AN12570

EdgeLock™ SE05x Quick start guide with Raspberry Pi

Rev. 1.3 — 22 January 2021 Application note

565813

Document information

Information	Content
Keywords	EdgeLock SE05x, EdgeLock SE Plug & Trust Middleware
Abstract	This document explains how to get started with the OM-SE05xARD board and the Raspberry Pi board, as a reference for any other device running a Linux distribution. This guide provides detailed instructions for connecting the boards and running the project examples included in EdgeLock SE Plug & Trust Middleware.

Revision history

Revision history

Revision number	Date	Description
1.0	2019-08-30	First document release
1.1	2020-02-06	Added OM-SE050RPI adapter board
1.2	2020-12-07	Updated to latest template and fixed broken links.
1.3	2021-01-22	Added EdgeLock SE051, terminal Figure changes and appendix addition to show the ssscli command line interface

1 Required hardware

The EdgeLock SE05x works as an auxiliary security device attached to a host controller, communicating with through an I²C interface. To follow the instructions provided in this document, you need an EdgeLock SE05x development board and a Raspberry Pi board, acting as a host controller.

1.1 Required hardware

The following hardware will be used throughout the document:

1. **OM-SE05xARD development boards ordering details:**
   The EdgeLock SE05x support package provides development boards for evaluating EdgeLock SE050 and EdgeLock SE051 features. Select the development board of the product you want to evaluate. Table 1 details the ordering details of the EdgeLock SE05x development boards.

Table 1. EdgeLock SE05x development boards.

Part number	12NC	Description	Picture
OM-SE050ARD	935383282598	SE050 Arduino® compatible development kit	
OM-SE051ARD	935399187598	SE051 Arduino® compatible development kit	

Note: *The pictures in this guide will show OM-SE050ARD, but OM-SE051ARD can be used as well with the same configuration.*

2. **OM-SE050RPI adapter board for Raspberry Pi:**

Table 2. OM-SE050RPI adapter board details

Part number	12NC	Content	Picture
OM-SE050RPI	935379833598	Raspberry Pi to OM-SE05xARD adapter	

3. **Raspberry Pi board:**

Table 3. Raspberry Pi

Part number	Content	Picture
Raspberry Pi	Any Raspberry Pi model	

2 Prepare your Raspberry Pi

This section explains how to get your Raspberry Pi ready to execute the EdgeLock SE Plug & Trust Middleware. For that, you need to go through the following steps:

1. Hardware setup for Raspberry Pi
2. Software setup for Raspberry Pi

2.1 Hardware setup

The hardware setup consists of two steps:

1. Configuring the OM-SE05xARD jumpers, as described in Section 2.1.1.
2. Connecting the OM-SE05xARD to the Raspberry Pi, as described in Section 2.1.2.

2.1.1 Jumper configuration

Make sure the jumpers in your OM-SE05xARD board are configured as shown in Figure 1:

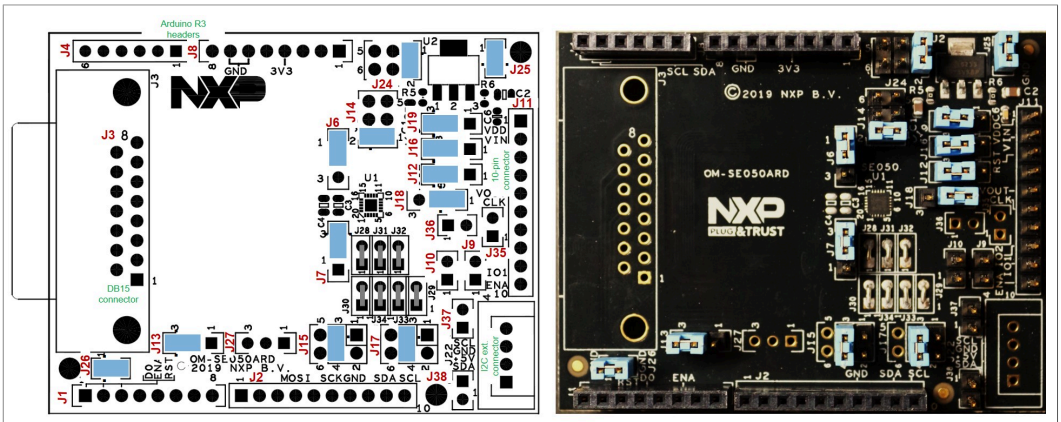

Figure 1. OM-SE05xARD jumper configuration

For more information about the OM-SE05xARD jumper settings, refer to AN12395 OM-SE050ARD hardware overview.

2.1.2 Connecting the OM-SE05xARD to the Raspberry Pi

You have two options to connect the Raspberry Pi to the OM-SE05xARD board:

1. Using the OM-SE05xRPI adapter board, as described in Section 2.1.2.1
2. Using the OM-SE05xARD connected with wires, as described in Section 2.1.2.2

2.1.2.1 Using the OM-SE05xRPI adapter board

The Raspberry Pi and the OM-SE05xARD boards can be directly connected using the OM-SE050RPI adapter board. Follow the steps shown in Figure 2:

1. Mount the OM-SE05xARD on top of the OM-SE05xRPI board using the Arduino connectors.
2. Mount the two boards on top of the Raspberry Pi using the Raspberry connectors in the OM-SE05xRPI.

