CY8CKIT-064S0S2-4343W provisioning guide

About this document

Scope and purpose

This document provides instructions to provision the "Standard Secure" - AWS Wi-Fi Bluetooth® Pioneer Kit (CY8CKIT-064S0S2-4343W) for connecting to AWS IoT Core. This is part of the AWS Getting started with the Infineon CY8CKIT-064S0S2-4343W kit guide. Provisioning is a process whereby secure assets like keys and security policies are injected into the device. See the "Secure Boot" SDK user guide for details about the PSoC™ 64 "Secure Boot MCU" provisioning process.

Intended audience

This document is aimed at customers and provisioning partners for implementing provisioning algorithms.

Table of contents

1 Install "Secure Boot" SDK

Follow these steps to install the "Secure Boot" SDK:

1. Install Python 3.8.10 or later on the computer. Download it from the Python webpage.
2. By default, the Python installation adds itself to the system paths. If you have multiple versions of Python, follow these steps to ensure the system is using the correct version.
   a) Add the *python.exe* file location to the system variable "Path." For example: *C:\Python38*.
   b) Add the *<Python installation directory>/Scripts* subfolder to the system variable "PATH." For example: *C:\Python38\Scripts.*
3. For setting up the path environment variable:

Windows: If Python 2.7 is also installed in the computer, make sure that *Python38* and *Python38\Scripts* have higher priority in PATH than *C:\Python27.*

   a) Open Control Panel, go to **System** > **Advanced System Settings** > **Environment Variables**.
   b) Find "PATH" in the list of user variables.
   c) Click **Edit**.
   d) Move "*C:\Python38*" and "*C:\Python38\Scripts*" to the top.
   e) Save changes and exit Control Panel.
   f) Open a command-line/terminal program and run `python --version` to verify python version.

Linux: Most distributions of Linux should already have python2 and python3 installed. To verify that 'python' by default points to python3, run `python --version`.

If python3 is not set as default, run the following commands. The number at the end of each command denotes a priority.

```
update-alternatives --install /usr/bin/python python /usr/bin/python2.7 1
update-alternatives --install /usr/bin/python python /usr/bin/python3.8 2
```

MacOS: By default, 'python' points to */usr/bin/python* that is python2. To make 'python' and 'pip' resolve to python3 versions, execute the following:

```
echo 'alias python=python3' >> ~/.bash_profile
echo 'alias pip=pip3' >> ~/.bash_profile
source ~/.bash_profile
```

To verify that 'python' and 'pip' by default point to python3, run the following:

```
python --version
Python 3.8.10
pip --version
pip 23.3.2 from
/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-
packages/pip (python 3.8)
```

4. Install the "Secure Boot" SDK package by running the following command in the terminal window:

```
pip install -U cysecuretools
```

5. Install the libusb dependency for pyOCD. Please check the *README.md* for the latest instructions on installing libusb.

   Note: *During installation, there can be possible errors when installing colorama, protobuf and jsonschema. These can be safely ignored. For reference, use the following command to show the path to the installed package:*

   ```
   pip show cysecuretools
   ```

How to install libusb depends on the OS:

- **macOS:** use Homebrew: brew install libusb
- **Linux:** should already be installed
- **Windows:**

  a) Download libusb and place the DLL in the Python installation folder next to python.exe.

  b) Make sure to use the same 32- or 64-bit architecture as your Python installation.

Note: *Because of a known issue, libusb v1.0.21 is recommended to use on Windows instead of the most recent version.*

2 Provision the kit

Follow these steps to provision the kit:

1. Open the command-line/terminal program.
2. In the command-line/terminal program, navigate to *<freertos>/vendors/cypress/MTB/psoc6/psoc64tfm/security*.
3. Set up the FreeRTOS Workspace with the "Secure Boot" SDK.

   What does this step do?

   "CySecureTools" provides default policies and other secure assets that can be used to quickly set up the chip with development parameters, this step sets up the folder with all the required assets.

