

# Strengthen Product Security with Microchip Trust Platform



---

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions



SMART | CONNECTED | SECURE

May 12, 2020

# Microchip Technology

---

E.H Chen – Director of Sales, Greater China

# Corporate Overview

- **Leading Total Systems Solutions provider:**
  - High-performance standard and specialized Microcontrollers, Digital Signal Controllers and Microprocessors
  - Mixed-Signal, Analog, Interface and Security solutions
  - Clock and Timing solutions
  - Wireless and Wired Connectivity solutions
  - FPGA solutions
  - Non-volatile EEPROM and Flash Memory solutions
  - Flash IP solutions
- **~ \$6 Billion revenue run rate**
- **~19,000 employees**
- **Headquartered near Phoenix in Chandler, AZ**

# Strengthen Product Security with Microchip Trust Platform

---

Roy Yen – Senior Embedded Solutions Engineer



# Security is essential for your IoT product

~~Yes — Encrypt/Decrypt is a MUST now~~

To authorize users' access

But how?

To secure communication data

To safely store secret keys

To prevent hacker cloning

# Authentication Seems to be the Basic Skill

How? Password is the answer

**How do we confirm someone during online shopping?**

**Key in the credit card number?**

**Key in the 3-digit security code?**

**How do we confirm someone while logging in ipcam?**

**Key in your ID/Password?**

# Once the Password is Stolen...

---

Well-known in-house smart camera hacked (December 2019)

# Relying on Password Alone is Not Secure Enough

Why could our passwords be stolen?



***Asymmetric security cipher is the key...***



# Second Authentication

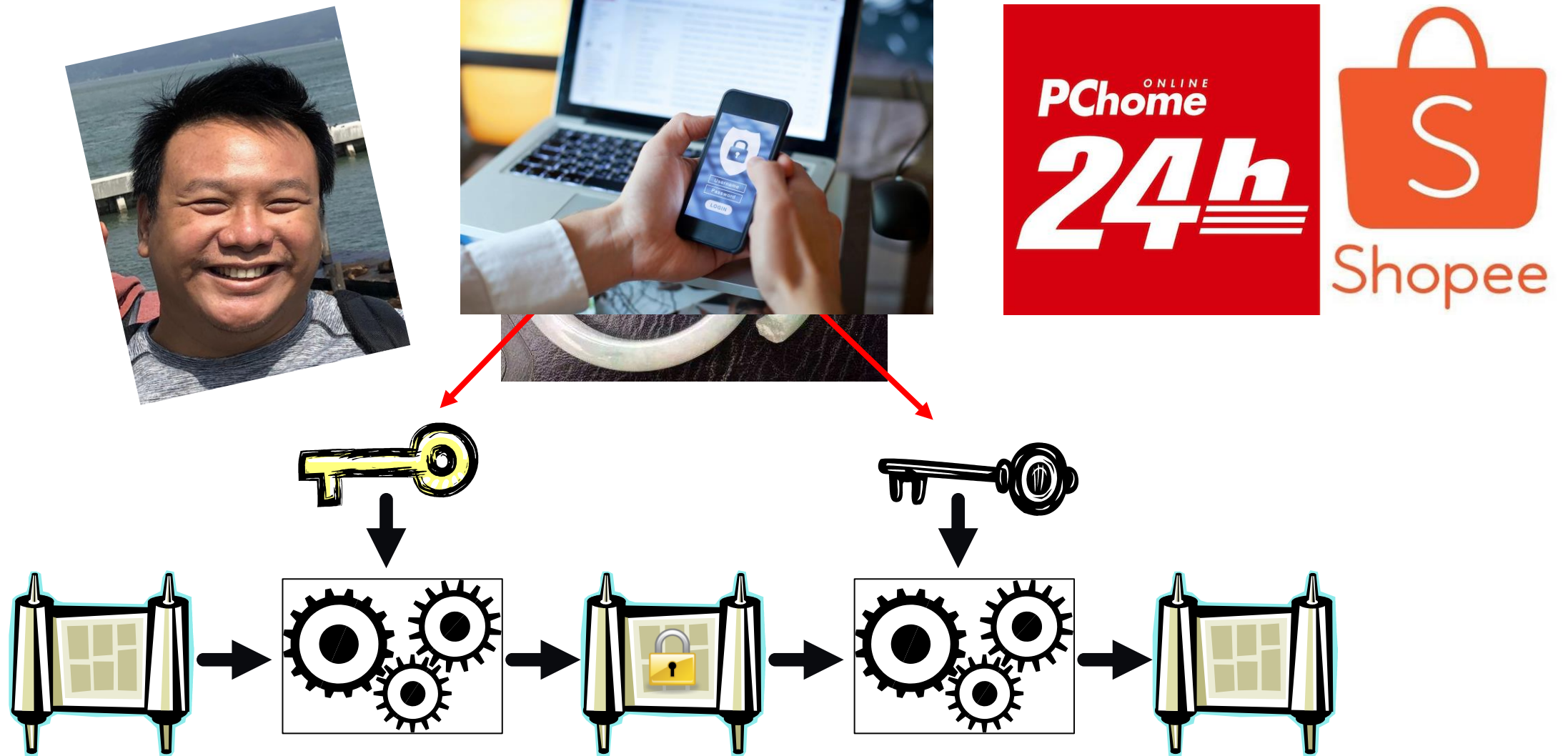
- **Many companies use second authentication**
  - Sending confirmation number through **phone message**
  - Sending confirmation number through **personal email**
  - **Face ID** recognition
  - **Fingerprint** recognition
- **They believe phone, email and face/fingerprint access only belongs to you**