The result of it is three boards stacked together, being the OM-SE05xRPI the board in between the Raspberry Pi and OM-SE05xARD.

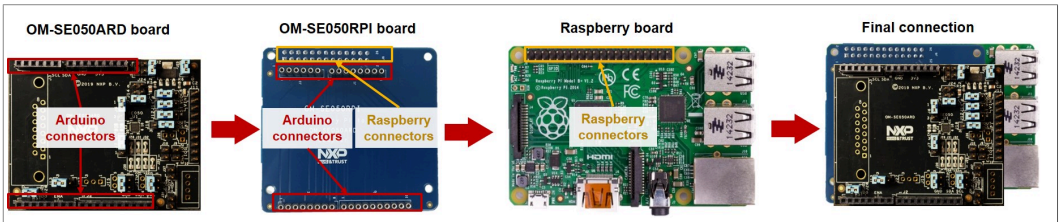

Figure 2. OM-SE05xARD connection to the Raspberry Pi using the OM-SE05xRPI adapter board

2.1.2.2 Connecting the OM-SE05xARD with wires

In case you do not have the OM-SE05xRPI adapter board, you can also manually wire the Raspberry Pi to the OM-SE05xARD using the I^2C connector, as shown in Figure 3:

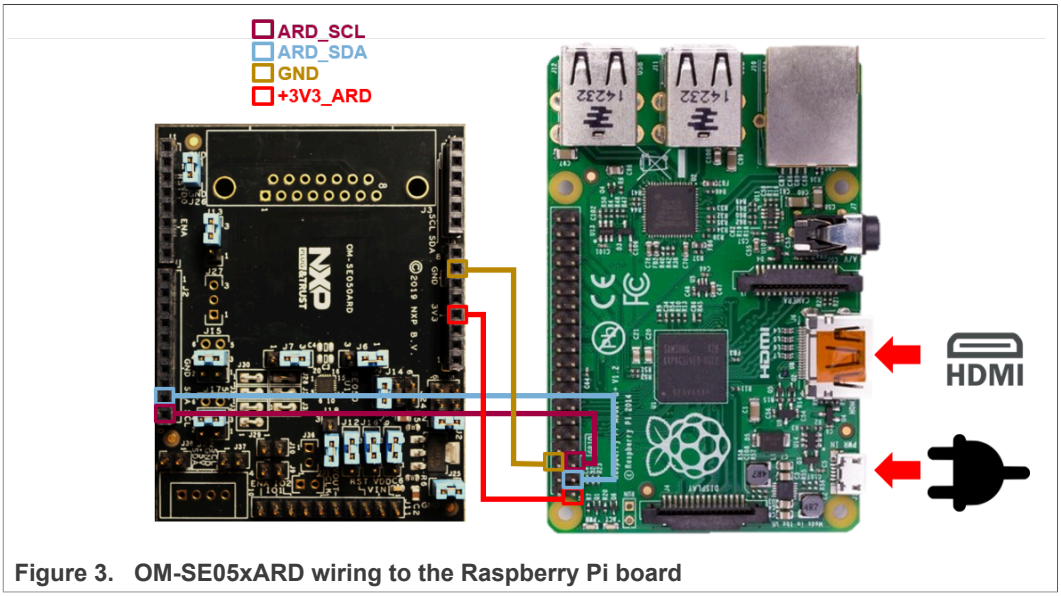

Figure 3. OM-SE05xARD wiring to the Raspberry Pi board

Table 4 shows the detailed connection of the OM-SE05xARD to the Raspberry Pi:

Table 4. OM-SE05xARD wiring to the Raspberry Pi board

OM-SE05xARD (# jumper - # pin)	Raspberry Pi (# jumper - # pin)
J2-P10 (ARD_SCL)	J8-P5 (SCL)
J2-P9 (ARD_SDA)	J8-P3 (SDA)
J8-P7 (GND)	J8-P6 (GND)
J8-P4 (3V3_ARD)	J8-P1 (3V3)

2.2 Software setup

The software setup consists of three steps:

1. Install your preferred Linux distribution in your device. In this guide the Raspberry Pi board running the Raspbian operating system is used as a reference. Raspbian can be installed as described in Section 2.2.1.
2. Install the build tools necessary to build the EdgeLock SE Plug & Trust Middleware and the test project examples. The procedure for the Raspbian operating system is described in Section 2.2.2.
3. Enable the I^2C interface in your Linux distribution to allow the communication with the security IC of the OM-SE05xARD board. The procedure for the Raspbian operating system is described in Section 2.2.3.

