Getting started with EdgeLock™ SE050 support package

PLUG &TRUST

JORDI JOFRE

03/09/19

jordi.jofre@themobileknowledge.com

PUBLIC

NXP PLUG &TRUST

SECURE CONNECTIONS
FOR A SMARTER WORLD

Agenda

- Support package overview.
- Get started with the FRDM-K64F*:
  - Get resources
  - Install required SW and tools
  - Prepare hardware
  - Build SE050 Plug & Trust middleware
  - Run test examples
- pySSSCLI tool
- Evaluate use case examples.

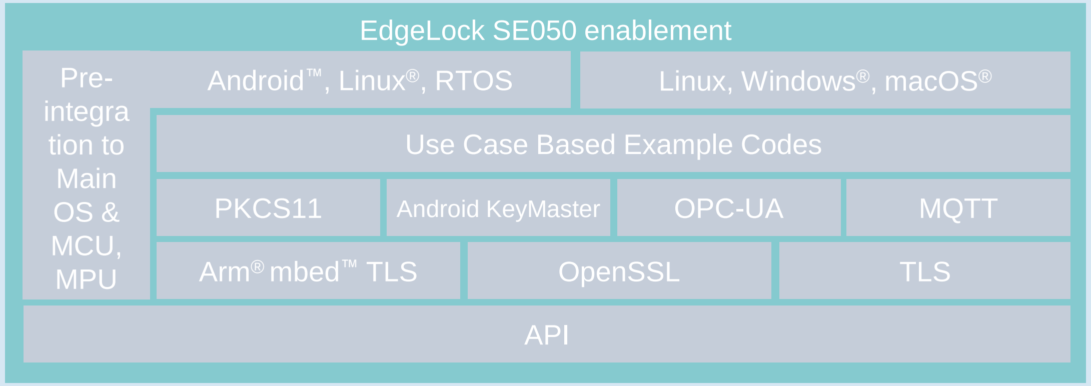
* SE050 Plug & Trust middleware supports several MCUs / MPUs. FRDM-K64F is used as an example

EdgeLock SE050 support package

SE050 Arduino compatible development kit

Supported evaluation MCU/MPU boards

EdgeLock SE050 Plug & Trust middleware



EdgeLock SE050 enablement

Pre-integration to Main OS & MCU, MPU

Android™, Linux®, RTOS

Linux, Windows®, macOS®

Use Case Based Example Codes

PKCS11

Android KeyMaster

OPC-UA

MQTT

Arm® mbed™ TLS

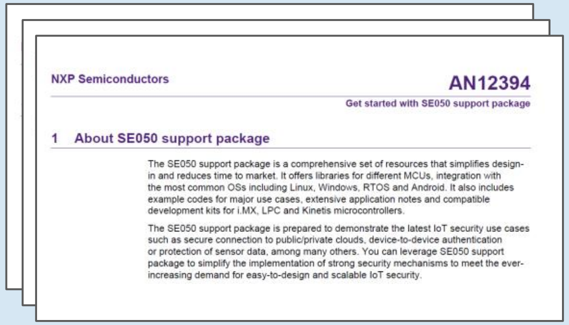
OpenSSL

TLS

API

Demo codes

Documentation



NXP Semiconductors

AN12394

Get started with SE050 support package

1 About SE050 support package

The SE050 support package is a comprehensive set of resources that simplifies design-in and reduces time to market. It offers libraries for different MCUs, integration with the most common OSs including Linux, Windows, RTOS and Android. It also includes example codes for major use cases, extensive application notes and compatible development kits for i.MX, LPC and Kinetis microcontrollers.

The SE050 support package is prepared to demonstrate the latest IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, among many others. You can leverage SE050 support package to simplify the implementation of strong security mechanisms to meet the ever-increasing demand for easy-to-design and scalable IoT security.

EdgeLock SE050 product variants

Group	Feature	SE050 A	SE050 B	SE050 C	Dev Kit
ECC algorithms	ECDSA	Yes	No	Yes	Yes
	ECDH	Yes	No	Yes	Yes
	ECDHE	Yes	No	Yes	Yes
	ECDAA	No	No	Yes	Yes
	EDDSA	No	No	Yes	Yes
ECC curves	ECC NIST (192 to 512 bit)	Yes	No	Yes	Yes
	ECC BrainPool (160 to 512 bit)	Yes	No	Yes	Yes
	Koblitz (160 to 256 bit)	Yes	No	Yes	Yes
	Montgomery curve25519	No	No	Yes	Yes
	Twisted Edwards (for Ed25519)	No	No	Yes	Yes
RSA	RSA (up to 4096 bit)	No	Yes	Yes	Yes
Symmetric	(T)DES	Yes	Yes	Yes	Yes
	AES (128-256 bit)	Yes	Yes	Yes	Yes
Key derivation	TLS KDF, TLS PSK	Yes	Yes	Yes	Yes
	MIFARE DESFire KDF	No	No	Yes	Yes
	WiFi KDF (PBKDF2)	Yes	Yes	Yes	Yes
	OPC_UA KDF	Yes	Yes	Yes	Yes
Interfaces	I²C slave	Yes	Yes	Yes	Yes
	I²C master	No	No	Yes	Yes
	ISO/IEC14443	No	No	Yes	Yes

OM-SE050ARD

OM-SE050ARD uses the SE050 Type C configuration

Get started with EdgeLock SE050 support package

How do I get familiar with support package contents?

AN12394 - Get started with SE050 support package

How do I get started?

AN12396 - Quick start guide with Kinetis K64

AN12397 - Quick start guide with i.MX6UltraLite

AN12542 - Quick start guide with LPC55S69*

AN12398 - Quick start guide to SE050 Visual Studio projects

AN12450 - Quick start guide with i.MX RT1050*

AN12570 - Quick start guide with Raspberry Pi*

How do I get familiar with OM-SE050ARD dev kit?

AN12395 - OM-SE050ARD hardware overview

* Will be published soon. Contact NXP if you need an early version.

FRDM-K64F is used as an example to run your first demo project. The same demo projects are available for each supported MCU / MPU.

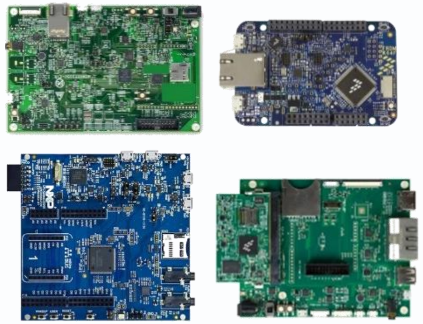
Get resources

Get EdgeLock SE050 support package resources

Step 1

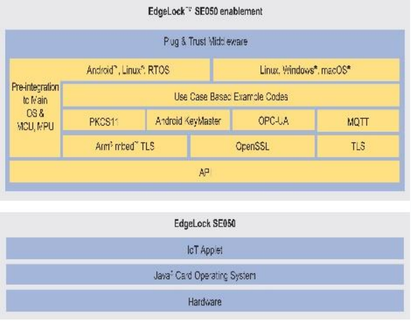
Get your SE050 Arduino compatible development kit

Step 2



Choose and get your MCU / MPU board (e.g., FRDM-K64F)

Step 3



EdgeLock™ SE050 enablement

Plug & Trust Middleware

Pre-integration to Main OS & MCU, MPU

Android™, Linux®, RTOS

Linux, Windows®, macOS®

Use Case Based Example Codes

PKCS11 | Android KeyMaster | OPC-UA | MQTT

Arm® mbed™ TLS | OpenSSL | TLS

API

EdgeLock SE050

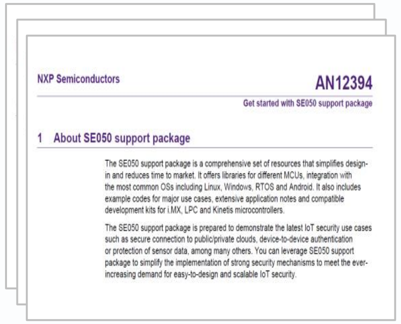
IoT Applet

Java® Card Operating System

Hardware

Download SE050 Plug & Trust middleware

Step 4



NXP Semiconductors

AN12394

Get started with SE050 support package

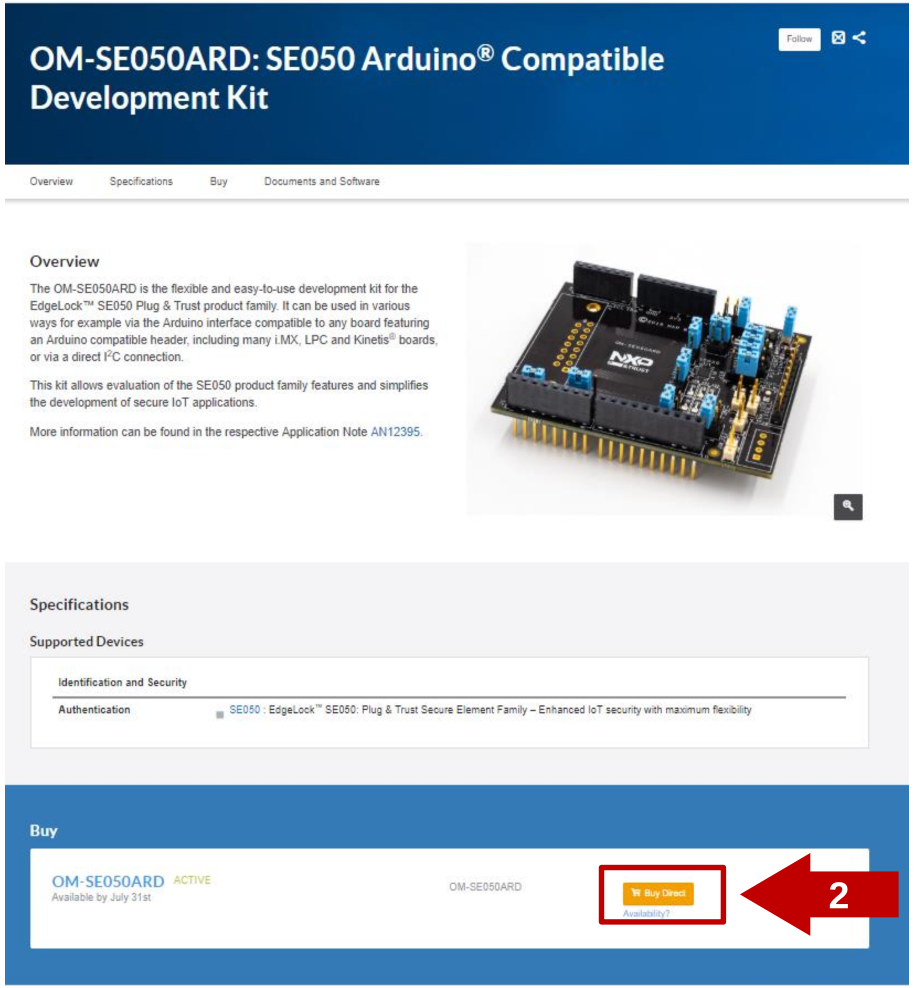
1 About SE050 support package

The SE050 support package is a comprehensive set of resources that simplifies design-in and reduces time to market. It offers libraries for different MCUs, integration with the most common OSs including Linux, Windows, RTOS and Android. It also includes example codes for major use cases, extensive application notes and compatible development kits for i.MX, LPC and Kinetis microcontrollers.

The SE050 support package is prepared to demonstrate the latest IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, among many others. You can leverage SE050 support package to simplify the implementation of strong security mechanisms to meet the ever-increasing demand for easy-to-design and scalable IoT security.

Read support package documentation

Get your SE050 Arduino compatible development kit



OM-SE050ARD: SE050 Arduino® Compatible Development Kit

Overview

The OM-SE050ARD is the flexible and easy-to-use development kit for the EdgeLock™ SE050 Plug & Trust product family. It can be used in various ways for example via the Arduino interface compatible to any board featuring an Arduino compatible header, including many i.MX, LPC and Kinetis® boards, or via a direct I²C connection.

This kit allows evaluation of the SE050 product family features and simplifies the development of secure IoT applications.

More information can be found in the respective Application Note AN12395.

Specifications

Supported Devices

Identification and Security	
Authentication	SE050 : EdgeLock™ SE050: Plug & Trust Secure Element Family – Enhanced IoT security with maximum flexibility

Buy

OM-SE050ARD ACTIVE
Available by July 31st

OM-SE050ARD

1. Go to https://www.nxp.com/products/:OM-SE050ARD

2. Scroll down and click on **Buy direct** button.

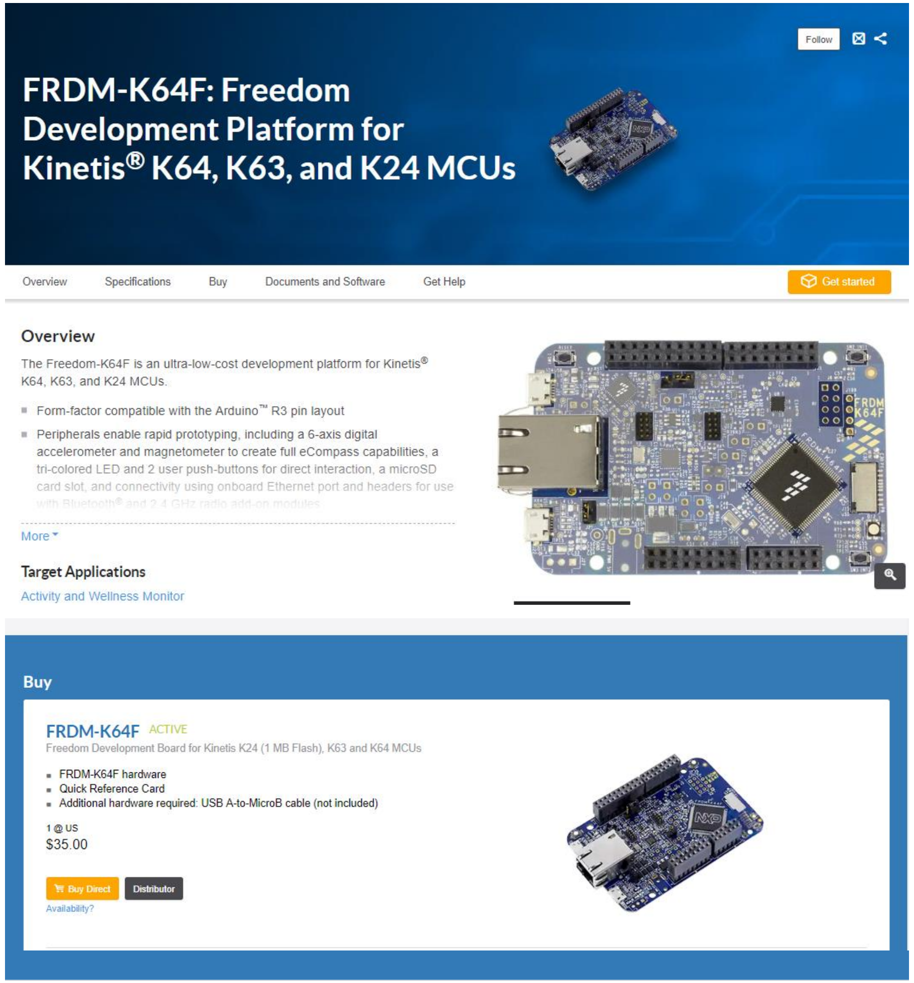
3. Sign-in with your account at the NXP website.

4. Fill-in your shopping basket and place your order.

* Ordering is also possible via NXP distributors.

PLUG&TRUST

Get your MCU/MPU board



Follow

FRDM-K64F: Freedom Development Platform for Kinetis® K64, K63, and K24 MCUs

Overview

The Freedom-K64F is an ultra-low-cost development platform for Kinetis® K64, K63, and K24 MCUs.

- Form-factor compatible with the Arduino™ R3 pin layout
- Peripherals enable rapid prototyping, including a 6-axis digital accelerometer and magnetometer to create full eCompass capabilities, a tri-colored LED and 2 user push-buttons for direct interaction, a microSD card slot, and connectivity using onboard Ethernet port and headers for use with Bluetooth® and 2.4 GHz radio add-on modules

More

Target Applications

Activity and Wellness Monitor

Buy

FRDM-K64F ACTIVE

Freedom Development Board for Kinetis K24 (1 MB Flash), K63 and K64 MCUs

- FRDM-K64F hardware
- Quick Reference Card
- Additional hardware required: USB A-to-MicroB cable (not included)

1 @ US
$35.00

1 Choose your MCU / MPU (e.g., FRDM-K64F*)

2 Go to the MCU/MPU board webpage.
https://www.nxp.com/products/:FRDM-K64F

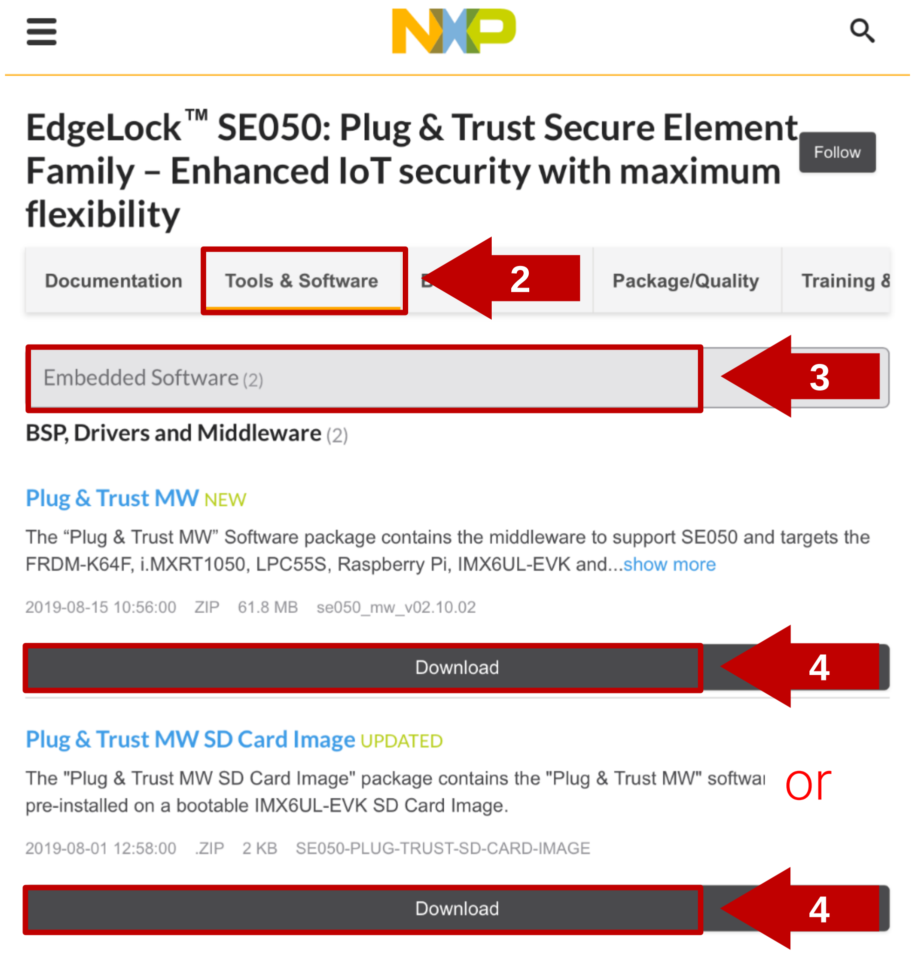
3 Scroll down and click on Buy direct button.