Run the following command. You will be asked to overwrite the files.

```
cysecuretools --target CY8CKIT-064S0S2-4343W init
```

2.1 Provisioning policy overview

The *policy_multi_cm0_cm4_tfm.json* file provided with the FreeRTOS repository sets up the chip with common security parameters used during development. Table 1 shows a high-level overview. For a detailed description of the policy parameters, refer to the "Secure Boot" SDK user guide.

Table 1 Policy parameters

Feature	Policy setup
"Secured" co-processor Debug Port	Open
CM4 Debug Port	Open
SysAP Debug Port	Open
"Secured" co-processor (TF-M) Flash Size	320 KB
CM4 (Application) Flash Size	1152 KB
External Memory Enabled for Update?	Yes
Re-provisioning Enabled?	Yes

1. Create a new signing key pair(s) (mandatory).

   What does this step do?

   "CySecureTools" looks at the provided policy, which specifies how many keys are needed to provision the chip. For this project, two key pairs are generated under the */keys/ folder* with the name TFM_S_KEY and TFM_NS_KEY.

   "CySecureTools" generates keys in two formats, PEM and JSON. Both the PEM and JSON files represent the same key.

   For a full description of what this does, refer to the "Secure Boot" SDK user guide.

Provision the kit

The FreeRTOS package has default keys available, you can choose to create a new key pair to sign your firmware by running the folowing command:

Note: *You will also be asked to overwrite files.*

```
cysecuretools --policy ./policy/policy_multi_CM0_CM4_tfm.json --target
CY8CKIT-064S0S2-4343W create-keys
```

2. Connect the CY8CKIT-064S0S2-4343W kit to the computer using the provided USB cable through the KitProg3 USB connector (J6).

   Ensure that the jumper shunt from J26 is removed to change VTARG voltage to 2.5 V and make sure jumper shunt on J14 is placed in VCC_3V3 position (between pin 2 and 3) before plugging in the kit to the computer. The 2.5 V supply is necessary for the next step, where PSoC™ 64 "Secure Boot" MCU eFuses are blown.

   Ensure the kit is in DAPLink mode. The status LED (LED2) will be ramping ON/OFF fast (~2 Hz) in this mode.

   Windows 7 KitProg3 driver issue:

   There is a known, sporadic issue with KitProg3 and Windows 7 that can prevent the kit from being recognized when you plug it in. Refer to the troubleshooting section of the KitProg3 user guide for information on how to resolve this.

3. Provision the device.

What does this step do?
This step sends the provisioning packet to the PSoC™ 64 "Secure Boot MCU" to finish provisioning.

   Run the following command in the command-line:

   ```
   cysecuretools --policy ./policy/policy_multi_CM0_CM4_tfm.json --target
   CY8CKIT-064S0S2-4343W provision-device
   ```

Note: *If you are using a pre-production kit, you will see a message such as:*

Note: *Early Production Units detected, please get earlier version of tools by running 'pip install --upgrade --force-reinstall cysecuretools==2.1.0'.*

   Run the following command to re-provision the kit that is already provisioned before you allow the re-provisioning:

   ```
   cysecuretools --policy ./policy/policy_multi_CM0_CM4_tfm.json --target
   CY8CKIT-064S0S2-4343W re-provision-device
   ```

4. Move the kit back to 3.3 V.

   Disconnect the kit from power and then put a shunt back on jumper J26 to the power to 3.3 V.

5. Move the kit back to CMSIS-DAP Bulk mode.

   Reconnect the kit to power then press and release the Mode button (SW3) one or more times until the KitProg3 is in CMSIS-DAP Bulk mode. The status LED (LED2) will be solid in this mode.

Congratulations! The kit is now provisioned and is ready to accept signed firmware.

Revision history

Document revision	Date	Description of changes
**	2020-09-03	Initial document.
*A	2021-02-01	Changed "optional" to "mandatory" in section 1.2 step 4.
*B	2021-04-15	Updated instructions to include a message about pre-production versions of the kit.
*C	2024-03-15	Updated the section Install "Secure Boot" SDK. Converted to IFX template.

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.
The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Infineon is under license.

Edition 2024-03-15
Published by

Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Email: erratum@infineon.com

Document reference
002-31073 Rev. *C

Important notice
The information contained in this document is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this document must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this document.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.