 1-2 illustrates the major connections of the CryptoAuth Trust Platform. For additional details refer to the board schematics referenced in section 1.3 Hardware Documentation of the document.

Figure 1-2. Block Diagram



Main Board Components

- **ATSAMD21:** The Microchip SAM D21 is an ARM® Cortex M0+ based microcontroller. The MCU connects to the three secure elements via I^{2}C. The mikroBUS header has I^{2}C, SPI, UART, GPIO and analog connections to the microcontroller. This enables the possibility of using the CryptoAuth Trust Platform with many types of MikroElektronika Click boards™.
- **Secure Elements:** The Trust Platform consists of three ATECC608A-based ICs, as listed in the following table. Please refer to the specific data sheets associated with each of these devices for more details.

Device	Default 7-bit I^{2}C Address	8-bit Programmed I^{2}C Address Value[(1)]
ATECC608A-TNGTLS	0x35	0x6A
ATECC608A-TFLXTLS	0x36	0x6C
ATECC608A-MAHDA	0x60	0xC0

Note:

1. This is the I2C_Address byte value programmed into the ATECC608A device.

- **mikroBUS Header:** The mikroBUS header is a pre-defined header connection for all the MikroElektronika boards. This lets the user connect many types of Click sensors and add-on boards to the Trust Platform. The Trust Platform has SPI, I^{2}C, UART and GPIO and analog connections to the host microcontroller.
- **DIP Switch:** The switch is used to select between the on-board ATECC608A Trust Platform devices and the mikroBUS header. The switches disconnect the SDA lines of the I^{2}C interface to prevent conflict in case two I^{2}C addresses are the same. Both switches can be enabled if all I^{2}C addresses are unique on all devices connected to the board.

Switch Settings		What is Enabled	
SW2_1	SW2_2	mikroBUS Header	On-Board Devices
ON	ON	Yes	Yes
OFF	ON	No	Yes
ON	OFF	Yes	No
OFF	OFF	No	No

- **nEDBG Debugger:** The debugger is used to program and flash the host MCU. Debug information can also be read back from the host MCU through the debugger interface. When plugged into the system and opened with MPLAB X IDE, the nEDBG debugger will show up with a serial number of MCHP3311xxxxxxxxxxxxxxx.
- **USB Hub:** The Microchip USB2422 is a dual-port USB hub. The hub will pass data between the upstream port and the downstream devices. The downstream devices are the debugger and the host MCU.

1.3 Hardware Documentation

Additional documentation for the kit can be found on the Microchip Website for the DM320118.

This includes:

1. Board Design Documentation including Schematics and 3D Views
2. Gerber Files
3. CryptoAuth Trust Platform User's Guide (DM320118)
4. Trust Platform Design Suite Tools

2. mikroBUS™ and Click Add-On Boards

The mikroBUS connector is emerging as a de facto industry-standard add-on board form factor. The CryptoAuth 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. All of the boards listed in Table 2-1 have been developed by MikroElektronika, except as noted.

Table 2-1. mikroBUS Add-on Boards

Board Name	Devices Supported	Manufacturer	Description
ATECC608A DT100104[1]	ATECC608A-TNGTLS ATECC608A-TFLXTLS ATECC608A-MAHDA	Microchip	The ATECC608A Trust board provides additional sample units for doing development work. This board was developed as an alternative to using socketed boards. Each of the devices can be individually selected using the on-board DIP switches.
Secure UDFN click	All Microchip CryptoAuthentication devices	MikroElektronika	The secure UDFN Click board™ has been developed as an 8-pin UDFN socketed solution for configuring and provisioning CryptoAuthentication™ devices. These devices may be used to mount to early prototype or production boards.
Secure SOIC click	All Microchip CryptoAuthentication devices	MikroElektronika	The secure SOIC click board has been developed as an 8-pin SOIC socketed solution for configuring and provisioning CryptoAuthentication devices. These devices may be used to mount to early prototype or production boards.
WiFi 7 click	ATWINC1510	MikroElektronika	WiFi module utilizing the ATWINC510. The board supports IEEE® 802.11 b/g/n protocols and communicates over the SPI interface.
Secure 4 click	ATECC608A	MikroElektronika	Has a generic ATECC608A secure element with an I^{2}C interface. This device is the same as the ATECC608A TrustCustom device that is mounted on the CryptoAuth Trust Platform board.
Secure click	ATECC508A	MikroElektronika	Has a generic ATECC508A secure element with an I^{2}C interface.
Secure 3 click	ATSHA204A	MikroElektronika	Has a generic ATSHA204A secure element with an I^{2}C interface. The device has a cryptographic coprocessor with symmetric secure hardware-based key storage.
Secure 6 click	ATSHA204A	MikroElektronika	Has a generic ATSHA204A secure element with a SWI interface. The device has a cryptographic coprocessor with symmetric secure hardware based key storage.
Secure 2 Click	ATAES132A	MikroElektronika	Has a generic ATAES132A secure element with an I^{2}C Interface. The ATAES132A is a 32K serial EEPROM that can be configured as a secure memory device.
mikroBUS Shuttle	Click expansion boards	MikroElektronika	The mikroBUS Shuttle is a small add-on board that can be used to expand the mikroBUS to multiple mikroBUS connectors.