4 Fill-in your shopping basket and place your order.

* Ordering is also possible via NXP distributors.

*FRDM-K64F used as an example. EdgeLock SE050 supports several MCU/MPUs

Get latest version of SE050 Plug & Trust middleware



EdgeLock™ SE050: Plug & Trust Secure Element Family – Enhanced IoT security with maximum flexibility

Embedded Software (2)

BSP, Drivers and Middleware (2)

Plug & Trust MW NEW

The “Plug & Trust MW” Software package contains the middleware to support SE050 and targets the FRDM-K64F, i.MXRT1050, LPC55S, Raspberry Pi, IMX6UL-EVK and...show more

2019-08-15 10:56:00 ZIP 61.8 MB se050_mw_v02.10.02

Download

Plug & Trust MW SD Card Image UPDATED

The "Plug & Trust MW SD Card Image" package contains the "Plug & Trust MW" softwa pre-installed on a bootable IMX6UL-EVK SD Card Image.

2019-08-01 12:58:00 .ZIP 2 KB SE050-PLUG-TRUST-SD-CARD-IMAGE

Download

1. Go to https://www.nxp.com/products/:SE050

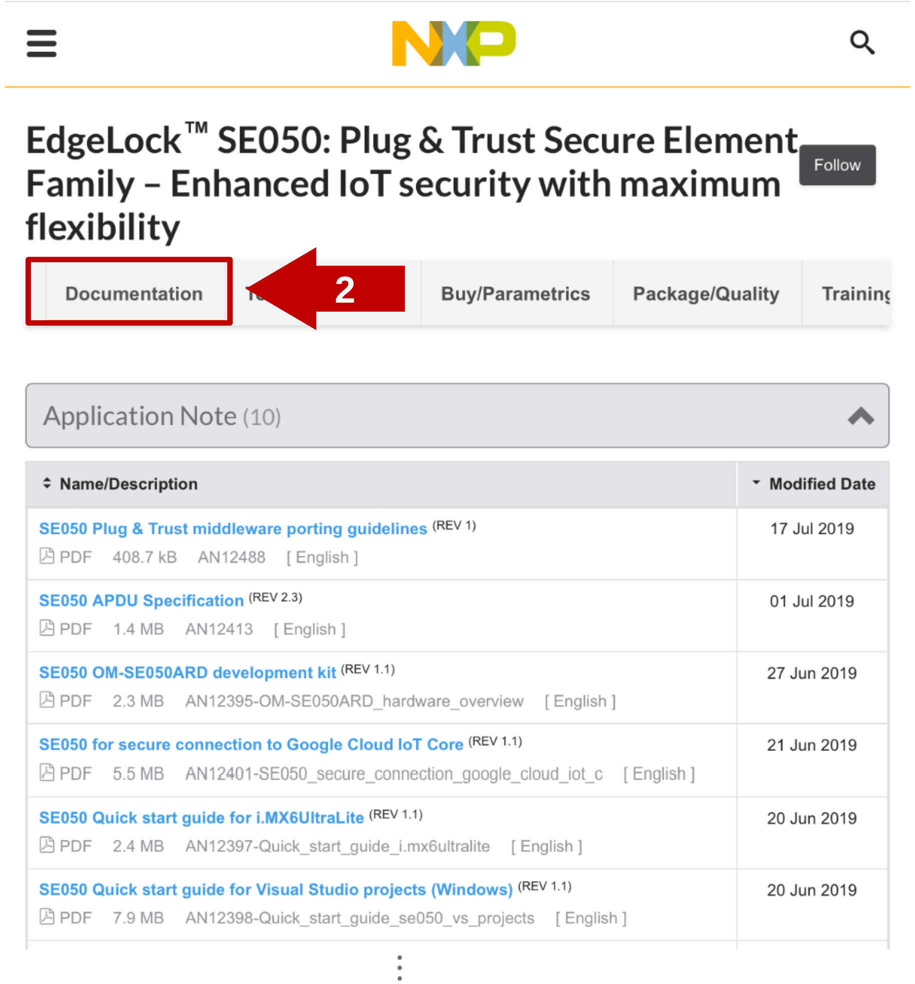
2. Click on Tools & Software tab.

3. Scroll down to the Embedded Software section.

4. *Download SE050 Plug & Trust MW.

*Plug & Trust MW: FRDM-K64F, i.MXRT1050, LPC55S, Raspberry Pi, IMX6UL-EVK and iMX8Q
*Plug & Trust MW SD Card image: IMX6UL-EVK

Get latest version of SE050 Plug & Trust documentation



EdgeLock™ SE050: Plug & Trust Secure Element Family – Enhanced IoT security with maximum flexibility

Follow

Application Note (10)

Name/Description	Modified Date
SE050 Plug & Trust middleware porting guidelines (REV 1) PDF 408.7 kB AN12488 [English]	17 Jul 2019
SE050 APDU Specification (REV 2.3) PDF 1.4 MB AN12413 [English]	01 Jul 2019
SE050 OM-SE050ARD development kit (REV 1.1) PDF 2.3 MB AN12395-OM-SE050ARD_hardware_overview [English]	27 Jun 2019
SE050 for secure connection to Google Cloud IoT Core (REV 1.1) PDF 5.5 MB AN12401-SE050_secure_connection_google_cloud_iot_c [English]	21 Jun 2019
SE050 Quick start guide for i.MX6UltraLite (REV 1.1) PDF 2.4 MB AN12397-Quick_start_guide_i.mx6ultralite [English]	20 Jun 2019
SE050 Quick start guide for Visual Studio projects (Windows) (REV 1.1) PDF 7.9 MB AN12398-Quick_start_guide_se050_vs_projects [English]	20 Jun 2019

⋮

1 Go to https://www.nxp.com/products/:SE050

2 Click on Documentation tab.

3 Find your document within Application Note, Brochure, User Guide page sections , etc.

Ready to start!

Install required SW and tools

Required software and tools

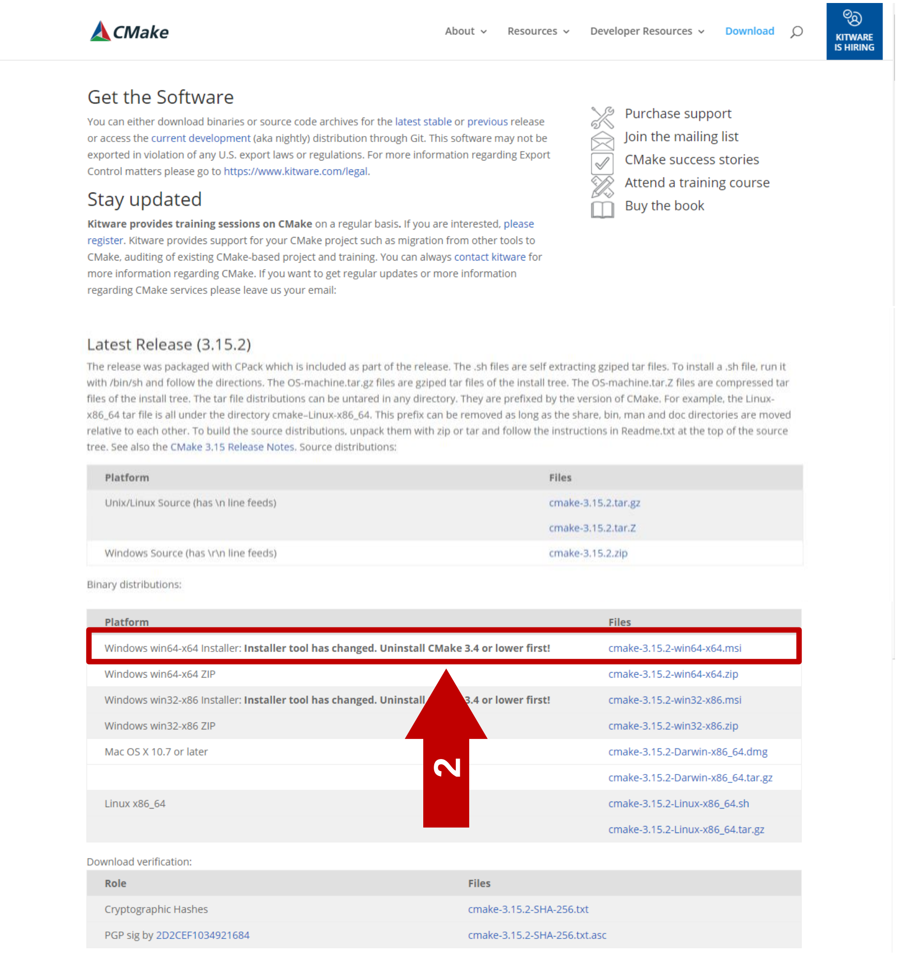
Install the following software tools in your development PC

CMake
An open-source, cross-platform tool designed to build, test and package software

Python 2.7 32-bit version
A programming language used to generate scripts that facilitate operation with the MW.

MCUXpresso
A free-of-charge, easy-to-use IDE for Kinetis and LPC MCUs, and i.MX RT processors

Install CMake



Get the Software

You can either download binaries or source code archives for the latest stable or previous release or access the current development (aka nightly) distribution through Git. This software may not be exported in violation of any U.S. export laws or regulations. For more information regarding Export Control matters please go to https://www.kitware.com/legal.

- Purchase support
- Join the mailing list
- CMake success stories
- Attend a training course
- Buy the book

Stay updated

Kitware provides training sessions on CMake on a regular basis. If you are interested, please register. Kitware provides support for your CMake project such as migration from other tools to CMake, auditing of existing CMake-based project and training. You can always contact kitware for more information regarding CMake. If you want to get regular updates or more information regarding CMake services please leave us your email:

Latest Release (3.15.2)

The release was packaged with CPack which is included as part of the release. The .sh files are self extracting gziped tar files. To install a .sh file, run it with /bin/sh and follow the directions. The OS-machine.tar.gz files are gziped tar files of the install tree. The OS-machine.tar.Z files are compressed tar files of the install tree. The tar file distributions can be untared in any directory. They are prefixed by the version of CMake. For example, the Linux-x86_64 tar file is all under the directory cmake–Linux-x86_64. This prefix can be removed as long as the share, bin, man and doc directories are moved relative to each other. To build the source distributions, unpack them with zip or tar and follow the instructions in Readme.txt at the top of the source tree. See also the CMake 3.15 Release Notes. Source distributions:

Platform	Files
Unix/Linux Source (has \n line feeds)	cmake-3.15.2.tar.gz
	cmake-3.15.2.tar.Z
Windows Source (has \r\n line feeds)	cmake-3.15.2.zip

Binary distributions:

Platform	Files
Windows win64-x64 Installer: **Installer tool has changed. Uninstall CMake 3.4 or lower first!**	cmake-3.15.2-win64-x64.msi
Windows win64-x64 ZIP	cmake-3.15.2-win64-x64.zip
Windows win32-x86 Installer: **Installer tool has changed. Uninstall 3.4 or lower first!**	cmake-3.15.2-win32-x86.msi
Windows win32-x86 ZIP	cmake-3.15.2-win32-x86.zip
Mac OS X 10.7 or later	cmake-3.15.2-Darwin-x86_64.dmg
	cmake-3.15.2-Darwin-x86_64.tar.gz
Linux x86_64	cmake-3.15.2-Linux-x86_64.sh
	cmake-3.15.2-Linux-x86_64.tar.gz

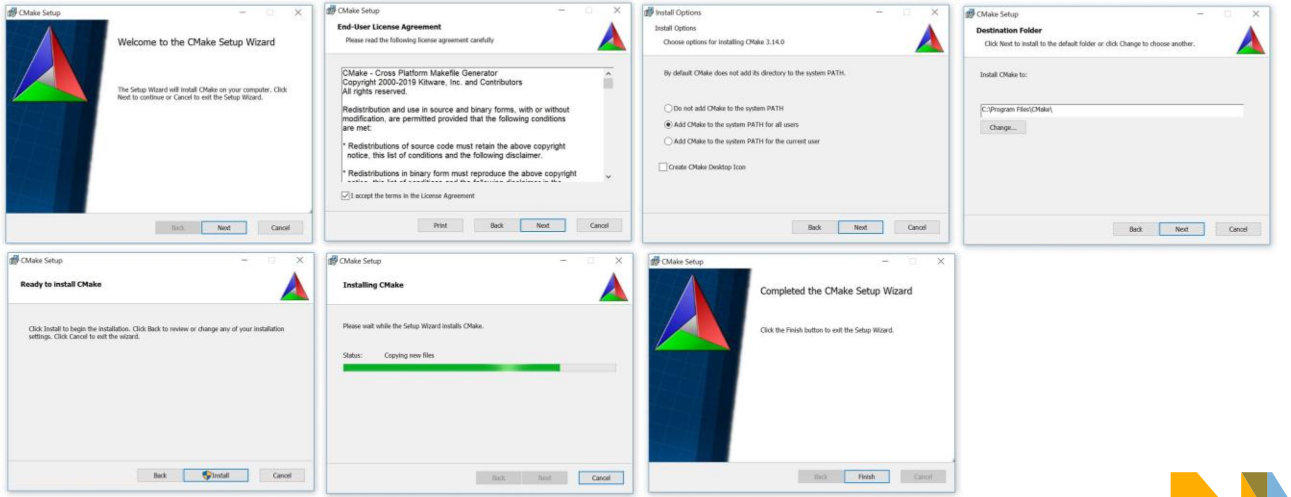
Download verification:

Role	Files
Cryptographic Hashes	cmake-3.15.2-SHA-256.txt
PGP sig by 2D2CEF1034921684	cmake-3.15.2-SHA-256.txt.asc

1 Go to https://cmake.org/download/

2 Scroll down and select your binary distribution.

3 Follow the setup wizard until the installation is completed.



CMake Setup — Welcome to the CMake Setup Wizard

The Setup Wizard will install CMake on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

CMake Setup — End-User License Agreement

Please read the following license agreement carefully

CMake - Cross Platform Makefile Generator
Copyright 2000-2019 Kitware, Inc. and Contributors
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

☑ I accept the terms in the License Agreement

Install Options — Install Options

Choose options for installing CMake 3.14.0

By default CMake does not add its directory to the system PATH.

○ Do not add CMake to the system PATH
● Add CMake to the system PATH for all users
○ Add CMake to the system PATH for the current user

□ Create CMake Desktop Icon

CMake Setup — Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install CMake to:

C:\Program Files\CMake\

CMake Setup — Ready to install CMake

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

CMake Setup — Installing CMake

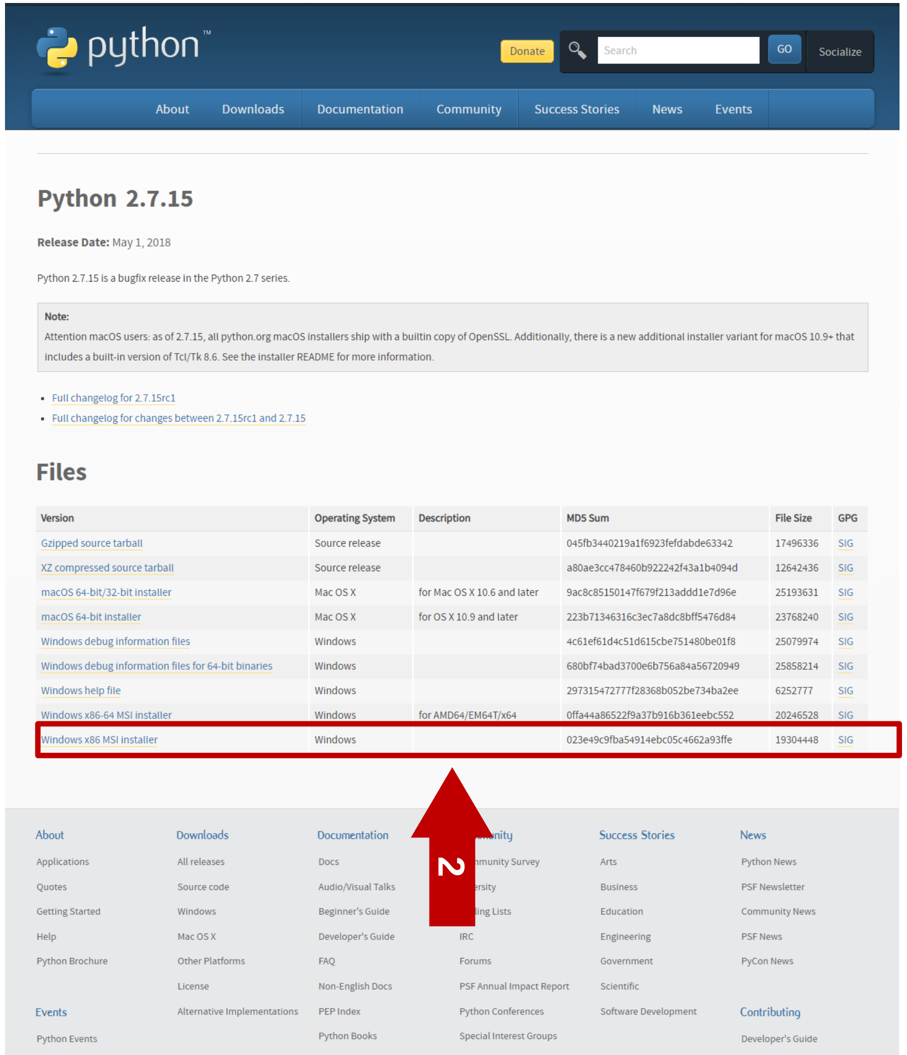
Please wait while the Setup Wizard installs CMake.

Status: Copying new files

CMake Setup — Completed the CMake Setup Wizard

Click the Finish button to exit the Setup Wizard.

Install Python



Python 2.7.15

Release Date: May 1, 2018

Python 2.7.15 is a bugfix release in the Python 2.7 series.

Note:
Attention macOS users: as of 2.7.15, all python.org macOS installers ship with a builtin copy of OpenSSL. Additionally, there is a new additional installer variant for macOS 10.9+ that includes a built-in version of Tcl/Tk 8.6. See the installer README for more information.