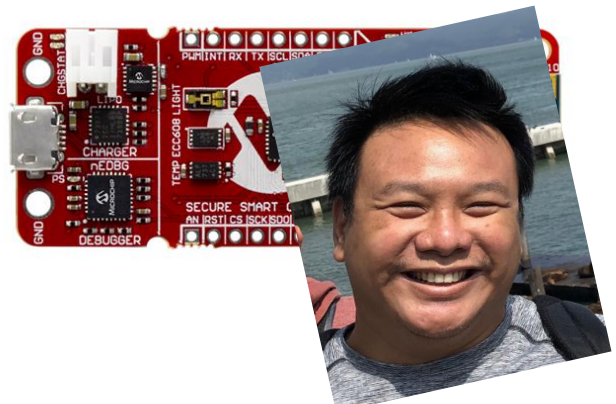
***No one can steal your data***

***Pub/Private Key System is also the solution***

# Private Key Only Belongs to Someone



# Private Key Only Belongs to Someone

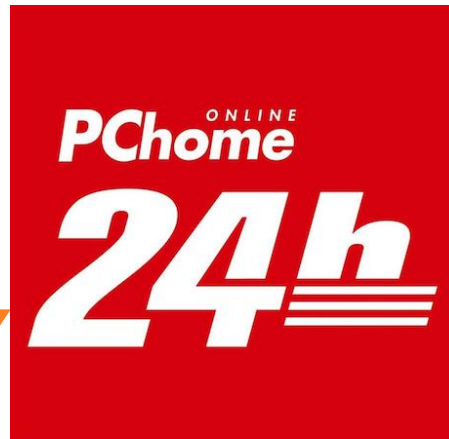


I want to buy a NB

Name?

I am Roy

Ok, please encrypt "5d96W3ceP8eH" by Roy's Private key



Here you are "85qg96Hw32P1A9" Please confirm

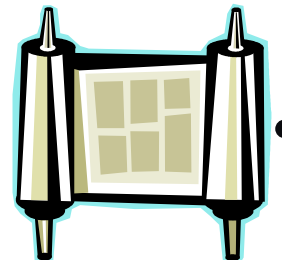
Prepare Roy's Public key

Ok, let me check

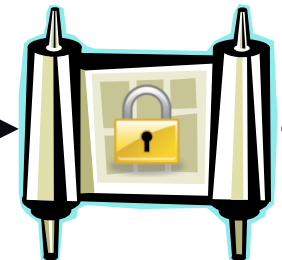
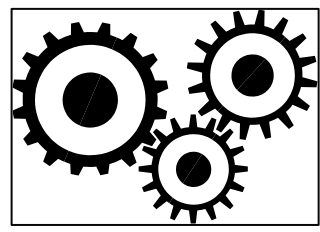
*Kept secured*

*Random Number*

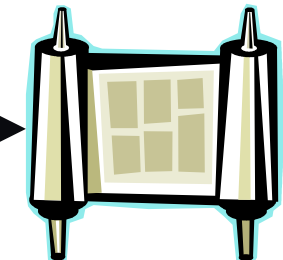
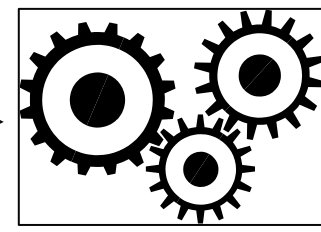
*Everyone can use the same pub key*



5d96W3ceP8eH

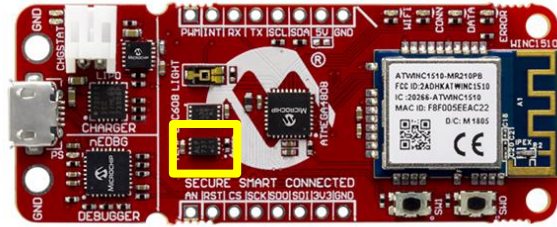


85qg96Hw32P1A9



5d96W3ceP8eH

# Private Key Only Belongs to Some Devices



I want to log in

ID?