2.2.1 Install Raspbian

Before executing the steps described in this guide, it is necessary to install the Raspbian operating system in the Raspberry Pi. The official Raspberry website recommends two options:

1. Using New Out of Box Software (NOOBS), an easy operating system installation manager for the Raspberry Pi. This tool is the easiest and most recommended option, but requires a screen to go through the initial installation process. Installation instructions are provided in the official Raspberry NOOBS webpage.
2. Downloading the official Raspbian image from the official Raspberry Pi image repository and then flashing the image in the SD card by following the instructions provided in the official documentation.

The steps described in this guide use the latest Raspbian release at the time of writing (Raspbian 10 Buster).

2.2.2 Install build tools

To build the EdgeLock SE Plug & Trust Middleware middleware and the example projects, it is necessary to have the Python and CMake packages installed in the system along with the libssl library (part of OpenSSL toolkit). CMake GUI packages are also required if you want to use the CMake graphical user interface. You can install the required packages by opening a Terminal window and following the steps as shown in Figure 4:

1. You can install all the required packages with a single command by sending:
```
>> sudo apt-get install python cmake cmake-curses-gui cmake-qt-gui libssl-dev
```

2. You may be asked to proceed with the installation:
   Send `>> y`

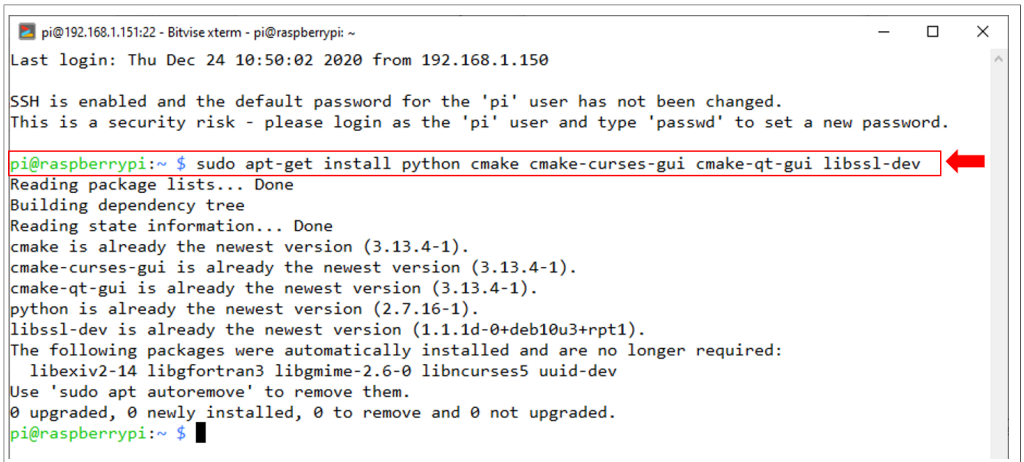

Figure 4. Install build tools

Note: In this case, the build tools were already installed in the environment.

2.2.3 Enable the I²C interface

The Raspberry Pi board communicates with the OM-SE05xARD security IC through the I²C interface. The I²C interface is not enabled by default in Raspbian and must be activated before the EdgeLock SE Plug & Trust Middleware test examples can be executed. To enable I²C, open a Terminal window and follow these steps:

1. Verify if I²C is active by listing the available I²C interfaces:
   `>> ls /sys/bus/i2c/devices/`
   If the *i2c-x* interface is listed, as shown in Figure 5 , then you can skip this section and proceed to Section 3.
   Note: *the I²C interface number might be different.*

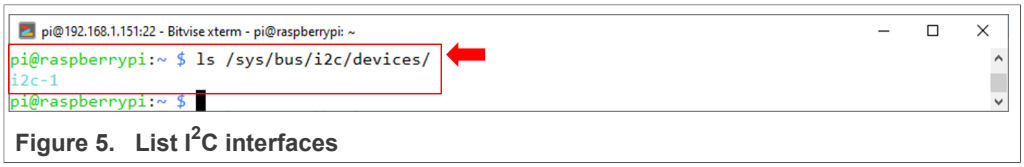

Figure 5. List I²C interfaces

2. Open the Raspberry Pi software configuration tool, as shown in Figure 6:
   `>> sudo raspi-config`

Figure 6. Open the Raspberry Pi software configuration tool

3. Use the up and down arrow keys to select the 5th menu entry (Interfacing Options) and then press Enter, as shown in Figure 7:

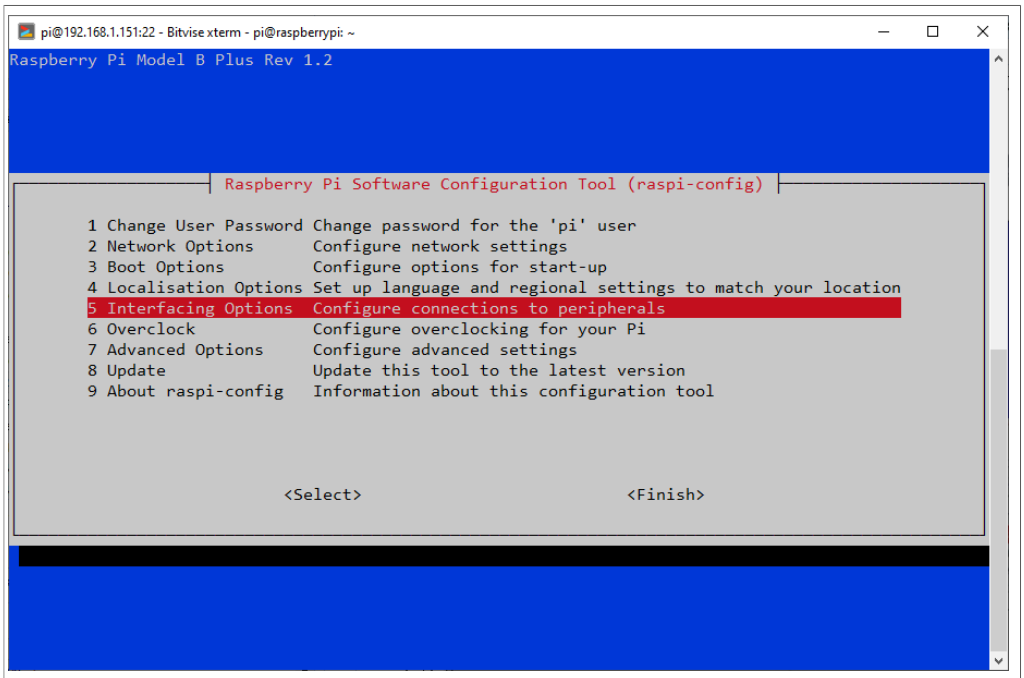

Figure 7. Enable I²C interface

4. Use the up and down arrow keys to select the 5th menu option (I²C) and then press Enter, as shown in Figure 8:

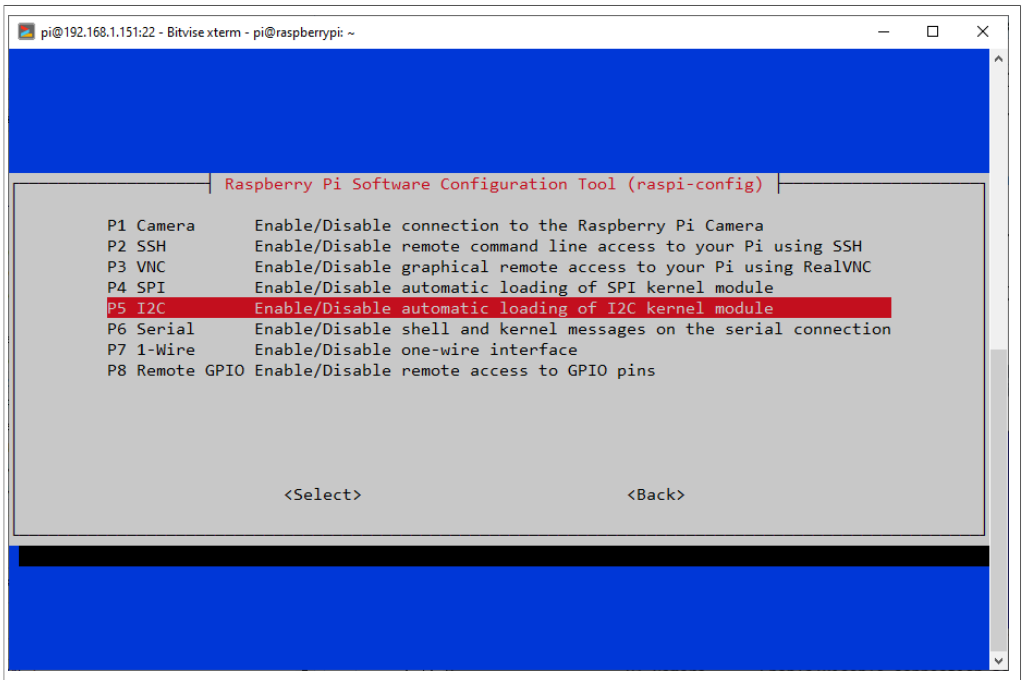

Figure 8. Enable I²C interface

5. You will be asked to confirm your choice to activate the I²C interface. Use the left and right arrow keys to select the Yes option and then press Enter, as shown in Figure 9:

Figure 9. Enable I²C interface

6. Close the Raspberry Pi software configuration tool. Use the left and right arrow keys to select the Finish option and then press Enter, as shown in Figure 10:

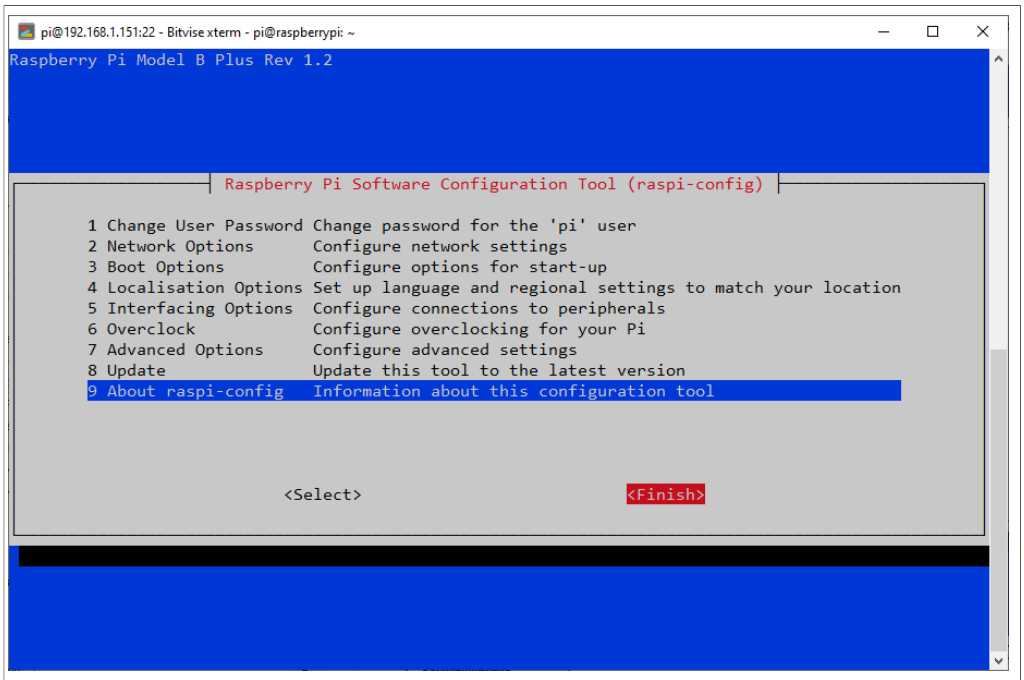

Figure 10. Close the Raspberry Pi sofware configuration tool

7. Verify the correct activation of the I²C interface, as shown in Figure 11:
   `>> ls /sys/bus/i2c/devices/`
   The *i2c-x* interface should now be listed.
   Note: *the I²C interface number might be different.*

Figure 11. List I²C interfaces

3 Run EdgeLock SE Plug & Trust Middleware test examples

This section details the steps required from the moment you download EdgeLock SE Plug & Trust Middleware until you are able to run an EdgeLock SE Plug & Trust Middleware test example.

3.1 Download EdgeLock SE Plug & Trust Middleware

The EdgeLock SE Plug & Trust Middleware stack includes several project examples for cloud service onboarding. To prepare the EdgeLock SE Plug & Trust Middleware:

1. Download the EdgeLock SE Plug & Trust Middleware from NXP website and place the .zip file in the */home/user* directory of your Raspbian distribution.
   Note:*The user folder can have different names, in this example the user folder's name is pi*
2. Open a Terminal window and follow the next steps as shown in Figure 12:
   a. Move to the user's *home* directory:
      (1) `>> cd ~`
   b. Create a folder called *se050_middleware:*
      (2) `>> mkdir se_mw`
   c. Unzip the EdgeLock SE Plug & Trust Middleware in the *se050_middleware* folder:
      (3) `>> unzip SE-PLUG-TRUST_MW.zip -d se_mw`
      Note:*The name of the zip file might be different.*
      Note:*This command may take a few seconds to complete.*

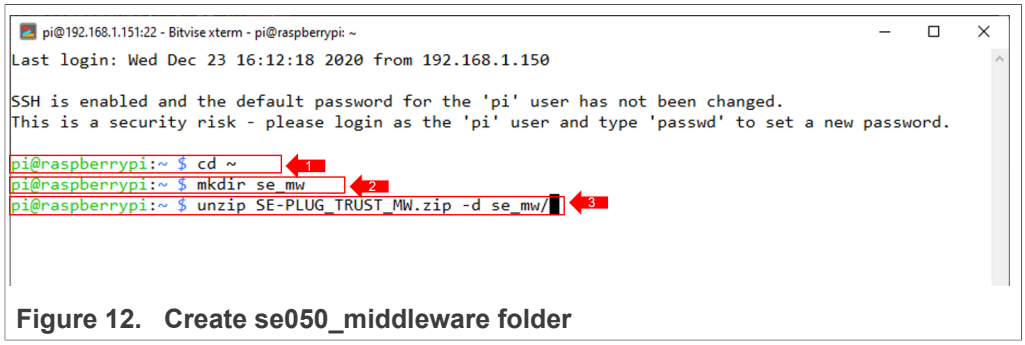

Figure 12. Create se050_middleware folder

3. You can verify that the files have been correctly unzipped by following these steps:
   a. Move to the *simw-top* folder inside the *se_mw* folder:
      `>> cd se_mw/simw-top`
   b. List the content of the *simw-top* folder:
      `>> ls`
      The content of the folder should be the same as shown in Figure 13:

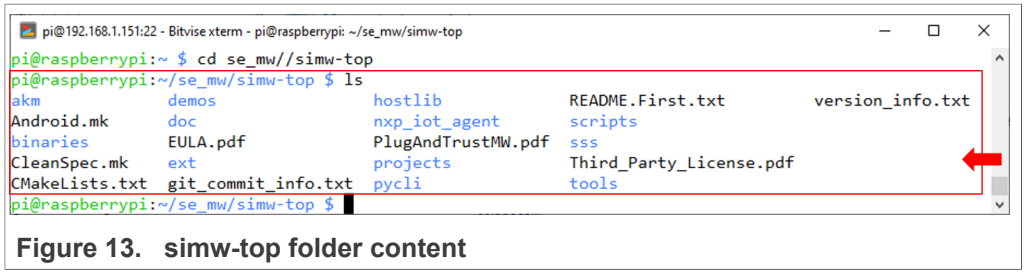

Figure 13. simw-top folder content

3.2 Build EdgeLock SE Plug & Trust Middleware

The EdgeLock SE Plug & Trust Middleware uses CMake for building the project examples into your local machine. To build the EdgeLock SE Plug & Trust Middleware middleware, open a Terminal window and follow the next steps as shown in Figure 14:

1. Go to the folder with the unzipped SE050 middleware:
   (1) `>> cd /home/pi/se_mw/simw-top/scripts`
2. Generate the EdgeLock SE Plug & Trust Middleware project examples:
   (2) `>> python create_cmake_projects.py`
   Note: *This command may take a few seconds to complete.*

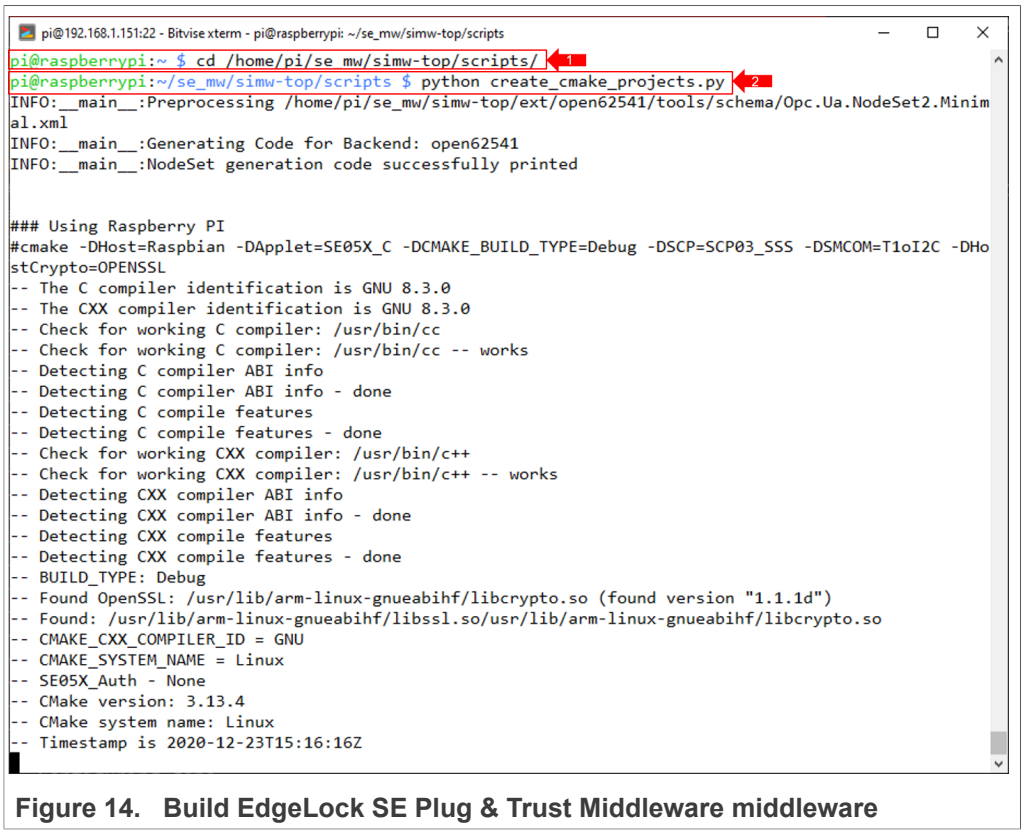

Figure 14. Build EdgeLock SE Plug & Trust Middleware middleware

3. If the compilation is successful you should (1) see a new *simw-top_build* folder inside the se_mw folder and (2) a new folder inside the `simw-top` folder as shown in Figure 15:

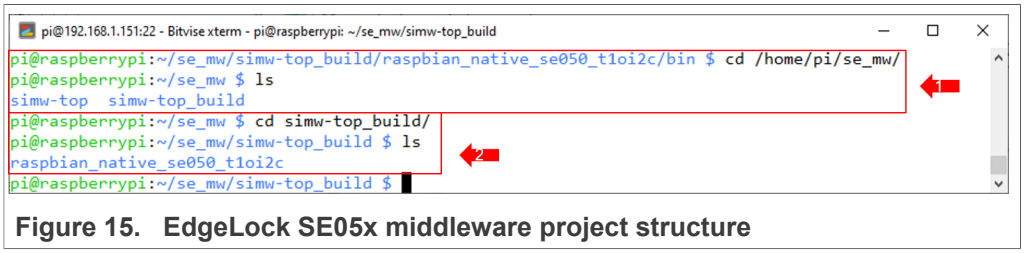

Figure 15. EdgeLock SE05x middleware project structure

3.3 Build EdgeLock SE Plug & Trust Middleware test examples

The EdgeLock SE Plug & Trust Middleware contains several examples used to verify atomic EdgeLock SE05x security IC features. This section explains how to compile the EdgeLock SE Plug & Trust Middleware test examples. Open a Terminal window and follow these steps:

1. Move to the folder that contains the test examples and the source code of the Raspbian EdgeLock SE05x libraries:
   `>> cd /home/pi/se_mw/simw-top_build/raspbian_native_se050_t1oi2c`
2. Optionally open the CMake configuration interface, as shown in Figure 16 to change build settings:
   `>> ccmake .`
   Note: *You can use the graphical interface by sending* `cmake-gui .` *instead.*

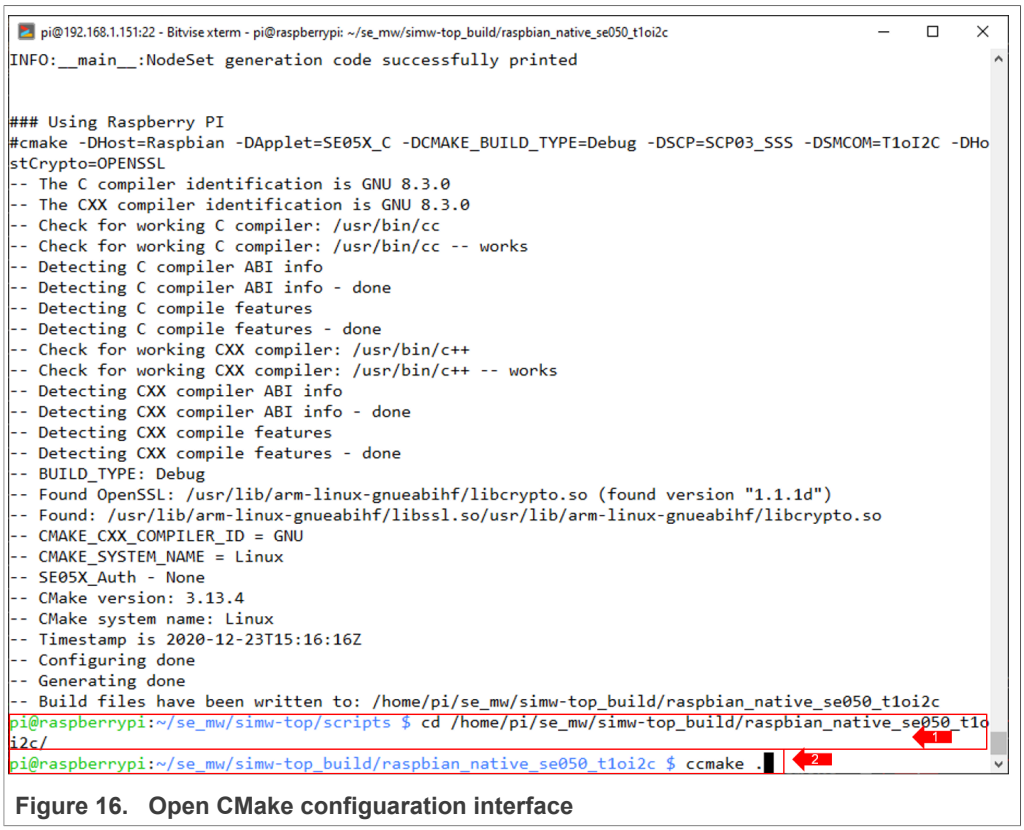

Figure 16. Open CMake configuaration interface

3. Review the build configuration and make sure that the *Host* parameter is set to the value *Raspbian*, as shown in Figure 17. Leave the default settings and press *q* to return to the console.
   Note: *If you want to change the configuration you can use the up and down arrow keys to navigate through the available options and the left and right arrow keys to*

change the option value. In case you edit the configuration, press `c` *(configure) and then* `g` *(generate)* to apply the changes.