- Full changelog for 2.7.15rc1
- Full changelog for changes between 2.7.15rc1 and 2.7.15

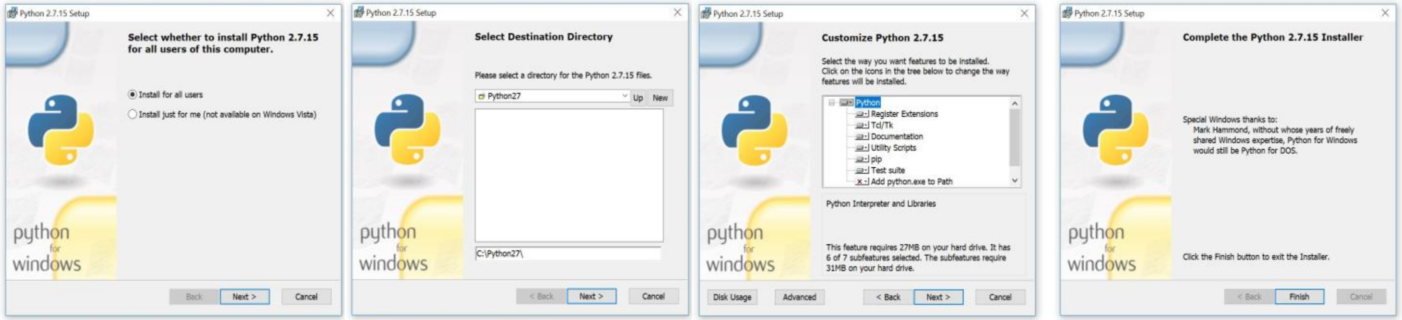
Files

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		045fb3440219a1f6923fefdabde63342	17496336	SIG
XZ compressed source tarball	Source release		a80ae3cc478460b922242f43a1b4094d	12642436	SIG
macOS 64-bit/32-bit installer	Mac OS X	for Mac OS X 10.6 and later	9ac8c85150147f679f213addd1e7d96e	25193631	SIG
macOS 64-bit installer	Mac OS X	for OS X 10.9 and later	223b71346316c3ec7a8dc8bff5476d84	23768240	SIG
Windows debug information files	Windows		4c61ef61d4c51d615cbe751480be01f8	25079974	SIG
Windows debug information files for 64-bit binaries	Windows		680bf74bad3700e6b756a84a56720949	25858214	SIG
Windows help file	Windows		297315472777f28368b052be734ba2ee	6252777	SIG
Windows x86-64 MSI installer	Windows	for AMD64/EM64T/x64	0ffa44a86522f9a37b916b361eebc552	20246528	SIG
Windows x86 MSI installer	Windows		023e49c9fba54914ebc05c4662a93ffe	19304448	SIG

1 Go to https://www.python.org/downloads/release/python-2715/

2 Download Python v.2.7.15 32-bit version.

3 Follow the setup wizard until the installation is completed.



Select whether to install Python 2.7.15 for all users of this computer.

● Install for all users
○ Install just for me (not available on Windows Vista)

Select Destination Directory

Please select a directory for the Python 2.7.15 files.

Python27

C:\Python27\

Customize Python 2.7.15

Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.

- Python
  - Register Extensions
  - Tcl/Tk
  - Documentation
  - Utility Scripts
  - pip
  - Test suite
  - Add python.exe to Path

Python Interpreter and Libraries

This feature requires 27MB on your hard drive. It has 6 of 7 subfeatures selected. The subfeatures require 31MB on your hard drive.

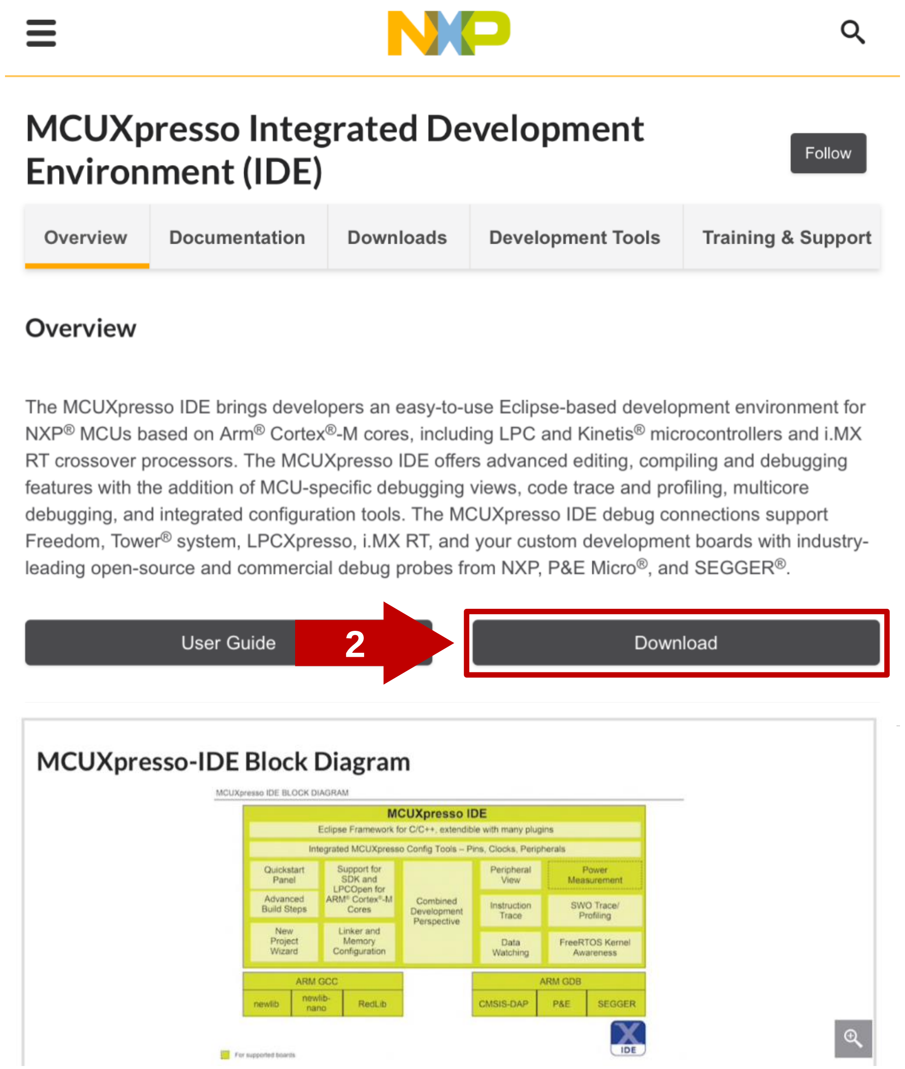
Complete the Python 2.7.15 Installer

Special Windows thanks to:
Mark Hammond, without whose years of freely shared Windows expertise, Python for Windows would still be Python for DOS.

Click the Finish button to exit the Installer.

Make sure you download Python v2.7.15 32 bit version. Python v3 is not yet supported and neither is the 64 bit

Install MCUXpresso



MCUXpresso Integrated Development Environment (IDE)

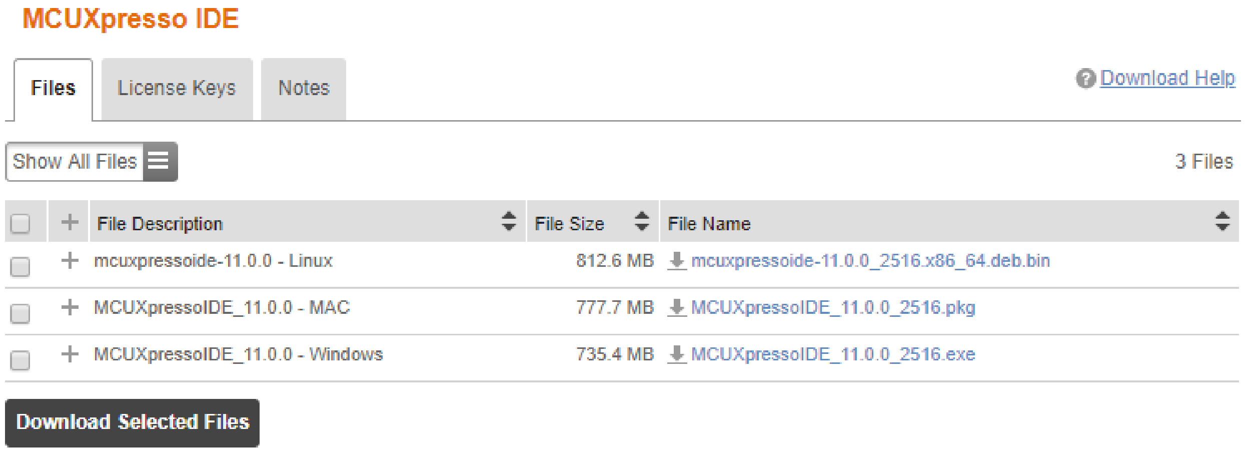
Overview

The MCUXpresso IDE brings developers an easy-to-use Eclipse-based development environment for NXP® MCUs based on Arm® Cortex®-M cores, including LPC and Kinetis® microcontrollers and i.MX RT crossover processors. The MCUXpresso IDE offers advanced editing, compiling and debugging features with the addition of MCU-specific debugging views, code trace and profiling, multicore debugging, and integrated configuration tools. The MCUXpresso IDE debug connections support Freedom, Tower® system, LPCXpresso, i.MX RT, and your custom development boards with industry-leading open-source and commercial debug probes from NXP, P&E Micro®, and SEGGER®.

MCUXpresso-IDE Block Diagram

MCUXpresso IDE BLOCK DIAGRAM
MCUXpresso IDE
Eclipse Framework for C/C++, extendible with many plugins
Integrated MCUXpresso Config Tools – Pins, Clocks, Peripherals
Quickstart Panel
Advanced Build Steps
New Project Wizard
Support for SDK and LPCOpen for ARM® Cortex®-M Cores
Linker and Memory Configuration
Combined Development Perspective
Peripheral View
Instruction Trace
Data Watching
Power Measurement
SWO Trace/ Profiling
FreeRTOS Kernel Awareness
ARM GCC
newlib
newlib-nano
RedLib
ARM GDB
CMSIS-DAP
P&E
SEGGER
IDE
For supported boards

1. Go to www.nxp.com/mcuxpresso/ide
2. Download MCUXpresso IDE v.11 installer.
3. Follow the setup wizard until the installation is completed.



MCUXpresso IDE

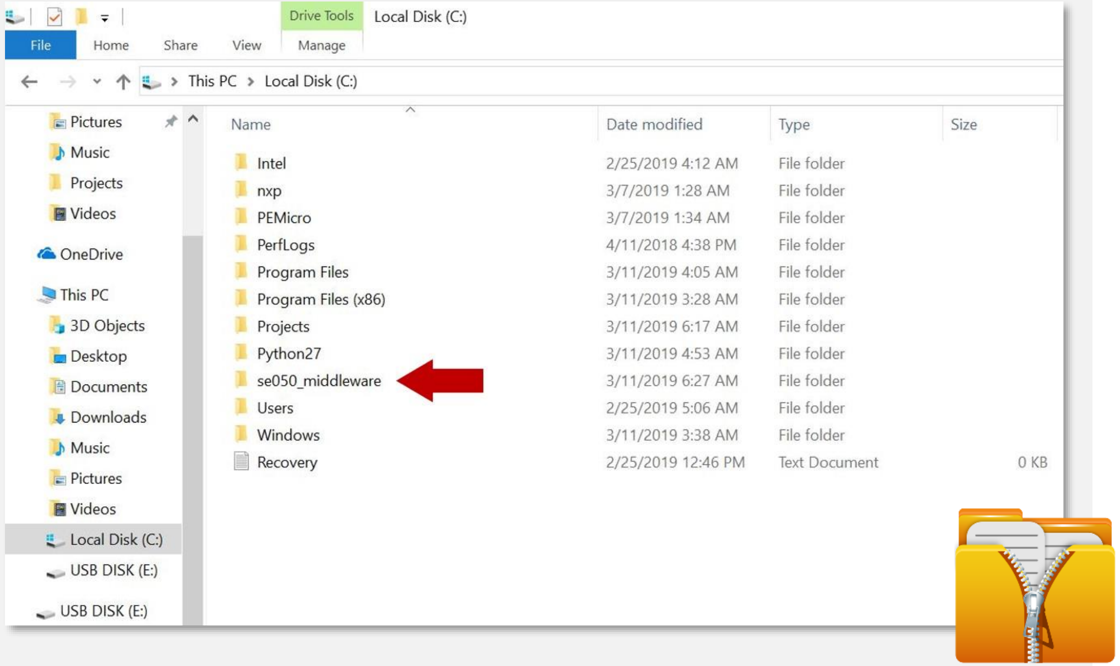
□	+	File Description	File Size	File Name
□	+	mcuxpressoide-11.0.0 - Linux	812.6 MB	mcuxpressoide-11.0.0_2516.x86_64.deb.bin
□	+	MCUXpressoIDE_11.0.0 - MAC	777.7 MB	MCUXpressoIDE_11.0.0_2516.pkg
□	+	MCUXpressoIDE_11.0.0 - Windows	735.4 MB	MCUXpressoIDE_11.0.0_2516.exe

Please, make sure you allow the installation of the additional drivers required by MCUXpresso during the installation process

Build SE050 Plug & Trust middleware

Unzip SE050 Plug & Trust middleware

1 Create folder to unzip SE050 Plug & Trust middleware in C:\ *



Drive Tools | Local Disk (C:)

File | Home | Share | View | Manage

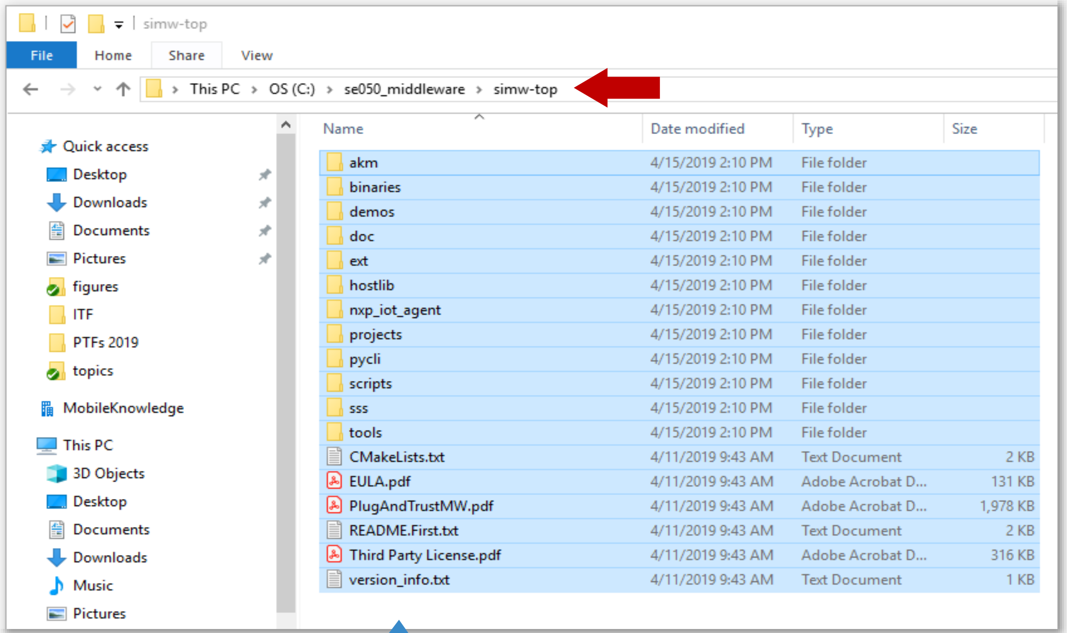
This PC > Local Disk (C:)

- Pictures
- Music
- Projects
- Videos
- OneDrive
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- USB DISK (E:)
- USB DISK (E:)

Name	Date modified	Type	Size
Intel	2/25/2019 4:12 AM	File folder	
nxp	3/7/2019 1:28 AM	File folder	
PEMicro	3/7/2019 1:34 AM	File folder	
PerfLogs	4/11/2018 4:38 PM	File folder	
Program Files	3/11/2019 4:05 AM	File folder	
Program Files (x86)	3/11/2019 3:28 AM	File folder	
Projects	3/11/2019 6:17 AM	File folder	
Python27	3/11/2019 4:53 AM	File folder	
se050_middleware	3/11/2019 6:27 AM	File folder	
Users	2/25/2019 5:06 AM	File folder	
Windows	3/11/2019 3:38 AM	File folder	
Recovery	2/25/2019 12:46 PM	Text Document	0 KB

se050_mw_v02.10.02

2 Unzip SE050 Plug & Trust middleware into a folder named *simw-top***



simw-top

File | Home | Share | View

This PC > OS (C:) > se050_middleware > simw-top

- Quick access
- Desktop
- Downloads
- Documents
- Pictures
- figures
- ITF
- PTFs 2019
- topics
- MobileKnowledge
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures

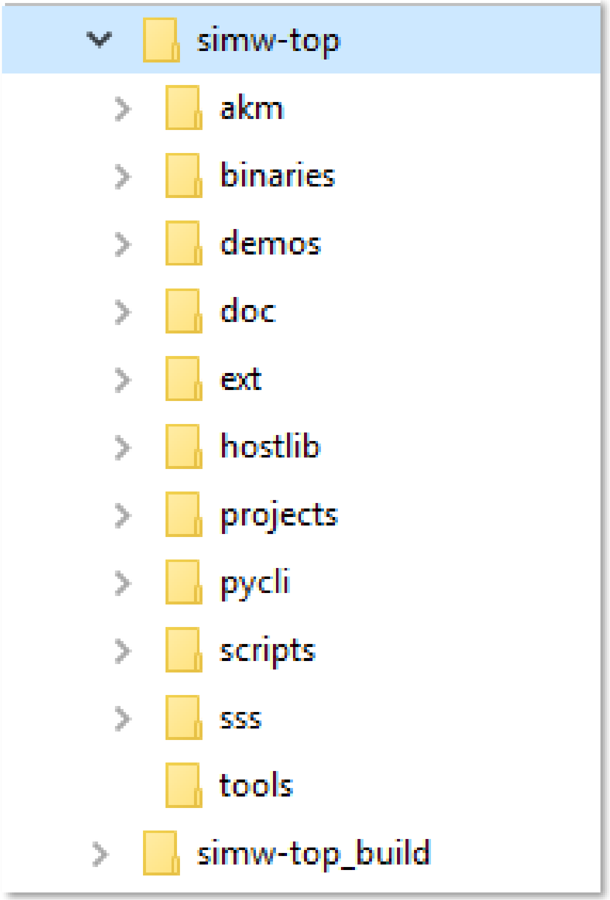
Name	Date modified	Type	Size
akm	4/15/2019 2:10 PM	File folder	
binaries	4/15/2019 2:10 PM	File folder	
demos	4/15/2019 2:10 PM	File folder	
doc	4/15/2019 2:10 PM	File folder	
ext	4/15/2019 2:10 PM	File folder	
hostlib	4/15/2019 2:10 PM	File folder	
nxp_iot_agent	4/15/2019 2:10 PM	File folder	
projects	4/15/2019 2:10 PM	File folder	
pycli	4/15/2019 2:10 PM	File folder	
scripts	4/15/2019 2:10 PM	File folder	
sss	4/15/2019 2:10 PM	File folder	
tools	4/15/2019 2:10 PM	File folder	
CMakeLists.txt	4/11/2019 9:43 AM	Text Document	2 KB
EULA.pdf	4/11/2019 9:43 AM	Adobe Acrobat D...	131 KB
PlugAndTrustMW.pdf	4/11/2019 9:43 AM	Adobe Acrobat D...	1,978 KB
README.First.txt	4/11/2019 9:43 AM	Text Document	2 KB
Third Party License.pdf	4/11/2019 9:43 AM	Adobe Acrobat D...	316 KB
version_info.txt	4/11/2019 9:43 AM	Text Document	1 KB

Unzip contents

* The shortest path possible and without spaces in it is recommended

**simw-top: secure interface middleware top-level directory
The naming is not strictly needed, but it is used in the rest of the presentation