I am A9632

Ok, please encrypt  
"5d96W3ceP8eH" by  
A9632's Private key



*Kept secured*

Here you are  
"85qg96Hw32P1A9"  
Please confirm

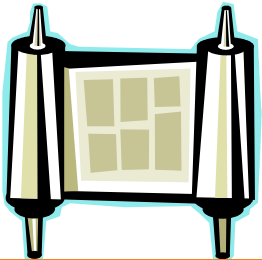
*Random Number*

Prepare A9632's  
Public key

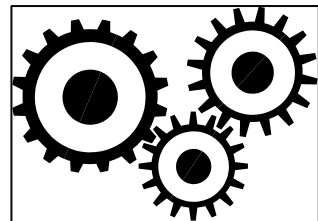
Ok, let me check



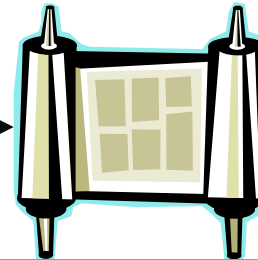
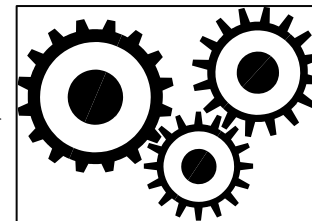
*Everyone can  
Use the same pub key*



5d96W3ceP8eH

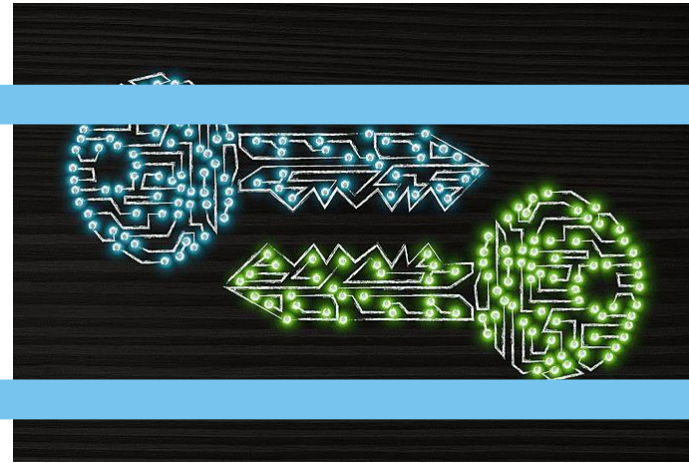
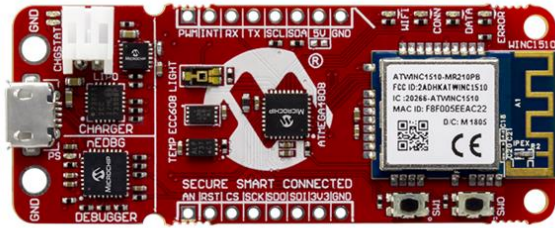


85qg96Hw32P1A9



5d96W3ceP8eH

# Private Key Only Belongs to Some Devices



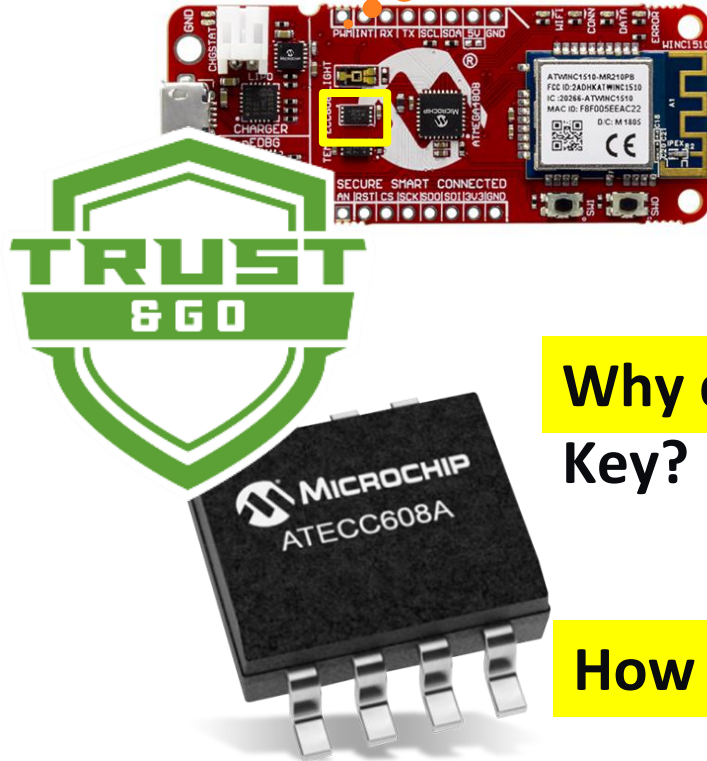
# Summary

- Security is important, but Encrypt/Decrypt is not enough
- Authentication is essential for user/device log in
- Symmetric password is an easy way to do authentication though risky
- Only use data which users have access to
  - Phone, email, face ID and fingerprint recognition
- **Asymmetric secret key (Pub/Private key pair) is a good method**
  - Generated randomly, no repeat
  - The one who own Public Key is the “Door Keeper”
  - The one who own Private Key is the “User”



# Private Key Only Belongs to Some Devices

A9632's  
Private key



Why does locker/AWS have A9632's Public Key?