...........continued

Board Name	Devices Supported	Manufacturer	Description
Shuttle Click	Click expansion boards	MikroElektronika	The Shuttle Click is a socket expansion board that provides an elegant solution for stacking up to four Click boards.

Note:

1. Manufactured by Microchip.

3. Software Requirements

The CryptoAuth Trust Platform can be used in a variety of ways. These include:

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 to develop your own applications using Microchip's Python-based tools or C-based tools.

Various software tools are available to work with the CryptoAuth Trust Platform.

3.1 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 are based on Jupyter Notebooks and Python programs to allow a developer to quickly define and develop applications for the Trust Platform products.

The Microchip Trust Platform Design Suite provides the ability to inter-operate with the on-board ATECC608A 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. The tool can also be used to develop applications utilizing the CryptoAuth 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 onboard SAM D21 microcontroller. The tool will automatically make use of the onboard nEDBG debugger to program the SAM D21 microcontroller. The debugger can also be used to provide debug information back from the host microcontroller to a terminal window through a COM port.

Atmel Studio 7

Atmel Studio 7 is an Integrated Development Environment (IDE) that works on Windows® environments. The tools can be used to develop new embedded applications using the onboard SAM D21 microcontroller. The tool will automatically make use of the onboard nEDBG debugger to program the SAM D21 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 make working with Microchip's CryptoAuthentication devices a simple and straightforward process. CryptoAuthLib has been designed with a Hardware Abstraction Layer (HAL) to make it easily extensible to other microcontrollers. Both C and Python versions of the library are available. The Python version of the library is maintained by Microchip and available through the PythonPackage Index website (pypi.org). The most recent version of CryptoAuthLib can be found on Microchip's GitHub site.

- CryptoAuthLib - Python
- CryptoAuthLib - GitHub

3.2 Firmware Upgrade

New firmware for the CryptoAuth Trust Platform may be available periodically with 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 will be found on the DM320118 product page.

Two Microchip tools exist for upgrading the firmware of the CryptoAuth Trust Platform development kit. Firmware upgrades are done in the standard way using both tools and are not described in more detail here. Both of these options utilized the nEDBG on-board debugger. These options are:

- MPLAB X IPE (Integrated Programming Environment) – This tool is provided as part of the MPLAB X IDE download.
- Atmel Studio 7 – Integrated Design Environment.

Notice: Upgrading to the latest version of the tools is recommended. Older versions of the tool may not recognize the nEDBG debugger or the specific kit information.

4. Document Revision History

Revision A (September 2019)

- Initial release of this User’s Guide.

The Microchip Website

Microchip provides online support via our website at http://www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to http://www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

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

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with

Trademarks

ISBN: 978-1-5224-5086-3

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit http://www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
http://www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Australia - Sydney
Tel: 61-2-9868-6733

China - Beijing
Tel: 86-10-8569-7000

China - Chengdu
Tel: 86-28-8665-5511

China - Chongqing
Tel: 86-23-8980-9588

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115

China - Hong Kong SAR
Tel: 852-2943-5100

China - Nanjing
Tel: 86-25-8473-2460

China - Qingdao
Tel: 86-532-8502-7355

China - Shanghai
Tel: 86-21-3326-8000

China - Shenyang
Tel: 86-24-2334-2829

China - Shenzhen
Tel: 86-755-8864-2200

China - Suzhou
Tel: 86-186-6233-1526

China - Wuhan
Tel: 86-27-5980-5300

China - Xian
Tel: 86-29-8833-7252

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444

India - New Delhi
Tel: 91-11-4160-8631

India - Pune
Tel: 91-20-4121-0141

Japan - Osaka
Tel: 81-6-6152-7160

Japan - Tokyo
Tel: 81-3-6880- 3770

Korea - Daegu
Tel: 82-53-744-4301

Korea - Seoul
Tel: 82-2-554-7200

Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

Malaysia - Penang
Tel: 60-4-227-8870

Philippines - Manila
Tel: 63-2-634-9065

Singapore
Tel: 65-6334-8870

Taiwan - Hsin Chu
Tel: 886-3-577-8366

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600

Thailand - Bangkok
Tel: 66-2-694-1351

Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-72400

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra'anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-72884388

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820