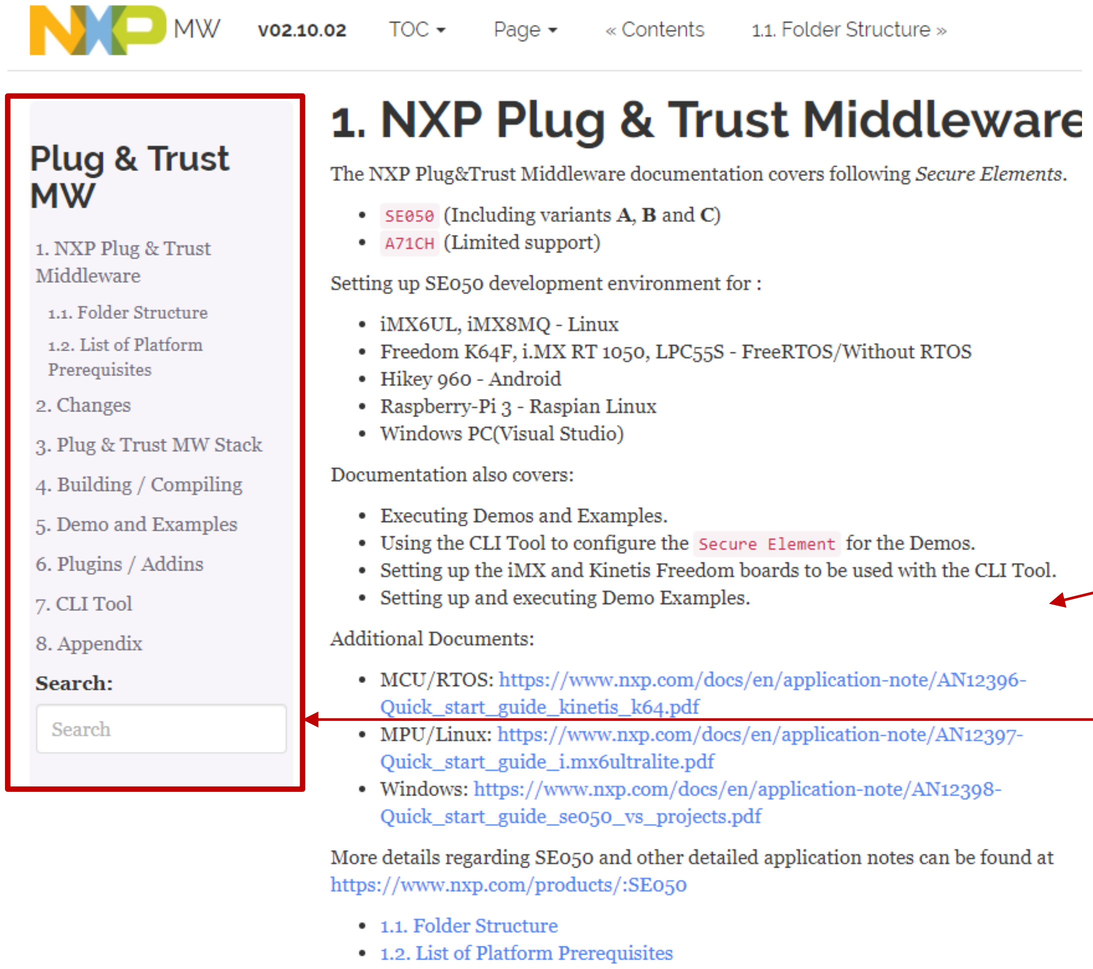
SE050 Plug & Trust middleware folder structure



A software stack designed to facilitate the integration of NXP security ICs (A71CH, SE050) into your MCU or MPU.

- Akm: Android Keymaster
- Binaries: Pre-compiled FW for command line interface and VCOM software
- Demos: Demo code examples
- Doc: HTML documentation
- Ext: External libraries
- Hostlib: Source folder of the host library
- Projects: MCUXpresso projectsd
- Pycli: command line client
- Scripts: Helper compilation scripts
- Sss: SSS api source code
- Tools: Compile MW .dll library

SE050 Plug & Trust code documentation



Plug & Trust MW

Search:

1. NXP Plug & Trust Middleware

The NXP Plug&Trust Middleware documentation covers following *Secure Elements*.

- `SE050` (Including variants **A**, **B** and **C**)
- `A71CH` (Limited support)

Setting up SE050 development environment for :

- iMX6UL, iMX8MQ - Linux
- Freedom K64F, i.MX RT 1050, LPC55S - FreeRTOS/Without RTOS
- Hikey 960 - Android
- Raspberry-Pi 3 - Raspian Linux
- Windows PC(Visual Studio)

Documentation also covers:

- Executing Demos and Examples.
- Using the CLI Tool to configure the `Secure Element` for the Demos.
- Setting up the iMX and Kinetis Freedom boards to be used with the CLI Tool.
- Setting up and executing Demo Examples.

Additional Documents:

- MCU/RTOS: https://www.nxp.com/docs/en/application-note/AN12396-Quick_start_guide_kinetis_k64.pdf
- MPU/Linux: https://www.nxp.com/docs/en/application-note/AN12397-Quick_start_guide_i.mx6ultralite.pdf
- Windows: https://www.nxp.com/docs/en/application-note/AN12398-Quick_start_guide_se050_vs_projects.pdf

More details regarding SE050 and other detailed application notes can be found at https://www.nxp.com/products/:SE050

- 1.1. Folder Structure
- 1.2. List of Platform Prerequisites

The code documentation is an HTML file created using the Sphinx documentation generator tool.

1 Go to `simw-top\doc` folder

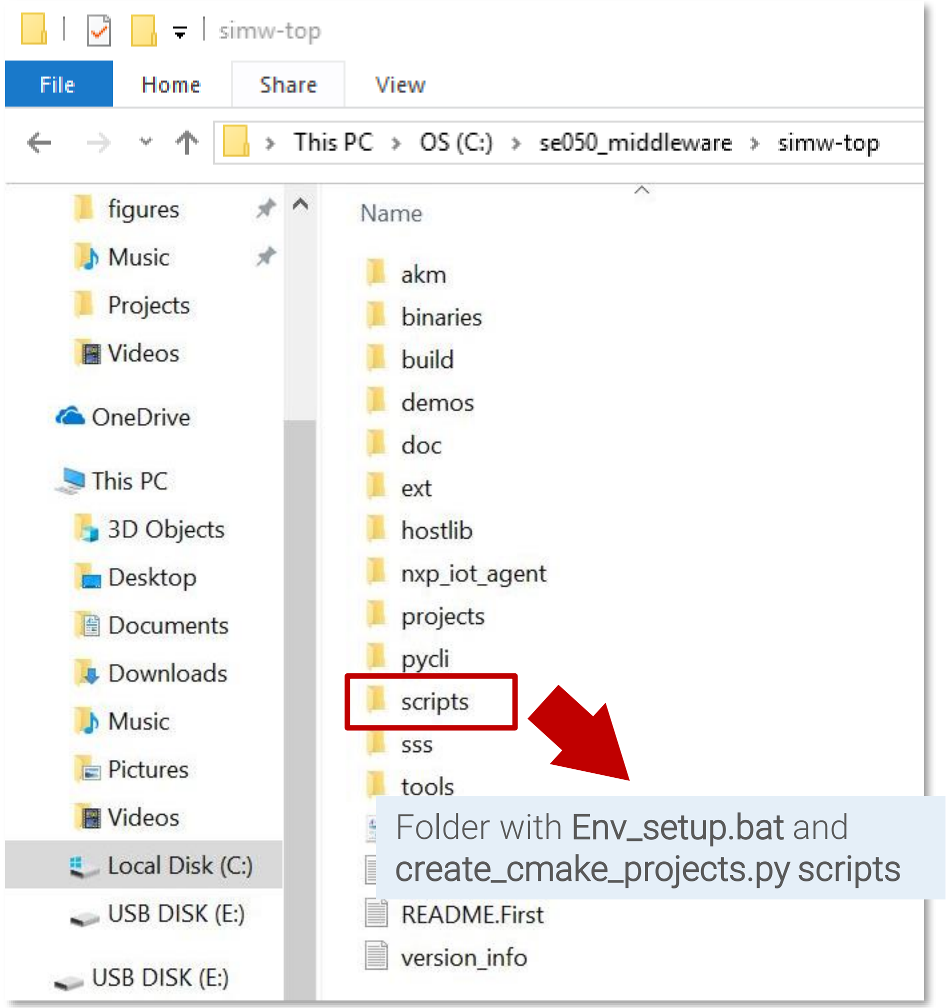
2 Double click in the `index.html` file

3 A browser with the documentation landing page will open

4 Navigate through the different document sections using the left-hand side menu

The primary audience of this HTML documentation are programmers, developers, system architects and system designers.

Build SE050 Plug & Trust middleware platform projects



Folder with Env_setup.bat and create_cmake_projects.py scripts

SE050 Plug & Trust middleware includes scripts to automatically generate build projects:

Env_setup.bat

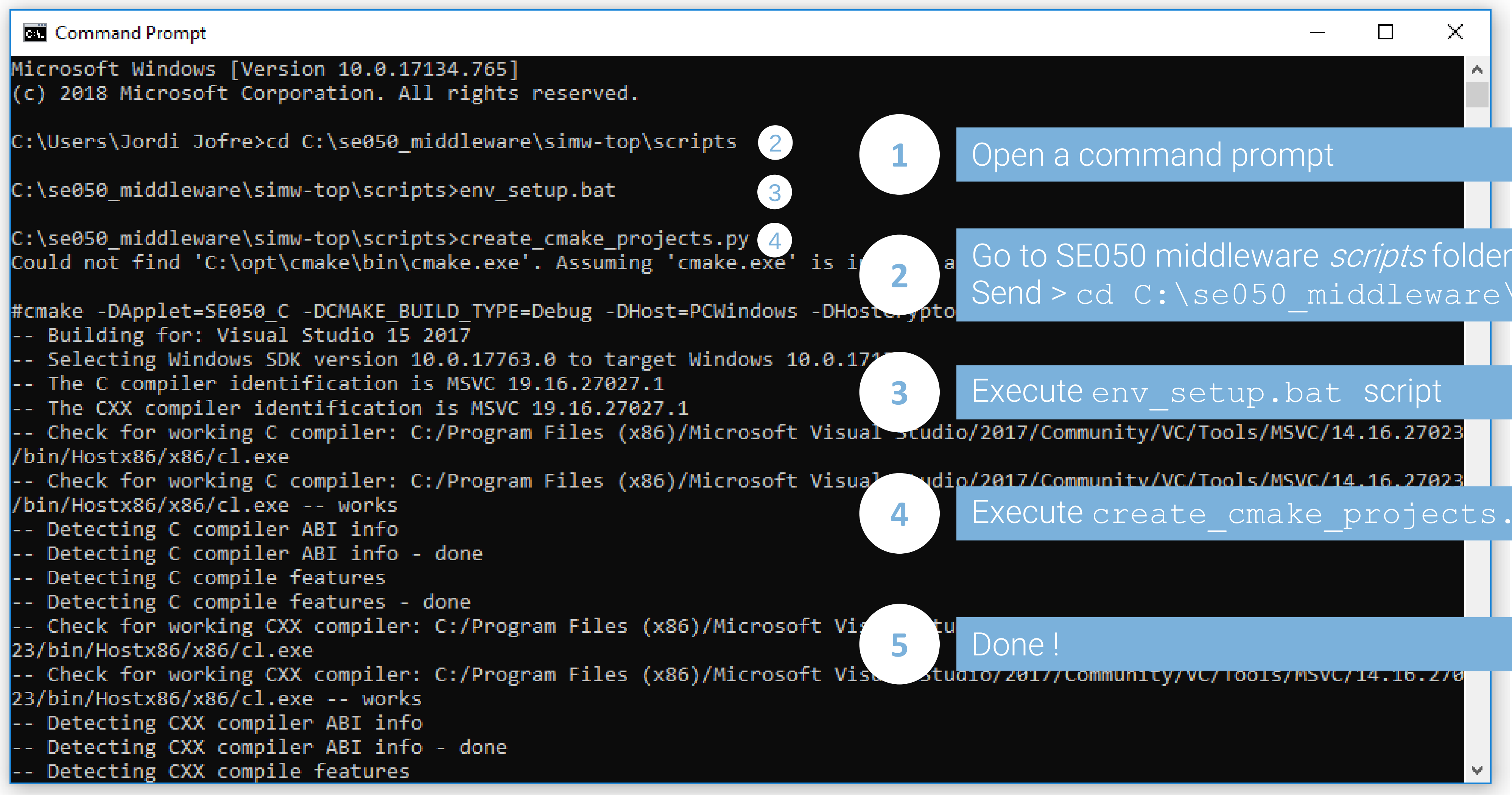
Scans for installed toolchains / build environments, sets variables and adds them to the path:

- IDE: MCUXpresso tools folder
- JAVA_HOME: Java bin folder
- PYTHON_DIR: location of Python 2.7
- CMAKE_DIR: location of CMake

Create_cmake_projects.py

Creates a build folder for each detected buildable platform and the toolchains

Build SE050 Plug & Trust middleware platform projects (II)



```
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Jordi Jofre>cd C:\se050_middleware\simw-top\scripts

C:\se050_middleware\simw-top\scripts>env_setup.bat

C:\se050_middleware\simw-top\scripts>create_cmake_projects.py
Could not find 'C:\opt\cmake\bin\cmake.exe'. Assuming 'cmake.exe' is i         a

#cmake -DApplet=SE050_C -DCMAKE_BUILD_TYPE=Debug -DHost=PCWindows -DHostCrypto
-- Building for: Visual Studio 15 2017
-- Selecting Windows SDK version 10.0.17763.0 to target Windows 10.0.171
-- The C compiler identification is MSVC 19.16.27027.1
-- The CXX compiler identification is MSVC 19.16.27027.1
-- Check for working C compiler: C:/Program Files (x86)/Microsoft Visual Studio/2017/Community/VC/Tools/MSVC/14.16.27023
/bin/Hostx86/x86/cl.exe
-- Check for working C compiler: C:/Program Files (x86)/Microsoft Visual Studio/2017/Community/VC/Tools/MSVC/14.16.27023
/bin/Hostx86/x86/cl.exe -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: C:/Program Files (x86)/Microsoft Vi          tu
23/bin/Hostx86/x86/cl.exe
-- Check for working CXX compiler: C:/Program Files (x86)/Microsoft Visu  Studio/2017/Community/VC/Tools/MSVC/14.16.270
23/bin/Hostx86/x86/cl.exe -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
```

1 Open a command prompt

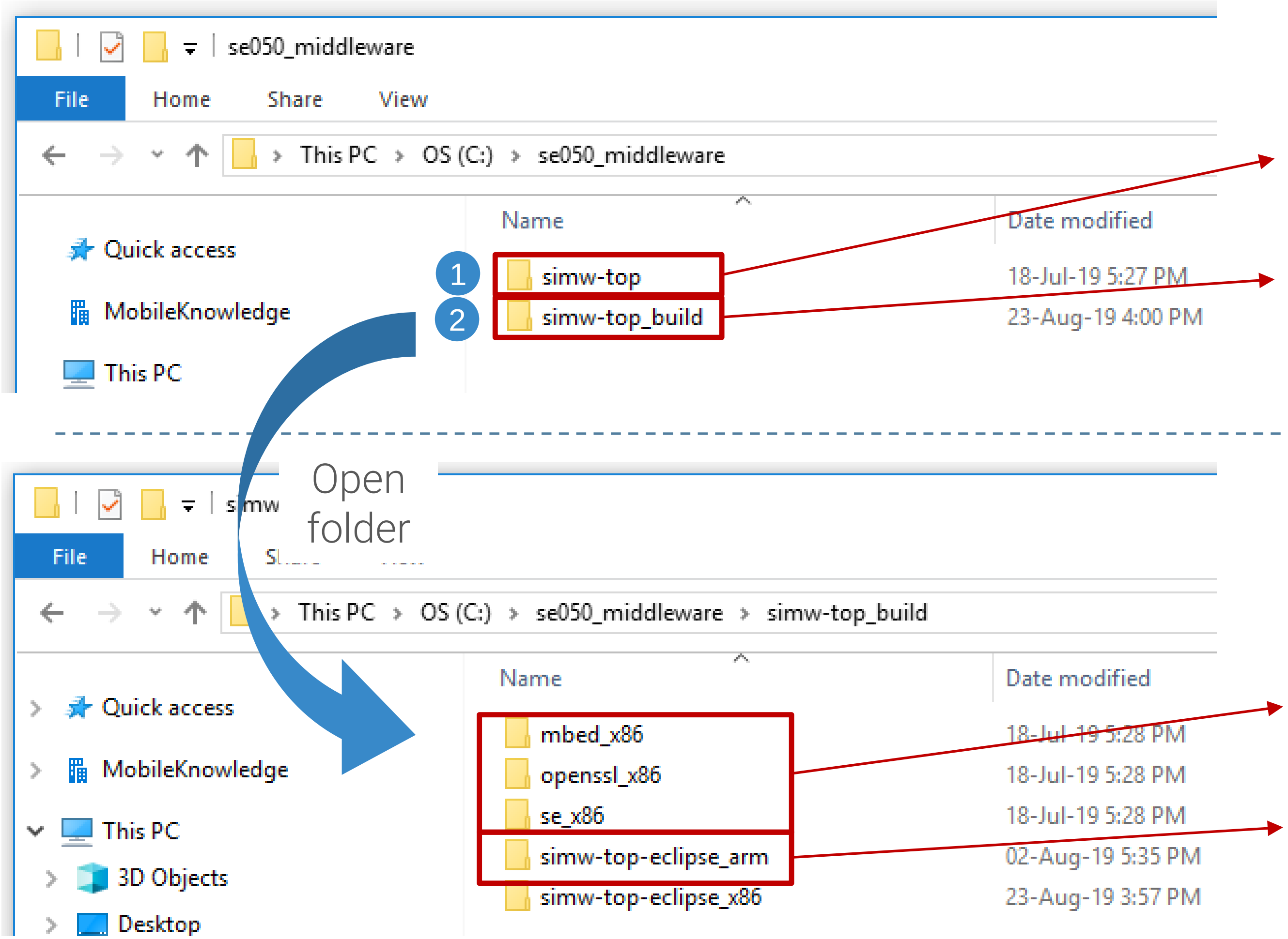
2 Go to SE050 middleware *scripts* folder.
Send > `cd C:\se050_middleware\simw-top\scripts`

3 Execute `env_setup.bat` script

4 Execute `create_cmake_projects.py` script

5 Done !

Check SE050 Plug & Trust build folder



se050_middleware

This PC › OS (C:) › se050_middleware

Name	Date modified
simw-top	18-Jul-19 5:27 PM
simw-top_build	23-Aug-19 4:00 PM

simw-top_build

This PC › OS (C:) › se050_middleware › simw-top_build

Name	Date modified
mbed_x86	18-Jul-19 5:28 PM
openssl_x86	18-Jul-19 5:28 PM
se_x86	18-Jul-19 5:28 PM
simw-top-eclipse_arm	02-Aug-19 5:35 PM
simw-top-eclipse_x86	23-Aug-19 3:57 PM

Top folder with unzipped SE050 Plug & Trust MW

Generated build-folder with platform projects

Generated MS Visual Studio projects

MCUXpresso build folder

Prepare HW

OM-SE050ARD kit contents

OM-SE050ARD board

A flexible and easy-to-use development kit for evaluation of the EdgeLock SE050 Plug & Trust product family.