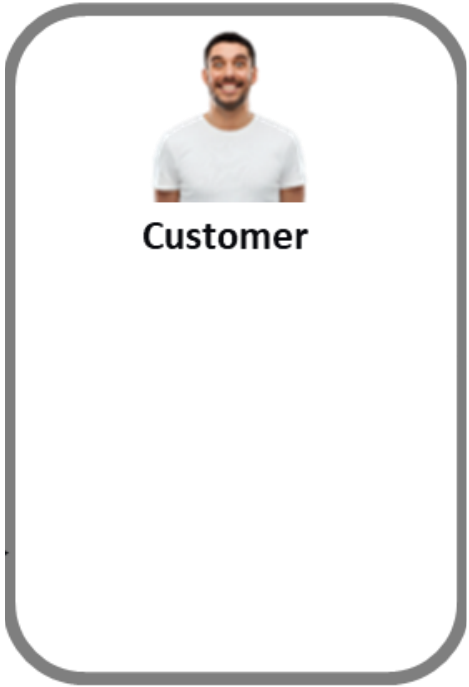
We should upload it first

How do we upload it? 1 by 1? When?

A9632's  
Public key

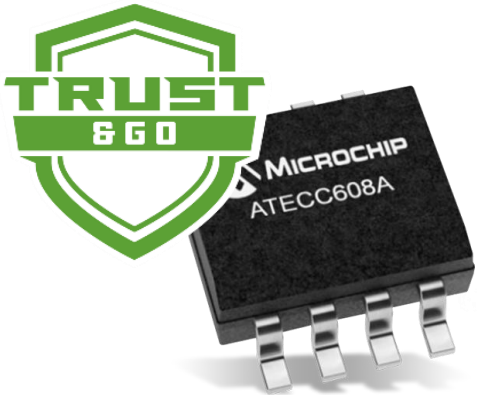
Microchip Trust&GO can collect all public keys in 1 file

# Trust&GO: Simple Ordering Process



Any cloud, any core

**How to provision keys?**



Order 10K pcs

**Private key can be pre-generated inside**



# A Scalable & Adaptable Provisioning Service

Can I still provision keys/information inside?

Private key is pre-generated inside the chip



Yes!

<b>Pre-configured</b>	YES	YES	NO
<b>Pre-provisioned</b>	YES	YES (flexible)	NO
<b>MOQ</b>	10 units	2000 units	4000 units
<b>Development time</b>	Lowest	Lower	Custom
<b>Complexity</b>	Lowest	Lower	Custom
<b>Secure key Storage</b>	JIL High	JIL High	JIL High

# Visit Microchip Trust Platform Webpage

<https://www.microchip.com/design-centers/security-ics/trust-platform>

Obtain the  
development kit

Ready to Get Started with the Trust Platform?

**Step 1:** Buy the Trust Platform hardware featuring an Arm<sup>®</sup> Cortex<sup>®</sup>-M0+ based **SAM D21** MCU and our **WINC1500** Wi-Fi<sup>®</sup>IoT network controller.

Buy the Development Kit

**Step 2:** As you work with the development kit, use the tutorial and code example and create the manifest file using the Trust Platform Design Suite, available for Windows<sup>®</sup> and macOS<sup>®</sup> operating systems.

Install Trust Platform Design Suite

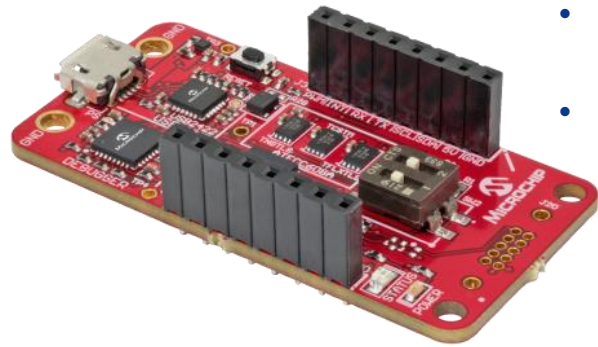
**Step 3:** Once the C code for the secure element is working in your embedded application, you are ready to go to production. Order the pre-provisioned devices and download the manifest file from our online store or from our distribution partners. Upload the list of public credentials in the corresponding cloud account.