OM-SE050ARD leaflet

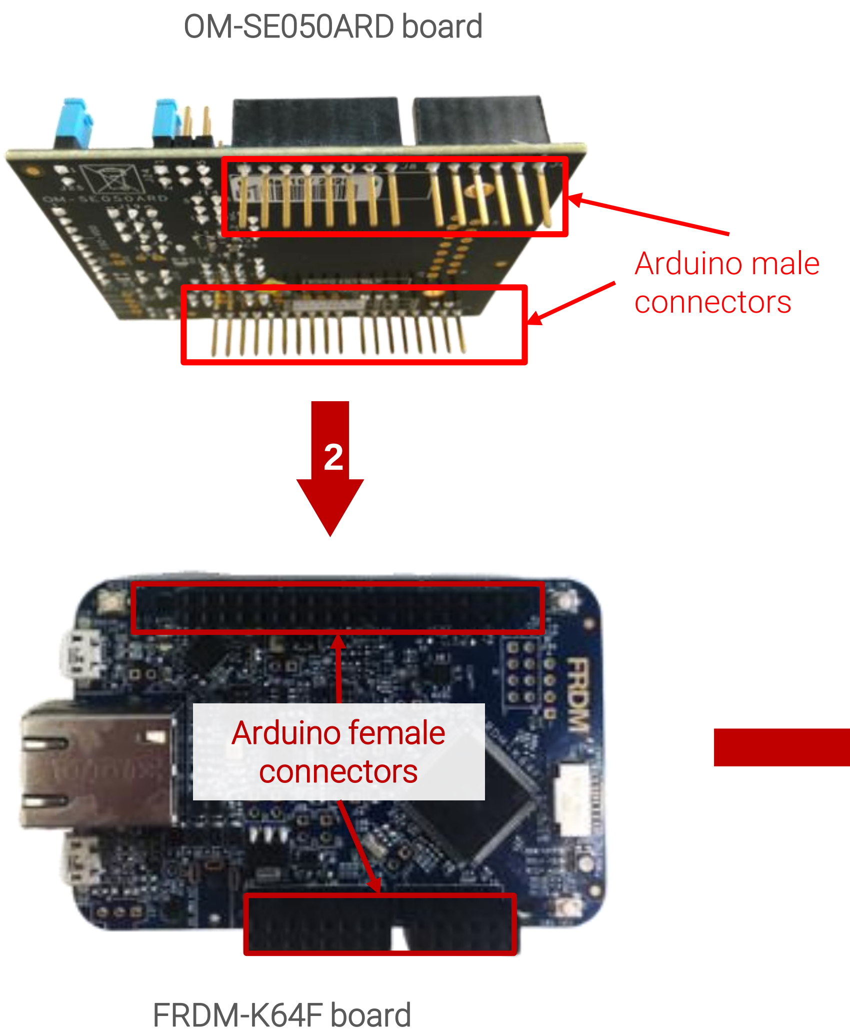
A short quick start guide describing OM-SE050ARD headers and jumper configuration

Male connectors

Four spare male connectors in case your host MCU does not included soldered Arduino header pinout.

Connector for direct I2C connection

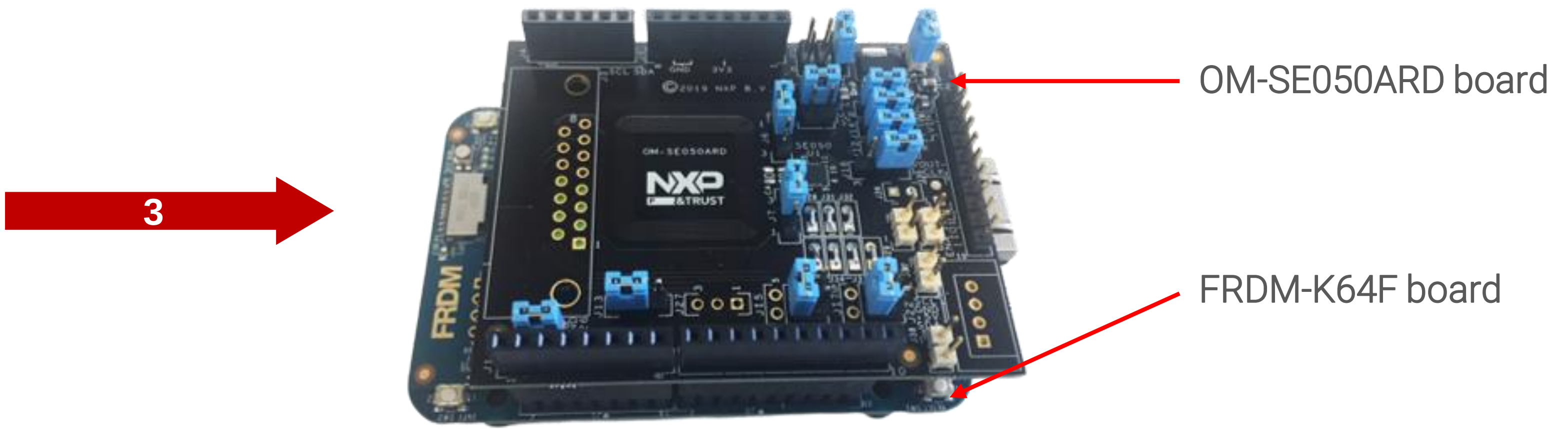
Hardware setup for FRDM-K64F



1. Disconnect the boards from your laptop (in case you have them connected).

2. Connect the OM-SE050ARD board on top of the FRDM-K64F using the Arduino headers.

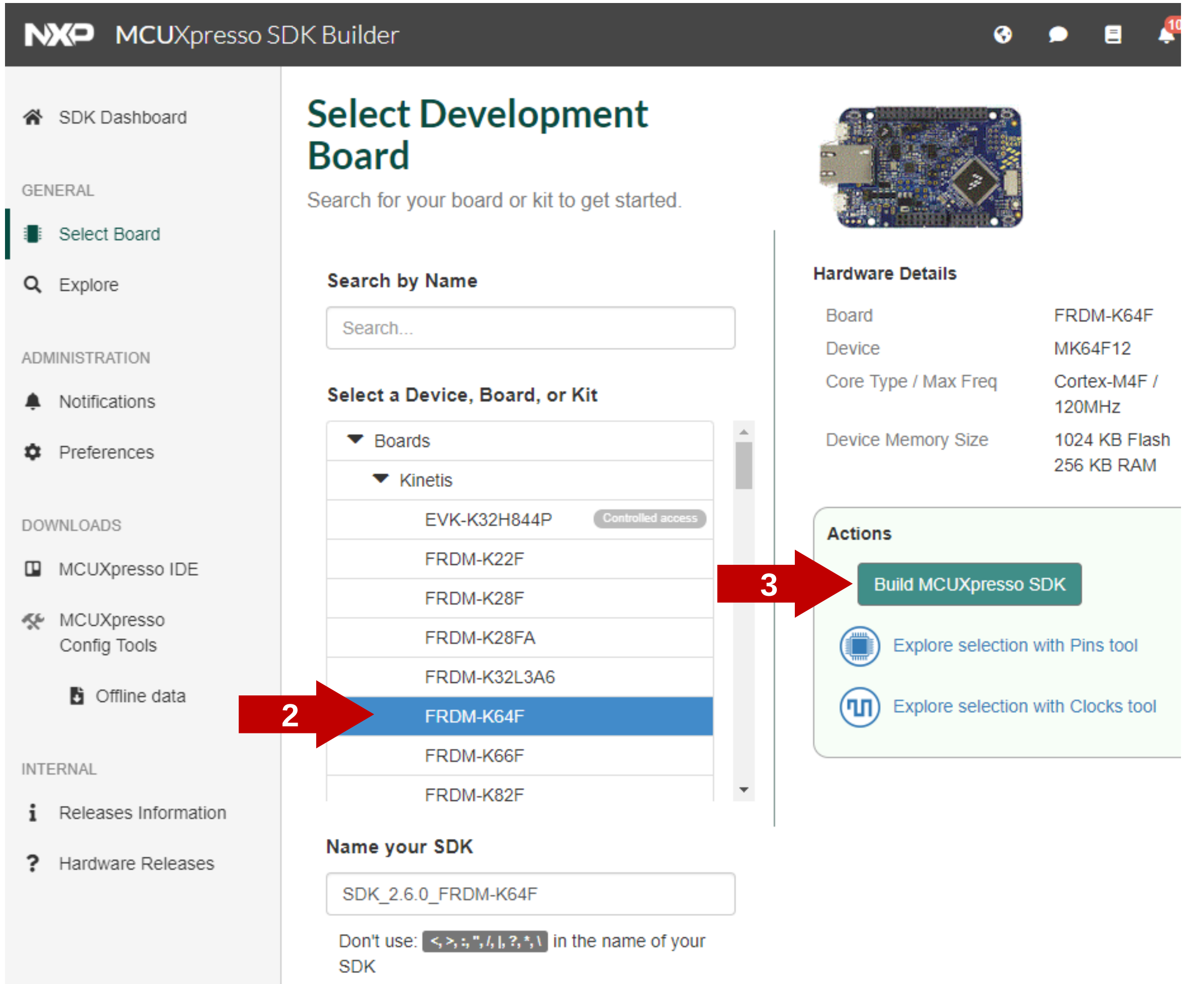
3. Double check that the two boards are connected as below:



*Check AN12396-Quick start guide with Kinetis K64 for details about OM-SE050ARD jumper configuration

Prepare MCUXpresso

Get FRDM-K64F SDK



MCUXpresso SDK Builder

- SDK Dashboard
- GENERAL
- Select Board
- Explore
- ADMINISTRATION
- Notifications
- Preferences
- DOWNLOADS
- MCUXpresso IDE
- MCUXpresso Config Tools
- Offline data
- INTERNAL
- Releases Information
- Hardware Releases

Select Development Board

Search for your board or kit to get started.

Search by Name

Search...

Select a Device, Board, or Kit

- Boards
  - Kinetis
    - EVK-K32H844P (Controlled access)
    - FRDM-K22F
    - FRDM-K28F
    - FRDM-K28FA
    - FRDM-K32L3A6
    - FRDM-K64F
    - FRDM-K66F
    - FRDM-K82F

Name your SDK

SDK_2.6.0_FRDM-K64F

Don't use: <, >, :, ", /, |, ?, *, \ in the name of your SDK

Hardware Details

Board	FRDM-K64F
Device	MK64F12
Core Type / Max Freq	Cortex-M4F / 120MHz
Device Memory Size	1024 KB Flash 256 KB RAM

Actions

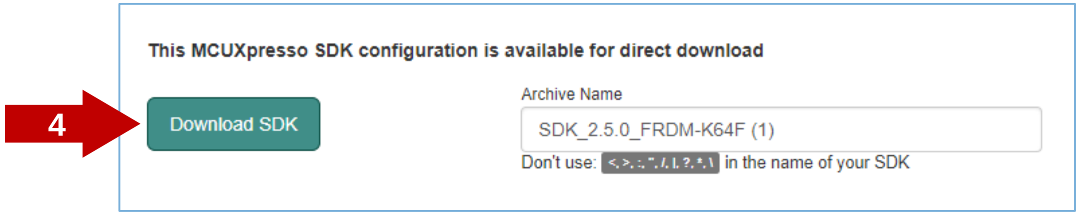
Build MCUXpresso SDK

Explore selection with Pins tool

Explore selection with Clocks tool

Generate a downloadable SDK archive for use with MCUXpresso tools:

1. Go to https://mcuxpresso.nxp.com
2. Select FRDM-K64F board from the drop-down list
3. Click Build MCUXpresso SDK button
4. In the next screen, click Download SDK button



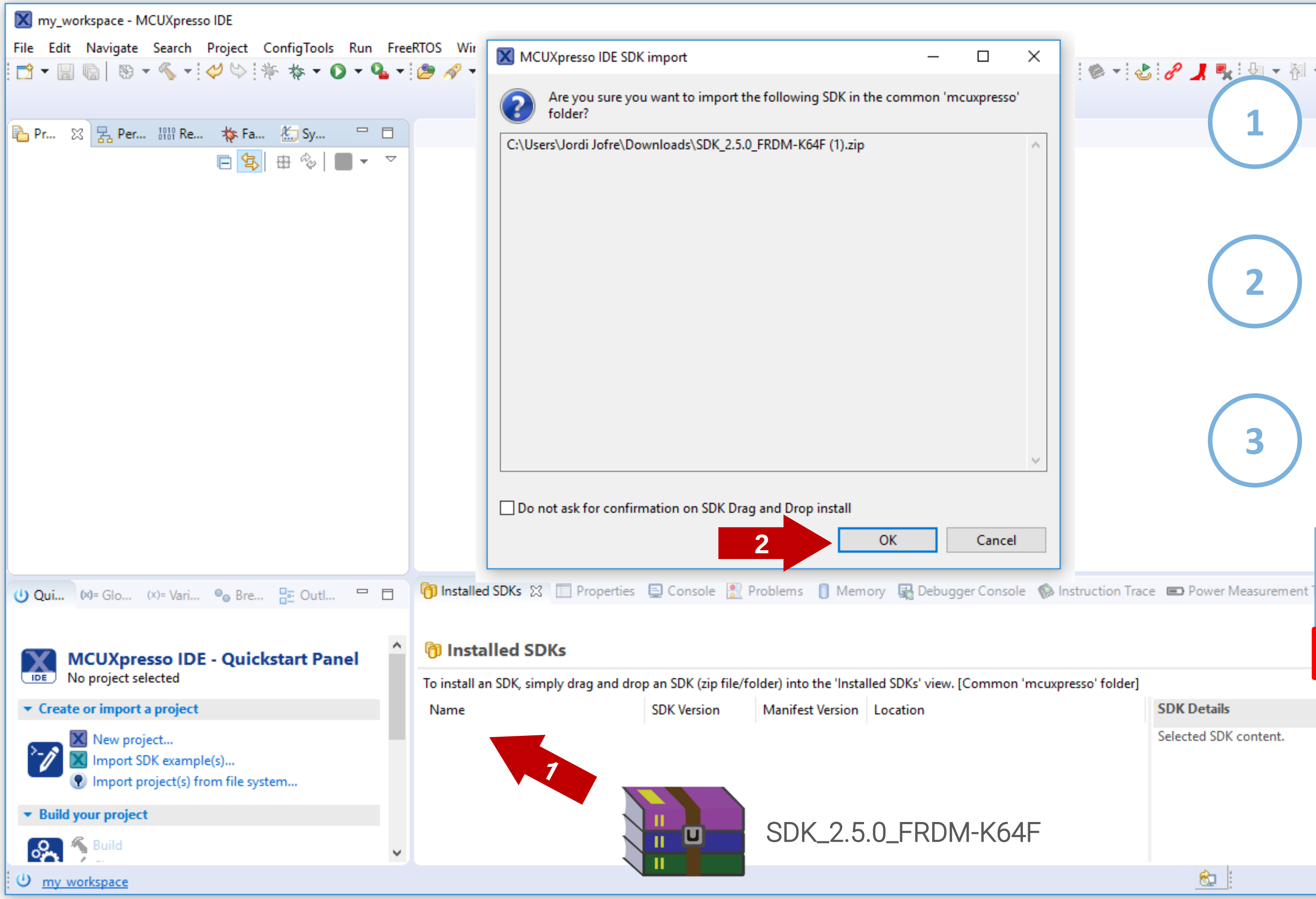
This MCUXpresso SDK configuration is available for direct download

Download SDK

Archive Name: SDK_2.5.0_FRDM-K64F (1)

Don't use: <, >, :, ", /, |, ?, *, \ in the name of your SDK

Import FRDM-K64F SDK into your MCUXpresso environment



my_workspace - MCUXpresso IDE
File Edit Navigate Search Project ConfigTools Run FreeRTOS Wir
Pr... Per... Re... Fa... Sy...
Qui... Glo... Vari... Bre... Outl...
Installed SDKs Properties Console Problems Memory Debugger Console Instruction Trace Power Measurement
my_workspace

MCUXpresso IDE SDK import

Are you sure you want to import the following SDK in the common 'mcuxpresso' folder?

C:\Users\Jordi Jofre\Downloads\SDK_2.5.0_FRDM-K64F (1).zip

☐ Do not ask for confirmation on SDK Drag and Drop install

OK Cancel

2

MCUXpresso IDE - Quickstart Panel
No project selected

- Create or import a project
  - New project...
  - Import SDK example(s)...
  - Import project(s) from file system...
- Build your project
  - Build

Installed SDKs

To install an SDK, simply drag and drop an SDK (zip file/folder) into the 'Installed SDKs' view. [Common 'mcuxpresso' folder]

Name	SDK Version	Manifest Version	Location

SDK Details
Selected SDK content.

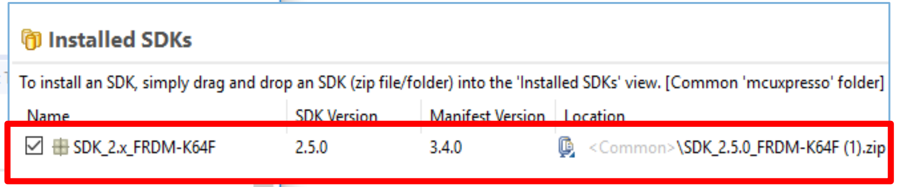
1

SDK_2.5.0_FRDM-K64F

1 Drag and drop the SDK zip file in the Installed SDKs section in the bottom part of the MCUXpresso IDE

2 Click OK in the MUCXpresso IDE SDK import window

3 Check that the SDK is successfully imported. You should see it listed in the Installed SDK window:

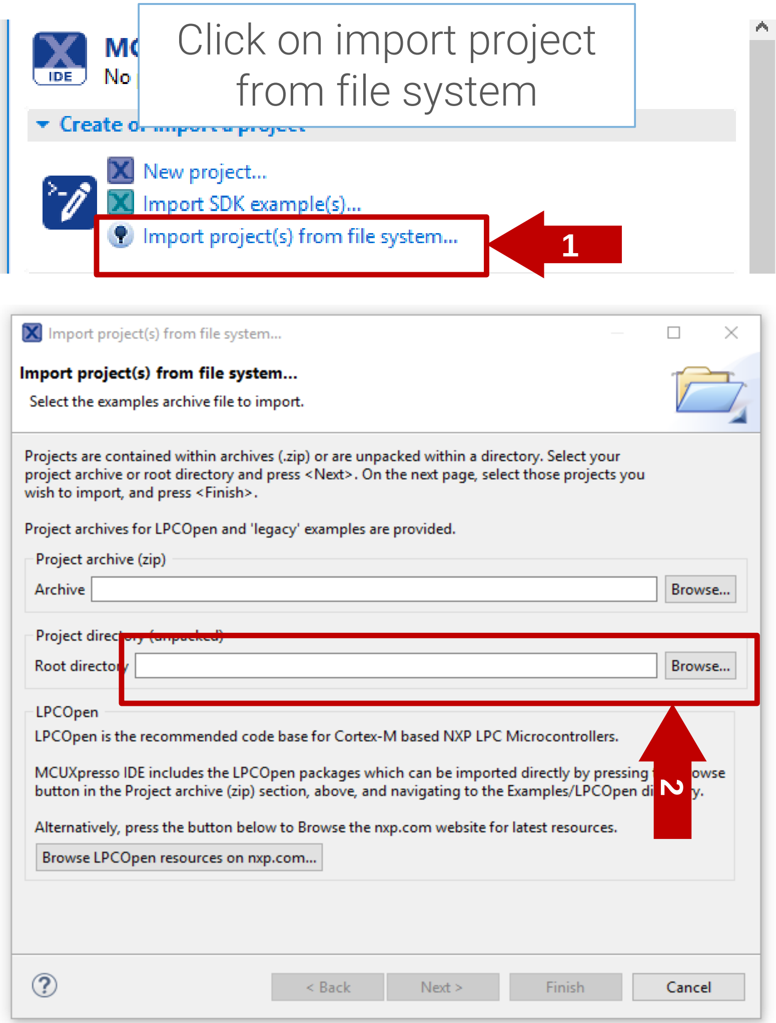


Installed SDKs

To install an SDK, simply drag and drop an SDK (zip file/folder) into the 'Installed SDKs' view. [Common 'mcuxpresso' folder]

Name	SDK Version	Manifest Version	Location
☑ SDK_2.x_FRDM-K64F	2.5.0	3.4.0	<Common>\SDK_2.5.0_FRDM-K64F (1).zip

Import project example



Click on import project from file system

MC
No
IDE
Create or import a project
New project...
Import SDK example(s)...
Import project(s) from file system...
1
2

Import project(s) from file system...

Import project(s) from file system...

Select the examples archive file to import.

Projects are contained within archives (.zip) or are unpacked within a directory. Select your project archive or root directory and press <Next>. On the next page, select those projects you wish to import, and press <Finish>.

Project archives for LPCOpen and 'legacy' examples are provided.

Project archive (zip)

Archive Browse...

Project directory (unpacked)

Root directory Browse...

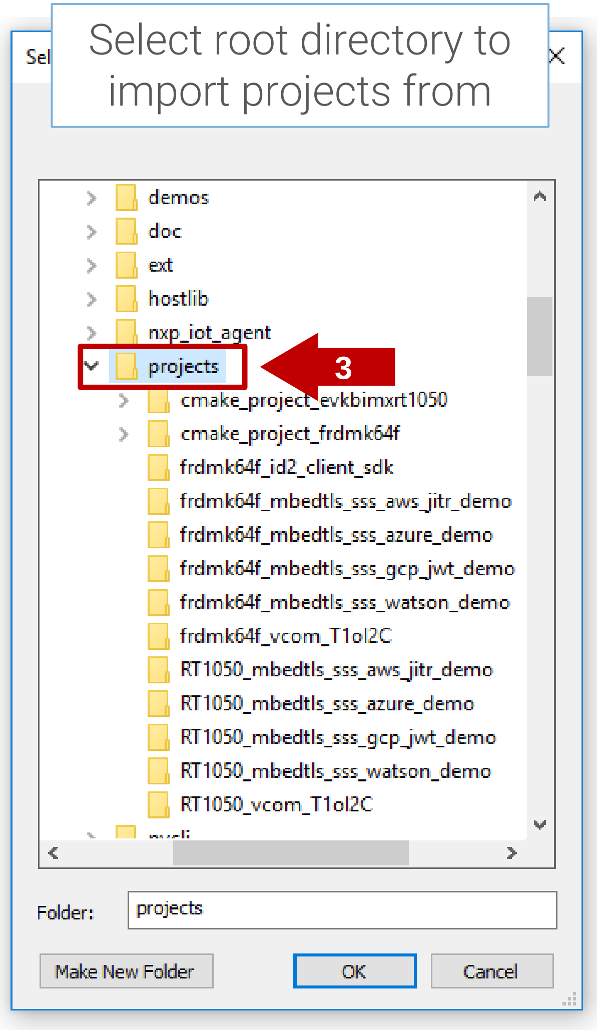
LPCOpen

LPCOpen is the recommended code base for Cortex-M based NXP LPC Microcontrollers.

MCUXpresso IDE includes the LPCOpen packages which can be imported directly by pressing the Browse button in the Project archive (zip) section, above, and navigating to the Examples/LPCOpen directory.

Alternatively, press the button below to Browse the nxp.com website for latest resources.

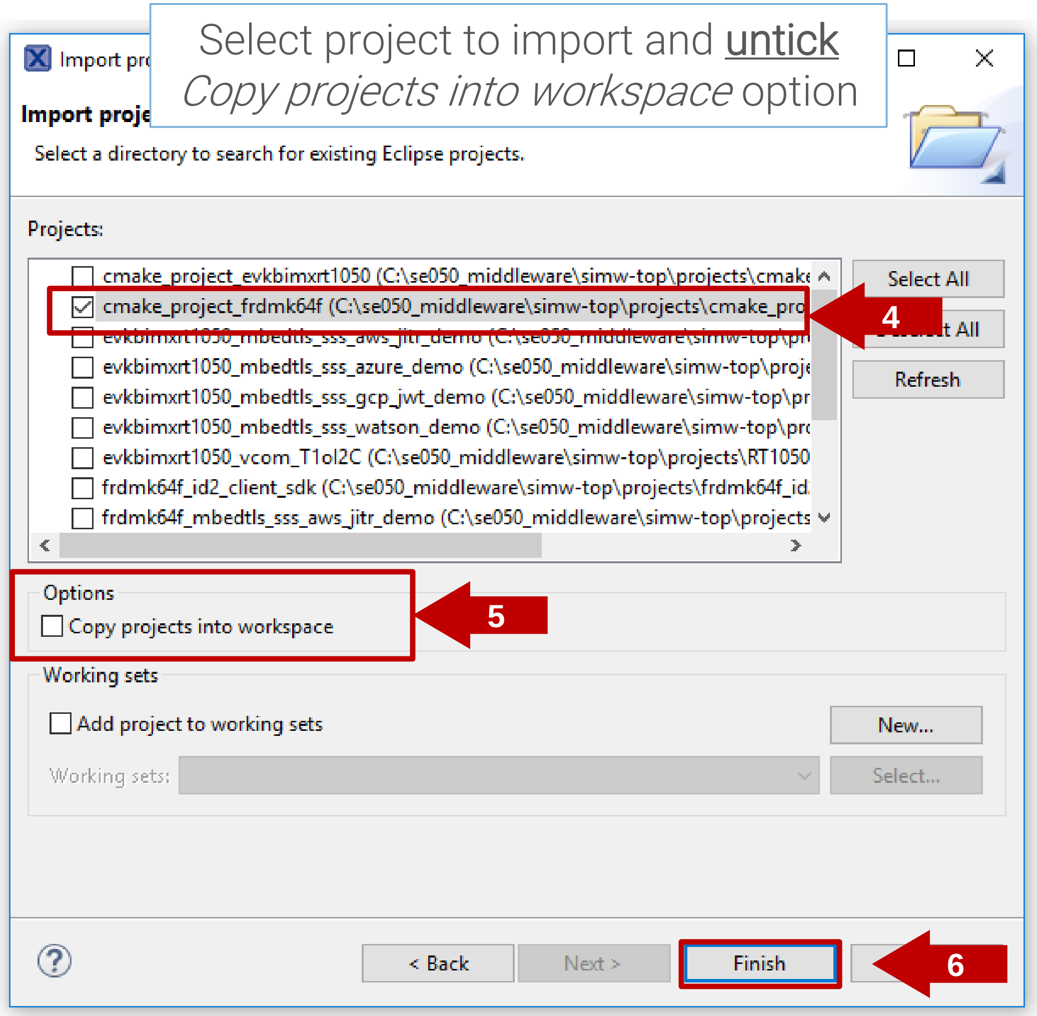
Browse LPCOpen resources on nxp.com...
< Back
Next >
Finish
Cancel



Select root directory to import projects from

Sel
demos
doc
ext
hostlib
nxp_iot_agent
projects
3
cmake_project_evkbimxrt1050
cmake_project_frdmk64f
frdmk64f_id2_client_sdk
frdmk64f_mbedtls_sss_aws_jitr_demo
frdmk64f_mbedtls_sss_azure_demo
frdmk64f_mbedtls_sss_gcp_jwt_demo
frdmk64f_mbedtls_sss_watson_demo
frdmk64f_vcom_T1ol2C
RT1050_mbedtls_sss_aws_jitr_demo
RT1050_mbedtls_sss_azure_demo
RT1050_mbedtls_sss_gcp_jwt_demo
RT1050_mbedtls_sss_watson_demo
RT1050_vcom_T1ol2C
Make New Folder
OK
Cancel

Folder: projects



Select project to import and untick *Copy projects into workspace* option

Import pro

Import proje

Select a directory to search for existing Eclipse projects.

Projects:

- □ cmake_project_evkbimxrt1050 (C:\se050_middleware\simw-top\projects\cmake
- ☑ cmake_project_frdmk64f (C:\se050_middleware\simw-top\projects\cmake_pro
- □ evkbimxrt1050_mbedtls_sss_aws_jitr_demo (C:\se050_middleware\simw-top\pr
- □ evkbimxrt1050_mbedtls_sss_azure_demo (C:\se050_middleware\simw-top\proje
- □ evkbimxrt1050_mbedtls_sss_gcp_jwt_demo (C:\se050_middleware\simw-top\pr
- □ evkbimxrt1050_mbedtls_sss_watson_demo (C:\se050_middleware\simw-top\pro
- □ evkbimxrt1050_vcom_T1ol2C (C:\se050_middleware\simw-top\projects\RT1050
- □ frdmk64f_id2_client_sdk (C:\se050_middleware\simw-top\projects\frdmk64f_id
- □ frdmk64f_mbedtls_sss_aws_jitr_demo (C:\se050_middleware\simw-top\projects

Options

□ Copy projects into workspace

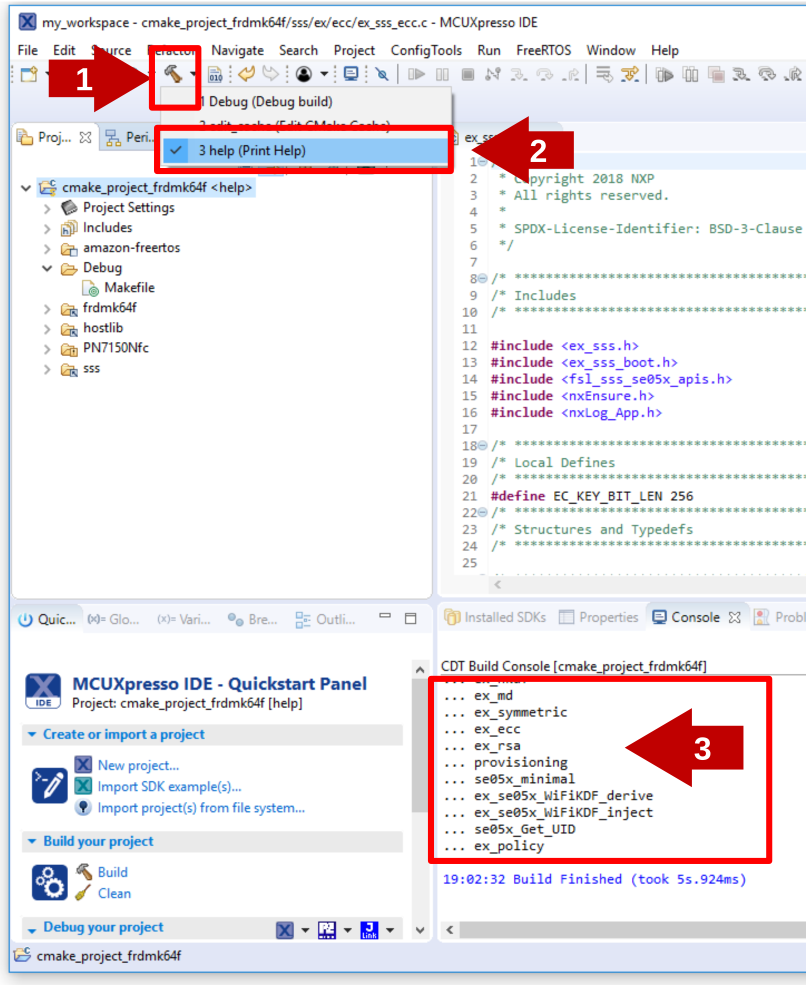
Working sets

□ Add project to working sets

Working sets:

Run examples

SE050 Plug & Trust middleware test examples


my_workspace - cmake_project_frdmk64f/sss/ex/ecc/ex_sss_ecc.c - MCUXpresso IDE
File Edit Source Refactor Navigate Search Project ConfigTools Run FreeRTOS Window Help
1
1 Debug (Debug build)
2 edit_cache (Edit CMake Cache)
3 help (Print Help)
2
cmake_project_frdmk64f <help>
Project Settings
Includes
amazon-freertos
Debug
Makefile
frdmk64f
hostlib
PN7150Nfc
sss
Quic... Glo... Vari... Bre... Outli...
Installed SDKs Properties Console Probl
MCUXpresso IDE - Quickstart Panel
Project: cmake_project_frdmk64f [help]
Create or import a project
New project...
Import SDK example(s)...
Import project(s) from file system...
Build your project
Build
Clean
Debug your project
cmake_project_frdmk64f
3

```
/*
 * Copyright 2018 NXP
 * All rights reserved.
 *
 * SPDX-License-Identifier: BSD-3-Clause
 */

/* ***************************************
/* Includes
/* ***************************************

#include <ex_sss.h>
#include <ex_sss_boot.h>
#include <fsl_sss_se05x_apis.h>
#include <nxEnsure.h>
#include <nxLog_App.h>

/* ***************************************
/* Local Defines
/* ***************************************
#define EC_KEY_BIT_LEN 256
/* ***************************************
/* Structures and Typedefs
/* ***************************************
```

CDT Build Console [cmake_project_frdmk64f]

```
... ex_md
... ex_symmetric
... ex_ecc
... ex_rsa
... provisioning
... se05x_minimal
... ex_se05x_WiFiKDF_derive
... ex_se05x_WiFiKDF_inject
... se05x_Get_UID
... ex_policy

19:02:32 Build Finished (took 5s.924ms)
```

The SE050 Plug & Trust MW comes with several test examples used to verify atomic SE050 security IC features.

... se05x_Get_Info: Gets SE050 system info (e.g. applet version)

... se05x_minimal: Gets free memory from SE050

... ex_ecc: Performs ECC signing and verify operation

... ex_rsa: Performs ECC signing and verify operation

... ex_symmetric: Performs AES encryption and decryption operation.

... ex_md: Performs Message Digest hashing operation

... ex_policy: demonstrate the use of policies for secure objects

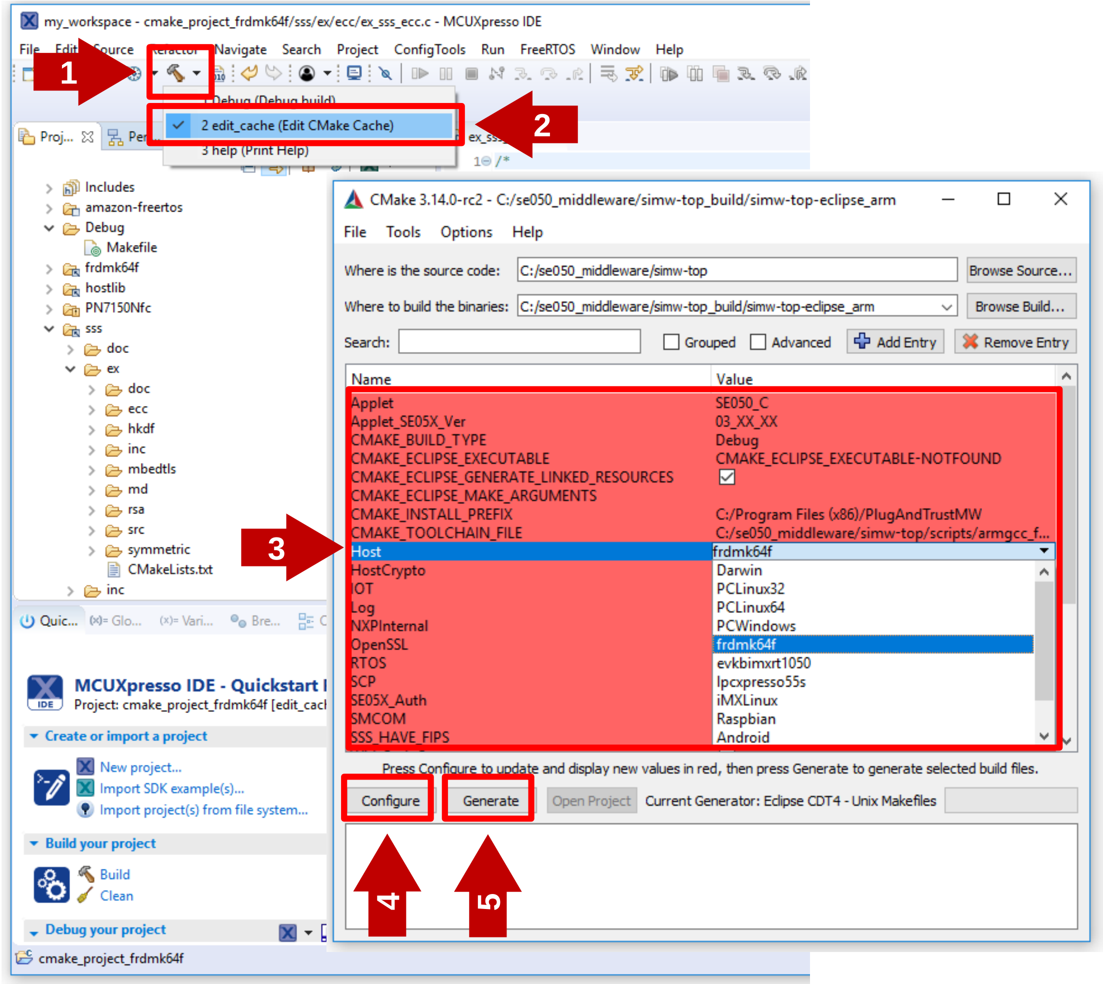
... ex_hkdf: Performs HMAC Key derivation operation.

And more...

Described in SE050 Plug & Trust MW HTML documentation:
`simwtop/doc/demos.html`

PLUG&TRUST

Edit CMake options


my_workspace - cmake_project_frdmk64f/sss/ex/ecc/ex_sss_ecc.c - MCUXpresso IDE
File Edit Source Refactor Navigate Search Project ConfigTools Run FreeRTOS Window Help
1
Debug (Debug build)
2 edit_cache (Edit CMake Cache)
3 help (Print Help)
2
Includes
amazon-freertos
Debug
Makefile
frdmk64f
hostlib
PN7150Nfc
sss
doc
ex
doc
ecc
hkdf
inc
mbedtls
md
rsa
src
symmetric
CMakeLists.txt
inc
3
MCUXpresso IDE - Quickstart
Project: cmake_project_frdmk64f [edit_cac
Create or import a project
New project...
Import SDK example(s)...
Import project(s) from file system...
Build your project
Build
Clean
Debug your project
cmake_project_frdmk64f
CMake 3.14.0-rc2 - C:/se050_middleware/simw-top_build/simw-top-eclipse_arm
File Tools Options Help
Browse Source...
Browse Build...
☐ Grouped ☐ Advanced
Add Entry
Remove Entry
Configure
Generate
Open Project
4
5

Where is the source code: C:/se050_middleware/simw-top

Where to build the binaries: C:/se050_middleware/simw-top_build/simw-top-eclipse_arm

Search:

Name	Value
Applet	SE050_C
Applet_SE05X_Ver	03_XX_XX
CMAKE_BUILD_TYPE	Debug
CMAKE_ECLIPSE_EXECUTABLE	CMAKE_ECLIPSE_EXECUTABLE-NOTFOUND
CMAKE_ECLIPSE_GENERATE_LINKED_RESOURCES	☑
CMAKE_ECLIPSE_MAKE_ARGUMENTS	
CMAKE_INSTALL_PREFIX	C:/Program Files (x86)/PlugAndTrustMW
CMAKE_TOOLCHAIN_FILE	C:/se050_middleware/simw-top/scripts/armgcc_f...
Host	frdmk64f
HostCrypto	Darwin
IOT	PCLinux32
Log	PCLinux64
NXPInternal	PCWindows
OpenSSL	frdmk64f
RTOS	evkbimxrt1050
SCP	lpcxpresso55s
SE05X_Auth	iMXLinux
SMCOM	Raspbian
SSS_HAVE_FIPS	Android

Press Configure to update and display new values in red, then press Generate to generate selected build files.