Order Devices

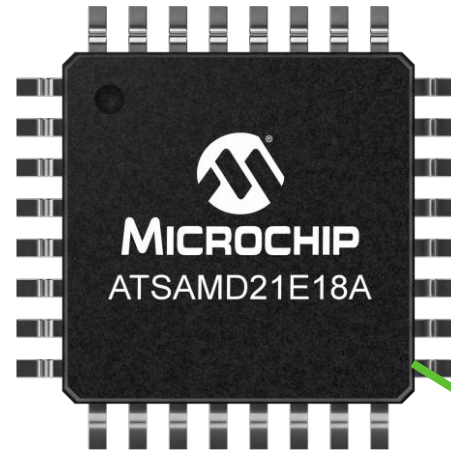
# Hardware Development Tools

## DM320118

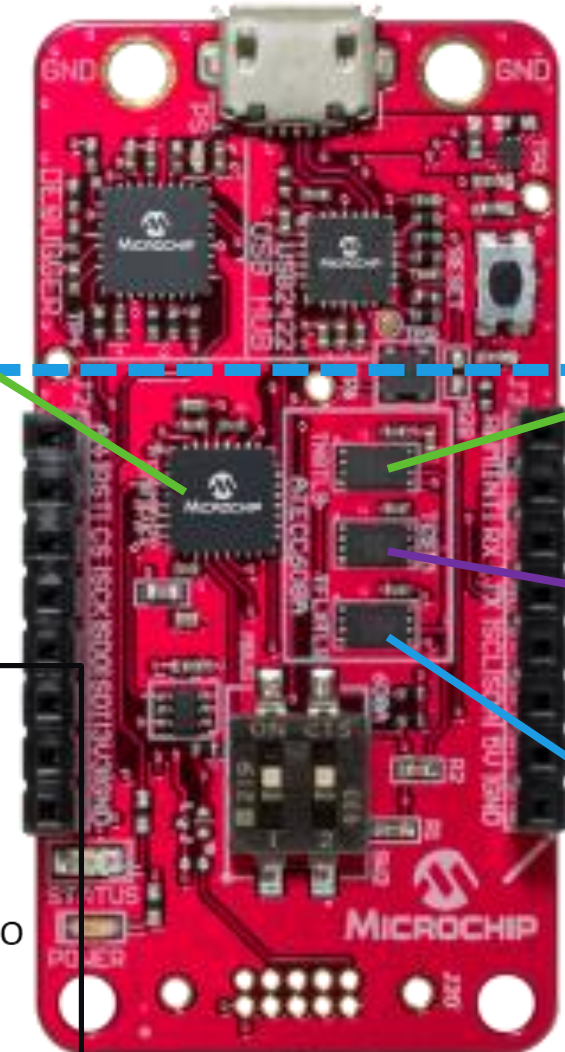
Trust Platform USB Kit



- Direct prototyping
- PC Host via USB (with Python Jupyter Notebook tutorials)
- Or onboard SAMD21 with debugger

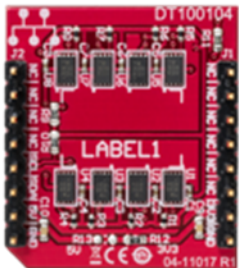


## Debug Board



## DT100104

ATECC608A Trust Platform Board



- Onboard:
  - Trust&GO,
  - TrustFLEX,
  - TrustCUSTOM
- MikroBUS male

## Mikroe.com socket



- UDFN and SOIC
- Same Functionality as XPRO Socket Boards
- MikroBUS male pinout
- Sold through Mikroe.com

# Visit Microchip Trust Platform Webpage

/security-ics/trust-platform

The screenshot shows the Microchip Developer Help website. The top navigation bar includes the Microchip logo and 'Developer Help'. A search bar is present. The left sidebar contains a navigation menu with categories like Home, Training, Development Tools, Functions, Projects, Products, Store, and Help. The 'Trust Platform Design Suite' is highlighted in the 'Functions' section. The main content area is titled 'Trust Platform Design Suite' and contains an overview, software installation instructions, and a list of requirements. A red circle highlights the 'Download the installer' link in the installation steps.

## Trust Platform Design Suite

This page provides a brief overview of the Trust Platform Design Suite for CryptoAuthentication™ along with installation and use.

The Trust Platform Design Suite is a combination of unique secure flows that enables you to easily prototype various security use cases. It's built around the ATECC608A CryptoAuthentication device sub-families: Trust&GO, TrustFLEX, and TrustCUSTOM, and an optimized secure provisioning flow.

To learn more, visit Microchip's web page Trust Platform for the CryptoAuthentication™ Family.

### Trust Platform Design Suite Overview

The Trust Platform Design Suite consists of a hardware prototyping kit, provisioning tools, example use case C-based projects, and a secret exchange package generator.

- The CryptoAuth Trust Platform hardware prototyping kit comes pre-programmed with firmware that allows the provisioning of the ATECC608 device.
- The software tools are Python-based computer programs allowing you to provision the ATECC608A device (on the CryptoAuth Trust Platform) for your specific use case. It includes:
  - Anaconda Python distribution
  - Jupyter Notebook
- The example security C-based projects allow you to use the provisioned ATECC608A devices in a working application.
- The secret exchange package generator enables Microchip to provision your ATECC608A devices for production.

### Trust Platform Design Suite Software Installation

The Trust Platform Design Suite requires one of the following operating systems:

- Microsoft Windows® 10 64-bit
- macOS® Mojave 10.14.6 or newer

It also requires one of the following Integrated Development Environments (for the C-based projects):

- MPLAB® X IDE v5.25 and XC32 C compiler v2.30 or later
- Atmel Studio 7 v7.0.2389 and Atmel Software Framework (ASF) v3.47.0

Choose your operating system from the tabs below:

Windows macOS

#### 1 Install the Trust Platform Design Suite

Google Chrome is the preferred web browser. The installer provides a simple solution that installs all the requirements to run the Trust Platform Design Suite.

- Download the installer.
- Run the Trust Platform executable file.
- Review and accept the end-user license agreement terms.
- Install for "Just Me" (not all users).
- You may need to change the install location folder. Verify the destination folder is:

The flowchart illustrates the process of getting started with the Trust Platform Design Suite. It starts with '500 Wi-Fi® IoT network' and leads to 'Buy the Development Kit'. From there, it goes to 'Install Trust Platform Design Suite', which is highlighted with a blue callout box. The next step is 'Order Devices', which leads to '500 production. Order the pre-load the list of public'. The flowchart is set against a background of a city skyline.