Current Generator: Eclipse CDT4 - Unix Makefiles

CMake configuration files are used to enable or disable several features, portability and setting flags to generate the build files for your platform and native build environment.

1 Click on the arrow on the "**hammer**" icon

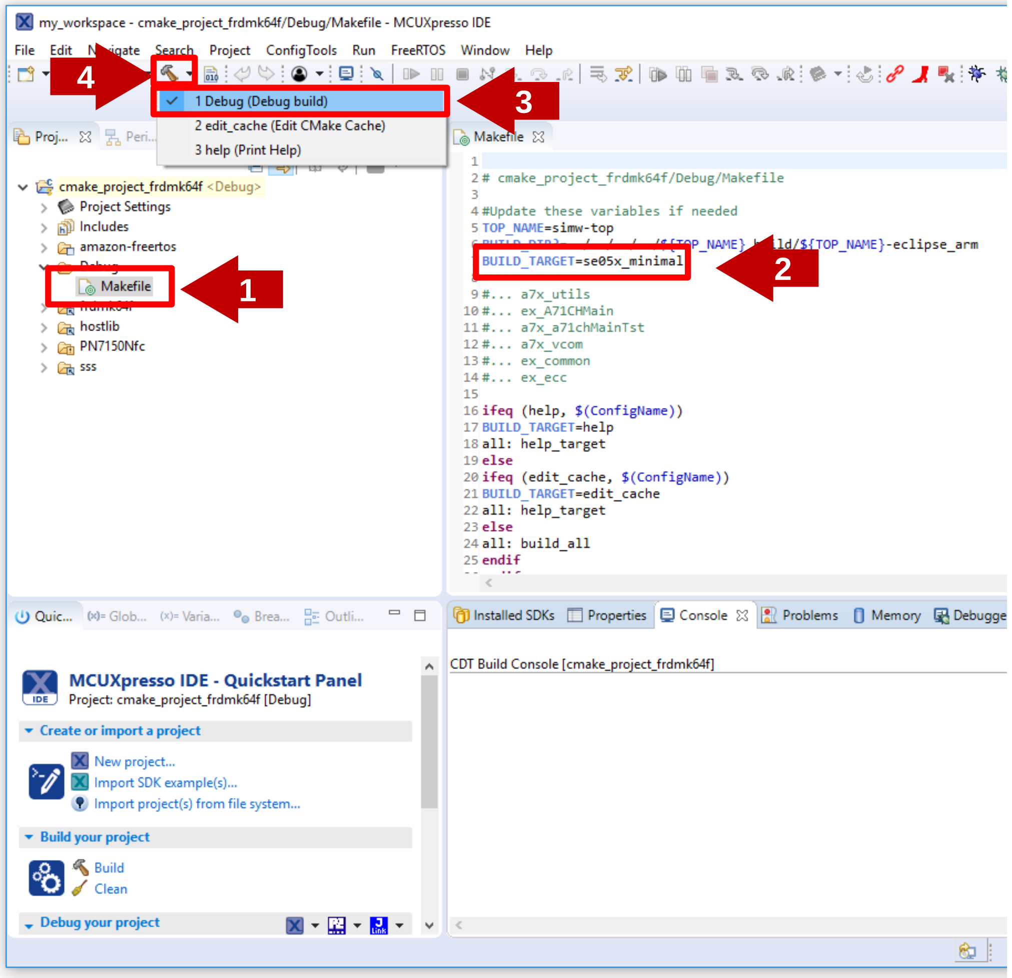
2 Select **2 edit_cache**

3 Use the **CMake GUI** window to change CMake options

4 Click on **Configure** button

5 Click on **Generate** button

Define the test example to be executed



my_workspace - cmake_project_frdmk64f/Debug/Makefile - MCUXpresso IDE
File Edit Navigate Search Project ConfigTools Run FreeRTOS Window Help
4
✓ 1 Debug (Debug build)
2 edit_cache (Edit CMake Cache)
3 help (Print Help)
3
Proj... Peri...
cmake_project_frdmk64f <Debug>
Project Settings
Includes
amazon-freertos
Debug
Makefile
1
frdmk64f
hostlib
PN7150Nfc
sss
Makefile
2
Quic... Glob... Varia... Brea... Outli...
Installed SDKs Properties Console Problems Memory Debugger
CDT Build Console [cmake_project_frdmk64f]
MCUXpresso IDE - Quickstart Panel
Project: cmake_project_frdmk64f [Debug]
Create or import a project
New project...
Import SDK example(s)...
Import project(s) from file system...
Build your project
Build
Clean
Debug your project

```

# cmake_project_frdmk64f/Debug/Makefile

#Update these variables if needed
TOP_NAME=simw-top
BUILD_DIR?=../../../${TOP_NAME}_build/${TOP_NAME}-eclipse_arm
BUILD_TARGET=se05x_minimal

#... a7x_utils
#... ex_A71CHMain
#... a7x_a71chMainTst
#... a7x_vcom
#... ex_common
#... ex_ecc

ifeq (help, $(ConfigName))
BUILD_TARGET=help
all: help_target
else
ifeq (edit_cache, $(ConfigName))
BUILD_TARGET=edit_cache
all: help_target
else
all: build_all
endif
```

Select the se05x_minimal as the project to be executed. For that, follow the steps

1 Go to Debug folder and open the **Makefile** file.

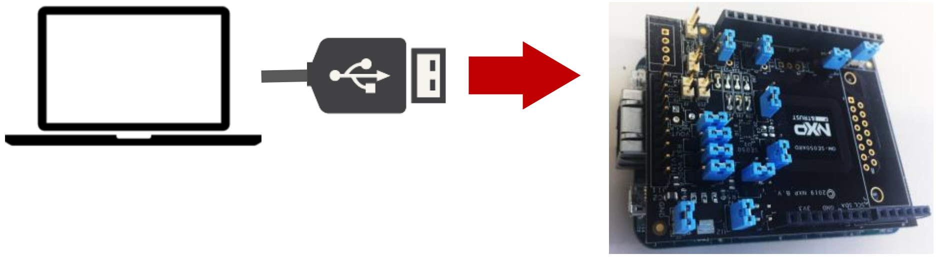
2 Write the name of the project to be executed in the **BUILD_TARGET** variable (e.g. se05x_minimal)

3 Click on the arrow on the "**hammer**" icon

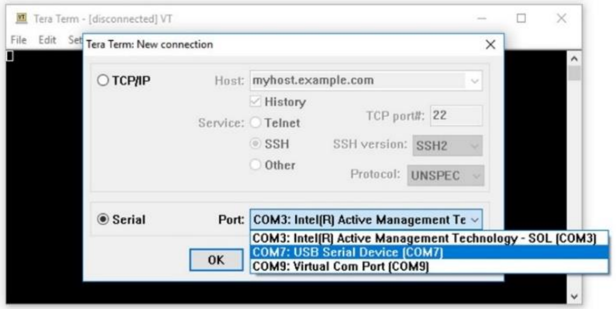
4 Select **1 Debug (Debug build).**

Run test example

1 Connect the FRDM-K64F board to your laptop



2 Configure TeraTerm

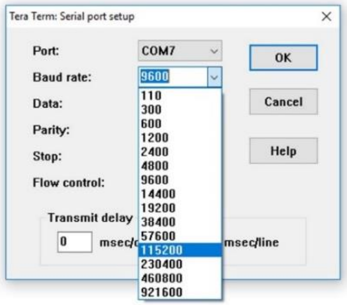


Tera Term: New connection

○ TCP/IP Host: myhost.example.com
☑ History
Service: ○ Telnet TCP port#: 22
● SSH SSH version: SSH2
○ Other Protocol: UNSPEC

● Serial Port: COM3: Intel(R) Active Management Te
COM3: Intel(R) Active Management Technology - SOL (COM3)
COM7: USB Serial Device (COM7)
COM9: Virtual Com Port (COM9)

OK

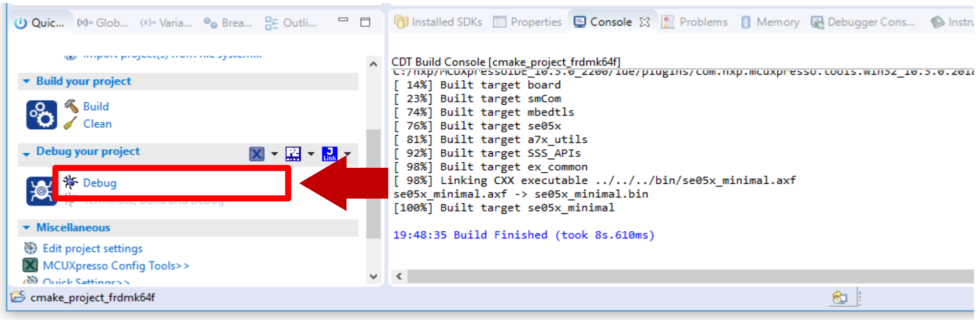


Tera Term: Serial port setup

Port: COM7
Baud rate: 9600
Data:
Parity:
Stop:
Flow control:
Transmit delay
0 msec/c msec/line

110
300
600
1200
2400
4800
9600
14400
19200
38400
57600
115200
230400
460800
921600

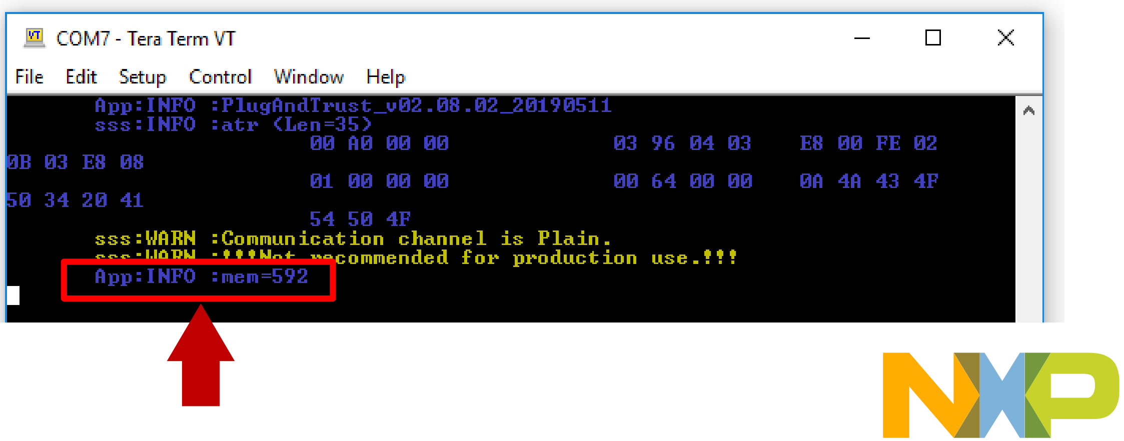
3 Click MCUXpresso Quickstart Panel Debug button


Quic... Glob... Varia... Brea... Outli...
Installed SDKs Properties Console Problems Memory Debugger Cons... Instru
Build your project
Build
Clean
Debug your project
Debug
Miscellaneous
Edit project settings
MCUXpresso Config Tools>>
Quick Settings>>
cmake_project_frdmk64f

CDT Build Console [cmake_project_frdmk64f]

```
C:/nxp/MCUXpressoIDE_10.3.0_2200/ide/plugins/com.nxp.mcuxpresso.tools.win32_10.3.0.201
[ 14%] Built target board
[ 23%] Built target smCom
[ 74%] Built target mbedtls
[ 76%] Built target se05x
[ 81%] Built target a7x_utils
[ 92%] Built target SSS_APIs
[ 98%] Built target ex_common
[ 98%] Linking CXX executable ../../../bin/se05x_minimal.axf
se05x_minimal.axf -> se05x_minimal.bin
[100%] Built target se05x_minimal

19:48:35 Build Finished (took 8s.610ms)
```

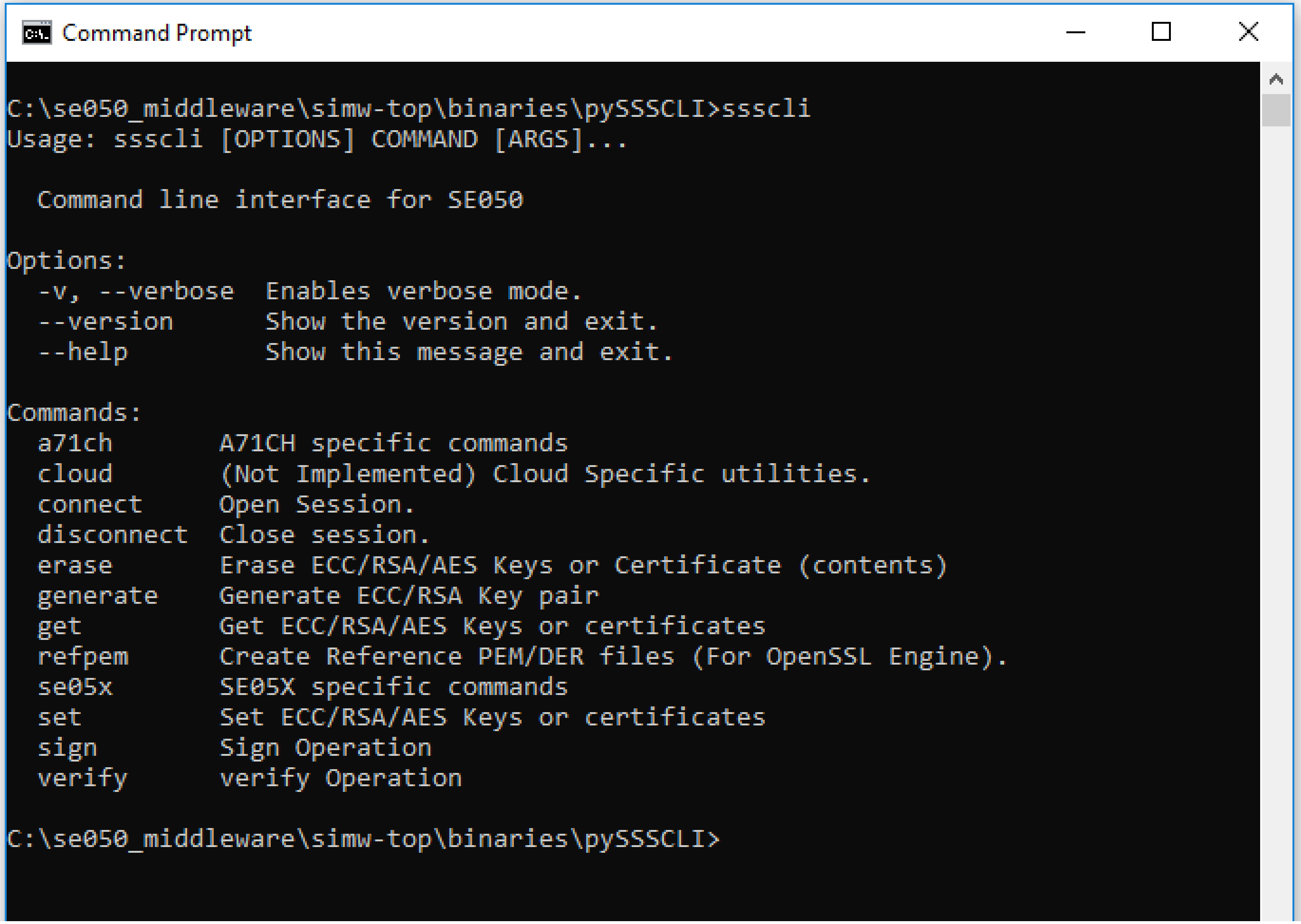
4 The project example is now running in. Check TeraTerm



```
        App:INFO :PlugAndTrust_v02.08.02_20190511
        sss:INFO :atr (Len=35)
                  00 A0 00 00          03 96 04 03    E8 00 FE 02
0B 03 E8 08
                  01 00 00 00          00 64 00 00    0A 4A 43 4F
50 34 20 41
                  54 50 4F
        sss:WARN :Communication channel is Plain.
        sss:WARN :!!!Not recommended for production use.!!!
        App:INFO :mem=592
```

pySSSCLI tool

pySSSCLI tool overview



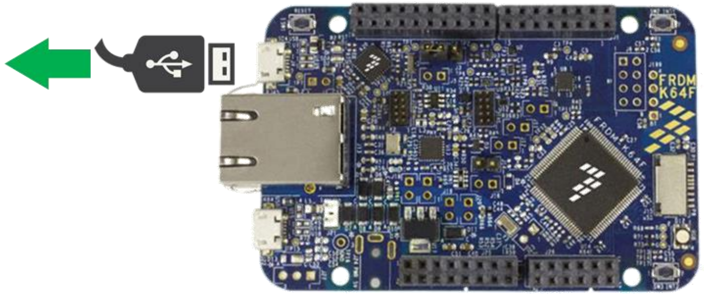
```
C:\se050_middleware\simw-top\binaries\pySSSCLI>ssscli
Usage: ssscli [OPTIONS] COMMAND [ARGS]...

  Command line interface for SE050

Options:
  -v, --verbose  Enables verbose mode.
  --version      Show the version and exit.
  --help         Show this message and exit.

Commands:
  a71ch       A71CH specific commands
  cloud       (Not Implemented) Cloud Specific utilities.
  connect     Open Session.
  disconnect  Close session.
  erase       Erase ECC/RSA/AES Keys or Certificate (contents)
  generate    Generate ECC/RSA Key pair
  get         Get ECC/RSA/AES Keys or certificates
  refpem      Create Reference PEM/DER files (For OpenSSL Engine).
  se05x       SE05X specific commands
  set         Set ECC/RSA/AES Keys or certificates
  sign        Sign Operation
  verify      verify Operation

C:\se050_middleware\simw-top\binaries\pySSSCLI>
```

- A command line tool able to insert keys and credentials inside the SE050.
- It is written in Python.
- It is meant for evaluation, development and testing phases.
- Supports complex provisioning scripts to be run on Windows, Linux, OS X and other embedded devices.
- Comes pre-compiled in SE050 Plug & Trust MW. Only requires to flash the VCOM software on the MCU board.