500 Wi-Fi® IoT network

Buy the Development Kit

Install Trust Platform Design Suite

500 production. Order the pre-load the list of public

the **design suite** and use to develop a secure application

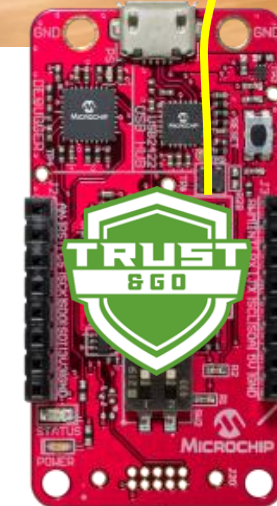
# Provide Jupyter (Python Code) to Run Trust Platform

## Easily evaluate security functions

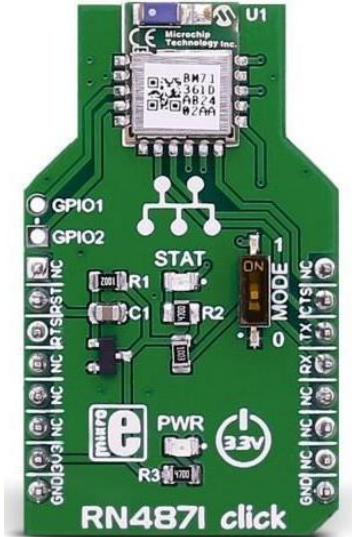
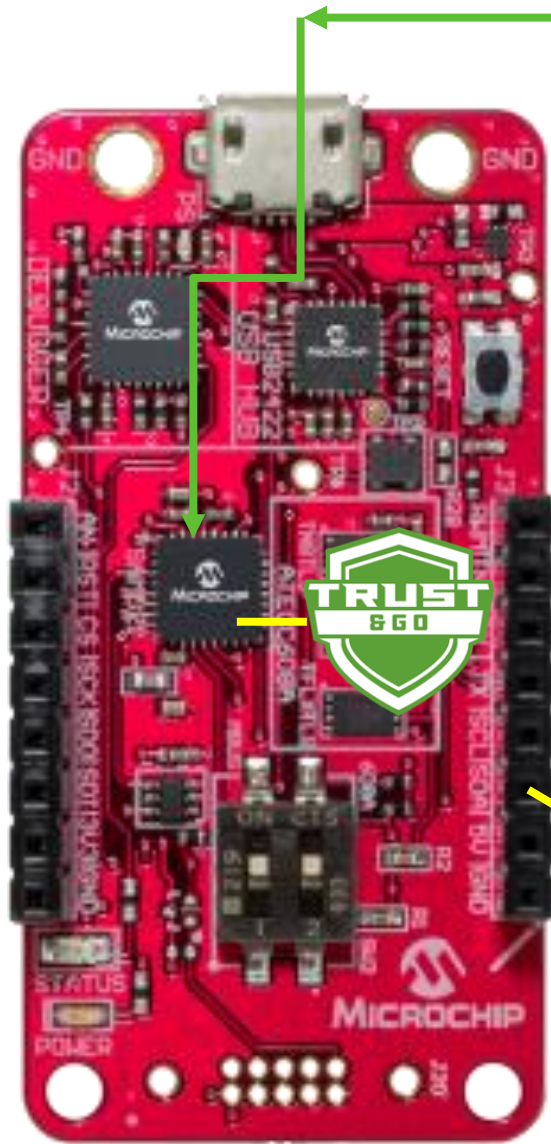
Home Page - Select or create x +  
localhost:8888/tree  
Quit Logout