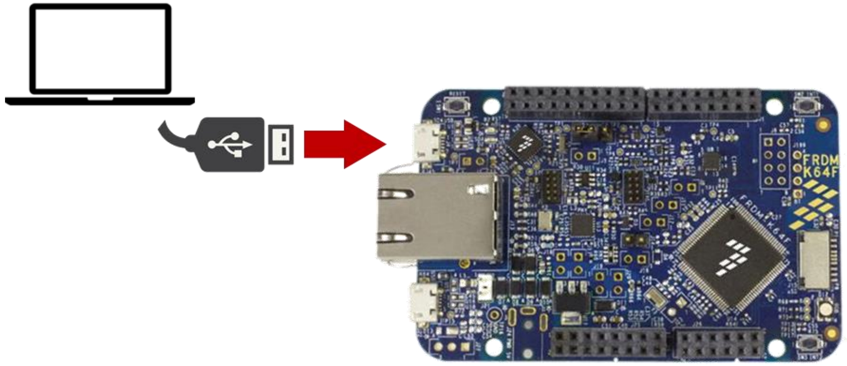
Further documentation about the commands:
`simw-top/doc/cli-tool.html`

Flash FRDM-K64F with VCOM software

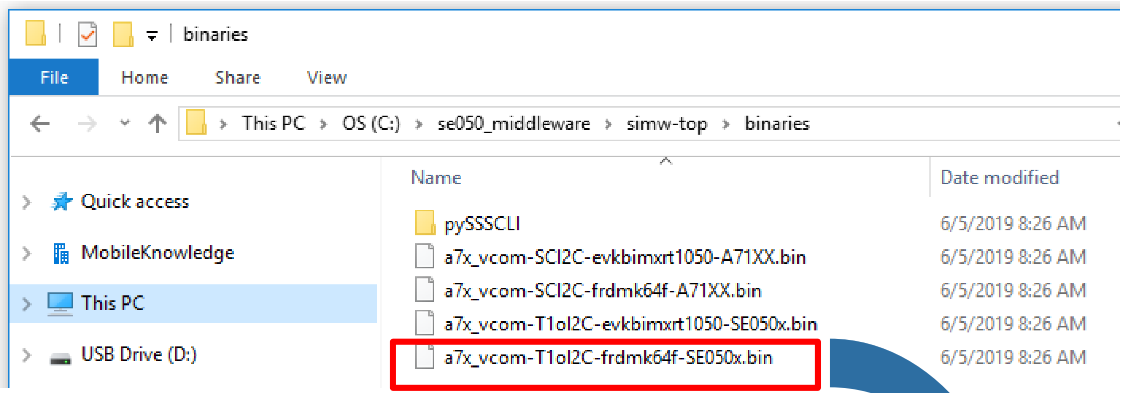
1 Unplug OpenSDA port



2 Plug OpenSDA port



3 Copy The VCOM software binary from the `simw-top\binaries`



binaries

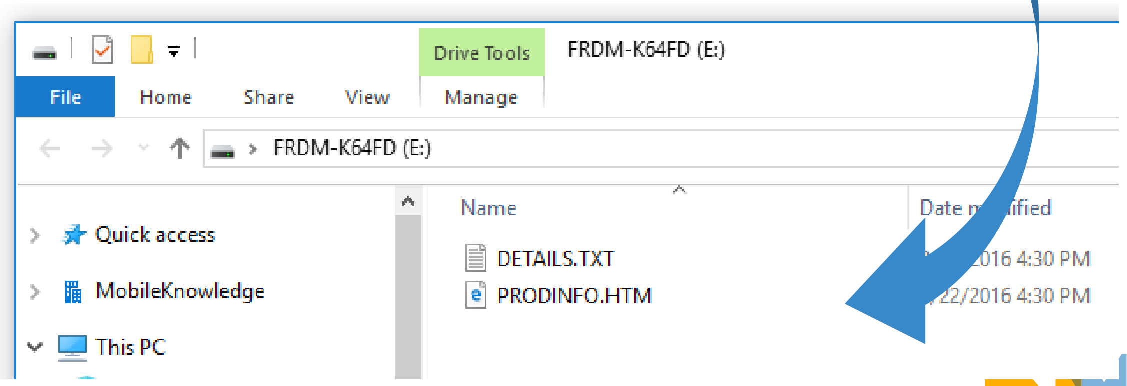
File Home Share View

This PC › OS (C:) › se050_middleware › simw-top › binaries

Quick access
MobileKnowledge
This PC
USB Drive (D:)

Name	Date modified
pySSSCLI	6/5/2019 8:26 AM
a7x_vcom-SCI2C-evkbimxrt1050-A71XX.bin	6/5/2019 8:26 AM
a7x_vcom-SCI2C-frdmk64f-A71XX.bin	6/5/2019 8:26 AM
a7x_vcom-T1oI2C-evkbimxrt1050-SE050x.bin	6/5/2019 8:26 AM
a7x_vcom-T1oI2C-frdmk64f-SE050x.bin	6/5/2019 8:26 AM

4 Paste the binary file into the FRDM-K64F mass storage drive



Drive Tools FRDM-K64FD (E:)

File Home Share View Manage

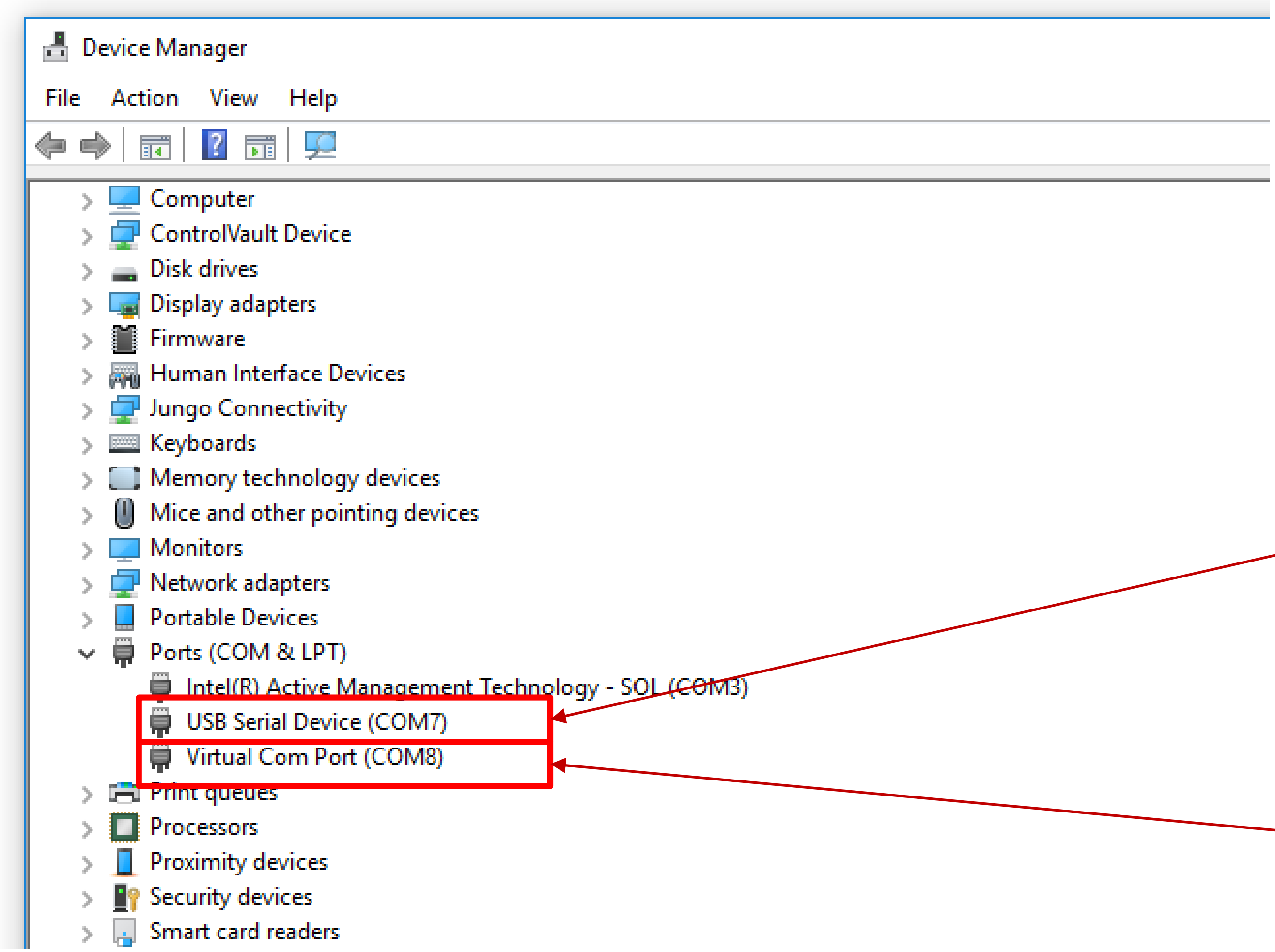
FRDM-K64FD (E:)

Quick access
MobileKnowledge
This PC

Name	Date modified
DETAILS.TXT	2016 4:30 PM
PRODINFO.HTM	22/2016 4:30 PM

PLUG&TRUST

Flash FRDM-K64F with VCOM software (II)



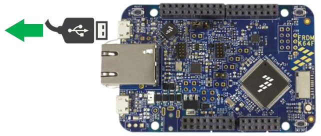
Device Manager

File Action View Help

- Computer
- ControlVault Device
- Disk drives
- Display adapters
- Firmware
- Human Interface Devices
- Jungo Connectivity
- Keyboards
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Portable Devices
- Ports (COM & LPT)
  - Intel(R) Active Management Technology - SOL (COM3)
  - USB Serial Device (COM7)
  - Virtual Com Port (COM8)
- Print queues
- Processors
- Proximity devices
- Security devices
- Smart card readers

Check that the VCOM port is recognized in your Device Manager (category Ports (COM & LTP)

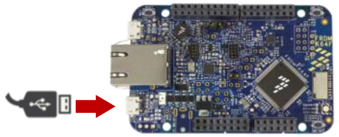
1 Unplug OpenSDA port



2 Plug OpenSDA port

3 Check serial port *

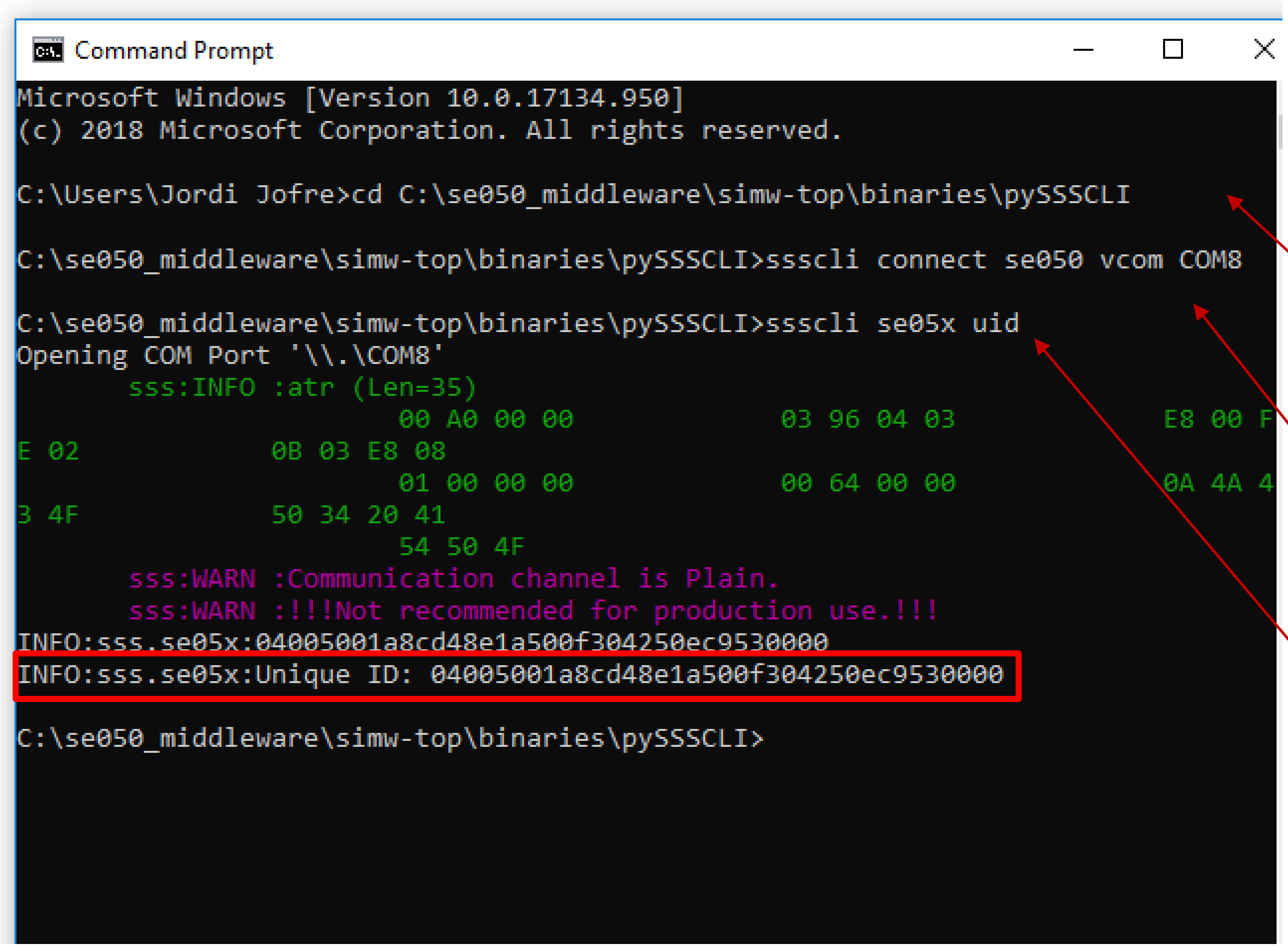
4 Plug K64F port



5 Check VCOM port *

* Port naming might change depending on the computer

Use of the pre-compiled pySSSCLI



```
Microsoft Windows [Version 10.0.17134.950]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Jordi Jofre>cd C:\se050_middleware\simw-top\binaries\pySSSCLI

C:\se050_middleware\simw-top\binaries\pySSSCLI>ssscli connect se050 vcom COM8

C:\se050_middleware\simw-top\binaries\pySSSCLI>ssscli se05x uid
Opening COM Port '\\.\COM8'
       sss:INFO :atr (Len=35)
                        00 A0 00 00             03 96 04 03             E8 00 F
E 02            0B 03 E8 08
                        01 00 00 00             00 64 00 00             0A 4A 4
3 4F            50 34 20 41
                        54 50 4F
       sss:WARN :Communication channel is Plain.
       sss:WARN :!!!Not recommended for production use.!!!
INFO:sss.se05x:04005001a8cd48e1a500f304250ec9530000
INFO:sss.se05x:Unique ID: 04005001a8cd48e1a500f304250ec9530000

C:\se050_middleware\simw-top\binaries\pySSSCLI>
```

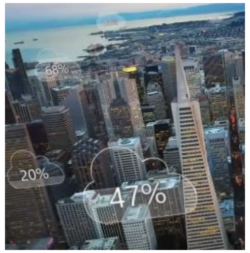
1 Go to simw-top\binaries\pySSCLI folder
`cd C:\se050_middleware\simw-top\binaries\pySSSCLI`

3 Open new connection
`Ssscli connect se050 vcom <COM_PORT>`

4 Send a command (e.g. read UID)
`Ssscli se05x uid`

Evaluate EdgeLock SE050 use case examples

Evaluate EdgeLock SE050 use cases examples



Secure cloud onboarding

AN12401- SE050 for secure connection to GCP.
AN12402- SE050 for secure connection to Azure IoT Hub.
AN12404 - SE050 for secure connection to AWS IoT Core.
AN12403- SE050 for secure connection to Watson IoT*.

Device-to-device authentication

AN12399- SE050 for device-to-device authentication

Sensor data protection

AN12401- SE050 for sensor data protection*

Microsoft Azure
Google Cloud
aws

Key injection
Using the pySSSCLI tool or SE050 ease of use configuration

Cloud account setup
Create an account, create a logical device, register root CA / intermediate CA, etc.

Run cloud onboarding demo
Import project, change project settings, start the demo and check connection.

* Will be published soon. Contact NXP if you need an early version.

Evaluate EdgeLock SE050 use cases examples (II)

Secure access module

AN12401- SE050 for secure access module*

Wi-Fi credential protection

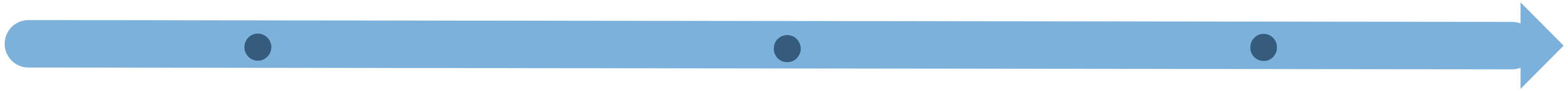
Application note under preparation

Late-stage parameter configuration

Application note under preparation

Device ID for Blockchain

Application note under preparation



Hardware setup & wiring
How to connect the two FRDM-K64F boards

Software setup
How to load the corresponding FW

Run example
Import project, change settings, start the demo

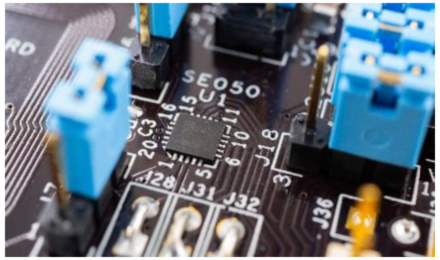
* Will be published soon. Contact NXP if you need an early version.

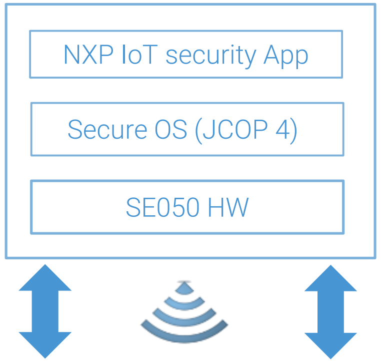
Last words

EdgeLock SE050 – a Root of Trust enabling new use cases

PLUG & TRUST

Out-of-the-box Solution





I²C slave

ISO/IEC 14443

I²C master

Flagship 40nm architecture and CC EAL 6+ certified state of the art security concepts strongly protect against most recent attack scenarios. Additional features enable use cases to answer multiple application needs in IoT and especially industrial needs.

Enhanced security

- 40nm Flagship Technology with IntegralSecurity 3.0
- CC EAL 6+ VAN5 certified HW & OS
- RSA & ECC functionalities
- Future proof curves & higher key length
- Encrypted communication via SCP
- Symmetric ciphers for encryption/decryption

Absolute flexibility

- Product family with multiple solutions for various new use cases
- Flexible applet with dynamic 50kB user memory
- Multiple interfaces – I2C Slave, I2C Master, ISO14443
- Plug & Trust: Easy integration with multiple MCU/MPU platforms & OS, major Cloud integration
- OPC-UA support & easy compliance for IEC62443

Product website: www.nxp.com/SE050

Development kit: www.nxp.com/ OM-SE050ARD

NXP PLUG&TRUST

Time for

Q & A

MobileKnowledge

MobileKnowledge is a team of HW, SW and system engineers, experts in **smart, connected and secure** technologies for the IoT world. We are your ideal **engineering consultant** for any specific support in connection with your **IoT** and **NFC** developments. We design and develop secure HW systems, embedded FW, mobile phone and secure cloud applications.

Our services include:

- **Secure hardware design**
- **Embedded software development**
- **NFC antenna design** and **evaluation**
- **NFC Wearable**
- **EMV L1 pre-certification support**
- **Mobile** and **cloud application development**
- **Secure e2e system design**

MIFARE
Accredited Training Partner

Approved Engineering Consultant
NXP

MOBILE
WORLD CAPITAL
BARCELONA

www.themobileknowledge.com

mk@themobileknowledge.com

We help companies leverage
the **secure IoT revolution**

NXP
PLUG &TRUST

NXP

PLUG &TRUST

SECURE CONNECTIONS
FOR A SMARTER WORLD