Files  
Select items

Microchip Proprietary and Confidential



# Provide C-code to Start the Real Design



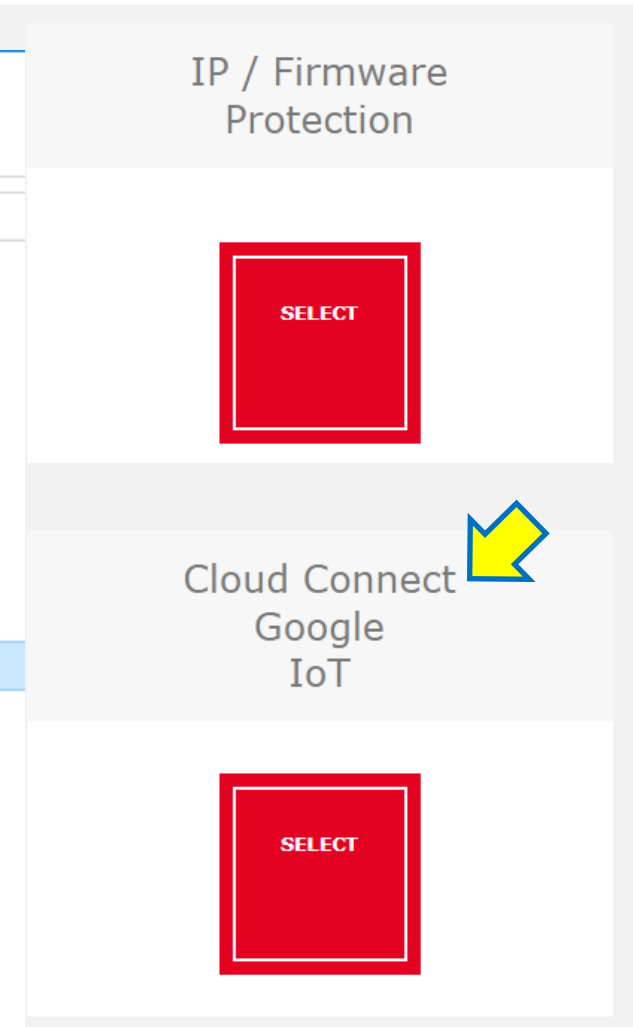
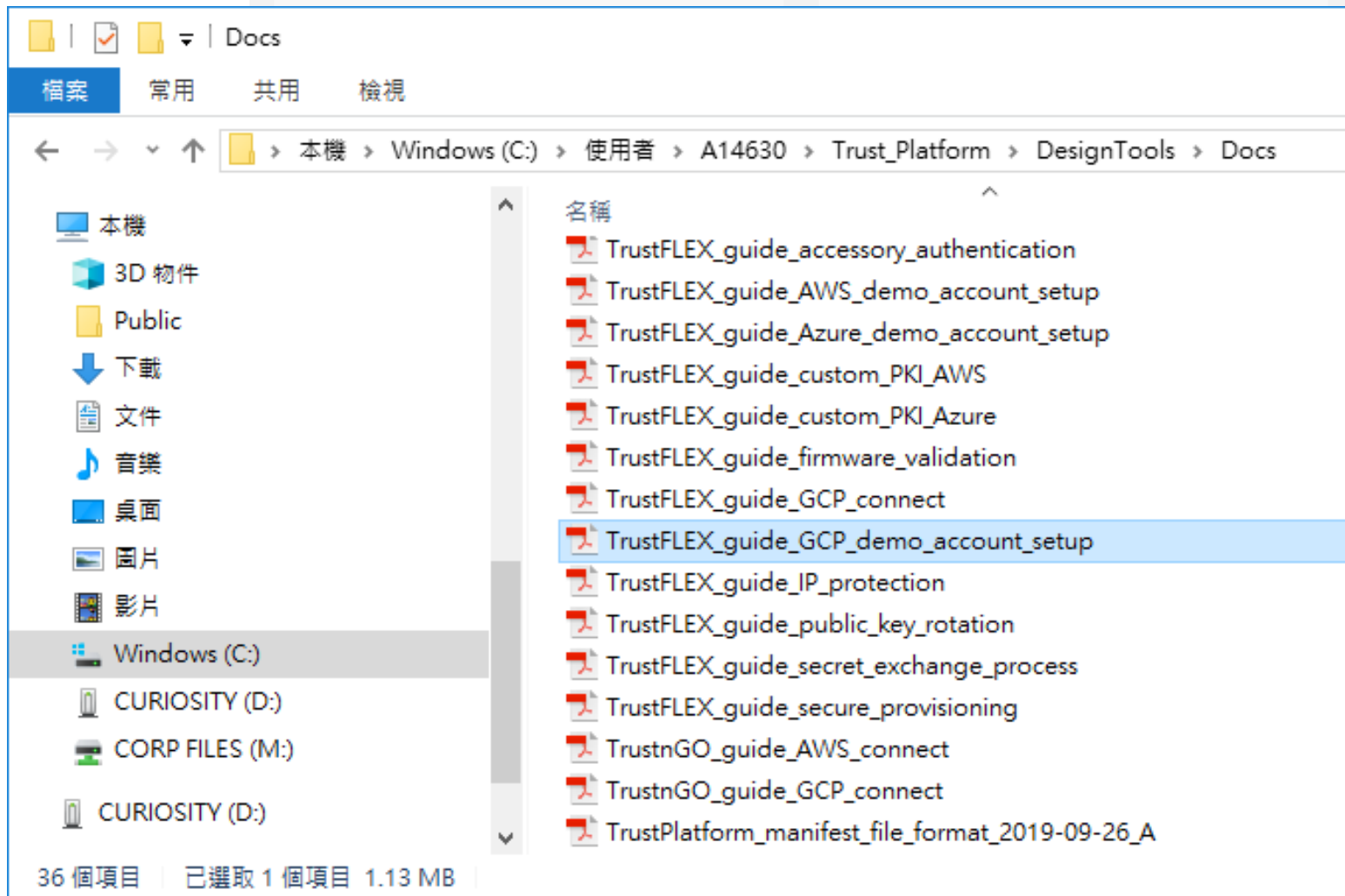
23 BT module

WiFi module



# Trust Platform Supports Many Use Cases

Find out the security use cases you want



# Connect to Google GCP with Trust&GO

## Follow the manual and Jupyter – easy instructions

Jupyter TNGTLS\_GCP\_connect (autosaved)

File Edit View Insert Cell Kernel Widgets Help

Code

```
display(gcp_gui)
print('-----')
```


Step1a. Load Manifest JSON File (1)

Step1b. Load Validation CERT File (1)

Step1c. Upload Manifest File

-----

Before clicking GCP GUI its required to have Manifest file  
ing embedded project to cloud by using host details and w  
ow GCP GUI button ONLY after establishing connection w

 GCP GUI

-----

Converting Manifest

Loading Manifest

Device registered succesfully

```
RealTerm: Serial Capture Program 2.0.0.70
SUCCESS: GCP Demo: Disconnected from WIFI access point.
WINC1500 WIFI: Disconnected from the WIFI access point.
Attempting to connect to GCP IoT ...
SSID: RoyYen
Password: 1234567890
WINC1500 WIFI: Connected to the WIFI access point.
WINC1500 WIFI: Device IP Address: 172.20.9.172
WINC1500 WIFI: DNS lookup:
Host: mqtt.googleapis.com
IP Address: 74.125.203.206
(APP)<INFO>Socket 3 session ID = 4
SUCCESS: GCP Demo: Connected to GCP IoT.
SUCCESS: Subscribed to the MQTT update topic subscription:
SUCCESS: /devices/d0123A02E502C5E8C01/config
Publishing MQTT Shadow Update Message:
00000000 7B 20 22 74 69 6D 65 73 74 61 6D 70 22 3A 20 31 < "timestamp": 1
00000010 35 37 35 33 35 39 35 32 30 2C 20 22 4C 65 64 5F 575359520, "Led_
00000020 53 74 61 74 75 73 22 3A 20 22 4F 4E 22 7D Status": "ON">
Publishing MQTT Shadow Update Message:
00000000 7B 20 22 74 69 6D 65 73 74 61 6D 70 22 3A 20 31 < "timestamp": 1
00000010 35 37 35 33 35 39 35 32 35 2C 20 22 4C 65 64 5F 575359525, "Led_
00000020 53 74 61 74 75 73 22 3A 20 22 4F 4E 22 7D Status": "OFF">
Publishing MQTT Shadow Update Message:
00000000 7B 20 22 74 69 6D 65 73 74 61 6D 70 22 3A 20 31 < "timestamp": 1
00000010 35 37 35 33 35 39 35 33 30 2C 20 22 4C 65 64 5F 575359530, "Led_
00000020 53 74 61 74 75 73 22 3A 20 22 4F 4E 22 7D Status": "ON">
Publishing MQTT Shadow Update Message:
00000000 7B 20 22 74 69 6D 65 73 74 61 6D 70 22 3A 20 31 < "timestamp": 1
00000010 35 37 35 33 35 39 35 33 35 2C 20 22 4C 65 64 5F 575359535, "Led_
00000020 53 74 61 74 75 73 22 3A 20 22 4F 4E 22 7D Status": "OFF">
```



# Connect to AWS IoT with Trust&GO

## Follow the manual and Jupyter – easy instructions

The image displays a Jupyter notebook interface on the left and a RealTerm Serial Capture Program window on the right. The Jupyter notebook is titled 'TNGTLS\_aws\_connect' and shows a series of steps for connecting to AWS IoT. The RealTerm window shows the following output:

```
Host: a2nvp3xflk12icw-ats.iot.us-west-2.amazonaws.com
IP Address: 52.43.200.75
(APP)<INFO>Socket 0 session ID = 1
SUCCESS: AWS Zero Touch Demo: Connected to AWS IoT.

SUCCESS: Subscribed to the MQTT update topic subscription:
SUCCESS: $aws/things/0123c190308ff2b601/shadow/update/delta

Publishing MQTT Shadow Update Message:
00000000 7B 22 73 74 61 74 65 22 3A 7B 22 72 65 70 6F 72 <"state":<"repor
00000010 74 65 64 22 3A 7B 22 6C 65 64 31 22 3A 22 6F 6E ted":<"led1":<"on
00000020 22 7D 7D 7D "}>>
WINC1500 WIFI: Device Time: 2020/04/27 08:53:04
```

The RealTerm window also shows the following configuration:

- Baud: 115200
- Port: 61
- Parity: None
- Data Bits: 8 bits
- Stop Bits: 1 bit
- Software Flow Control: Receive Xon Char: 17, Transmit Xoff Char: 19
- Hardware Flow Control: None
- Winsock is: Telnet

The Jupyter notebook shows the following steps:

- Step1. Config AWS-CLI
- Step2. [Empty]
- Step3. AWS GUI

The Jupyter notebook also shows the following text:

Before clicking AWS GUI its re...  
ring embedded project to cloud...  
low AWS GUI button ONLY after...

AWS User Region: us-east-2

Created policy Default  
number of certificates: 1

Loading the manifest\_item  
uniqueId: 0123c190308ff2b601  
About to try certificate impor...  
exception occurred: An error...  
RegisterCertificateWithoutCA...  
ed to access Multi-Account Device Cel...

MANIFEST\_IMPORT INFO attach\_thing...  
MANIFEST\_IMPORT FAIL False  
MANIFEST\_IMPORT SUCCESS False Fals...

number of thingIds to check: 1

Checking the manifest\_item  
uniqueId: 0123c190308ff2b601

# Demo

---

Connect to AWS IoT

# Q&A Section

---

# Thank You

---