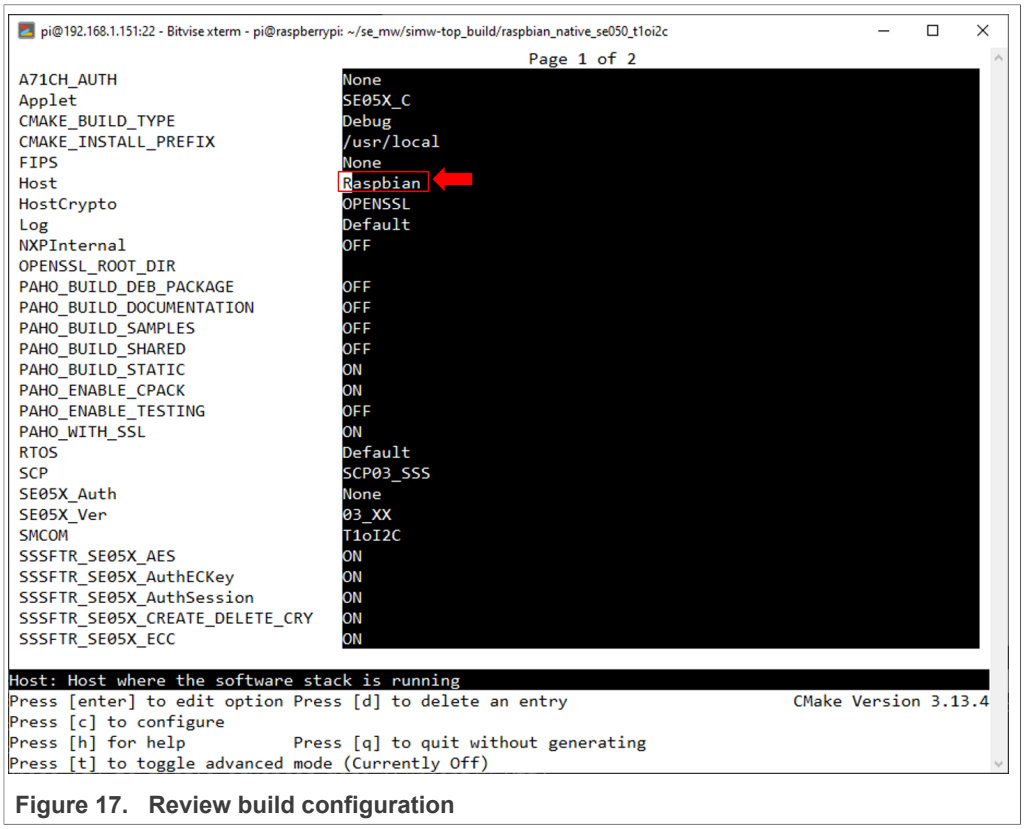

Figure 17. Review build configuration

4. Build the project examples, as shown in Figure 18:
   `>> cmake --build .`
   Note: *This command may take a few seconds to complete.*

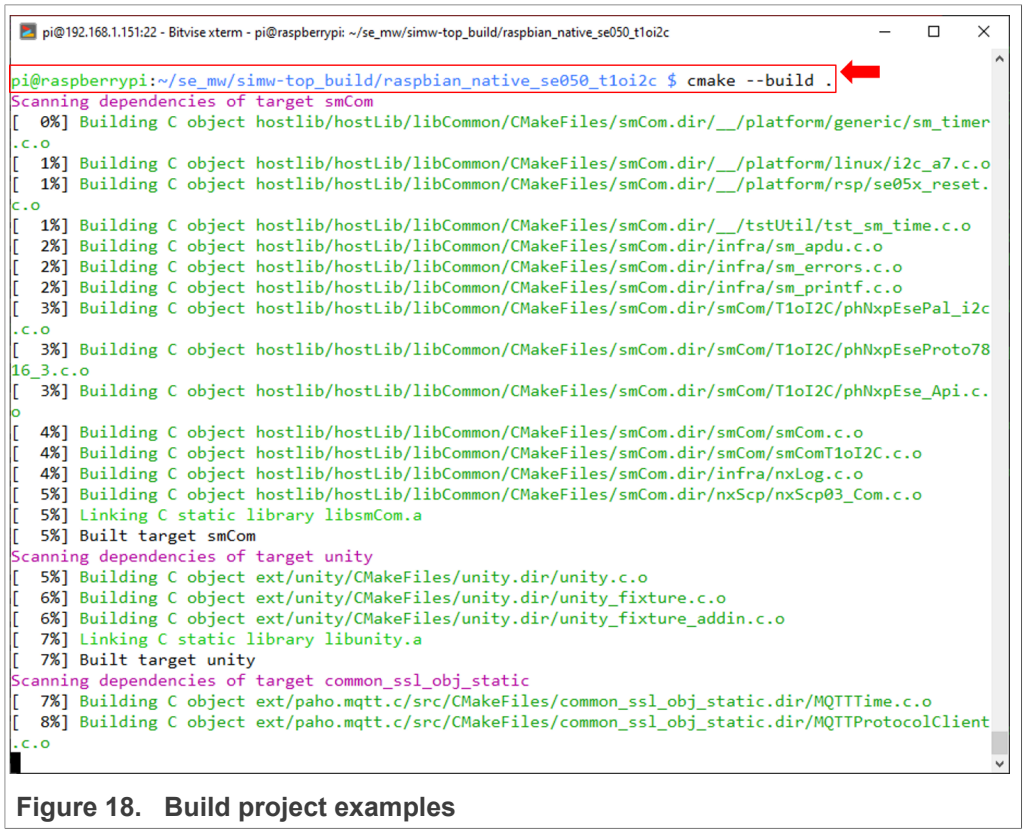

Figure 18. Build project examples

5. Install the projects in the system as shown in Figure 19:

```
>> sudo make install
```

Note: *This command may take a few seconds to complete.*

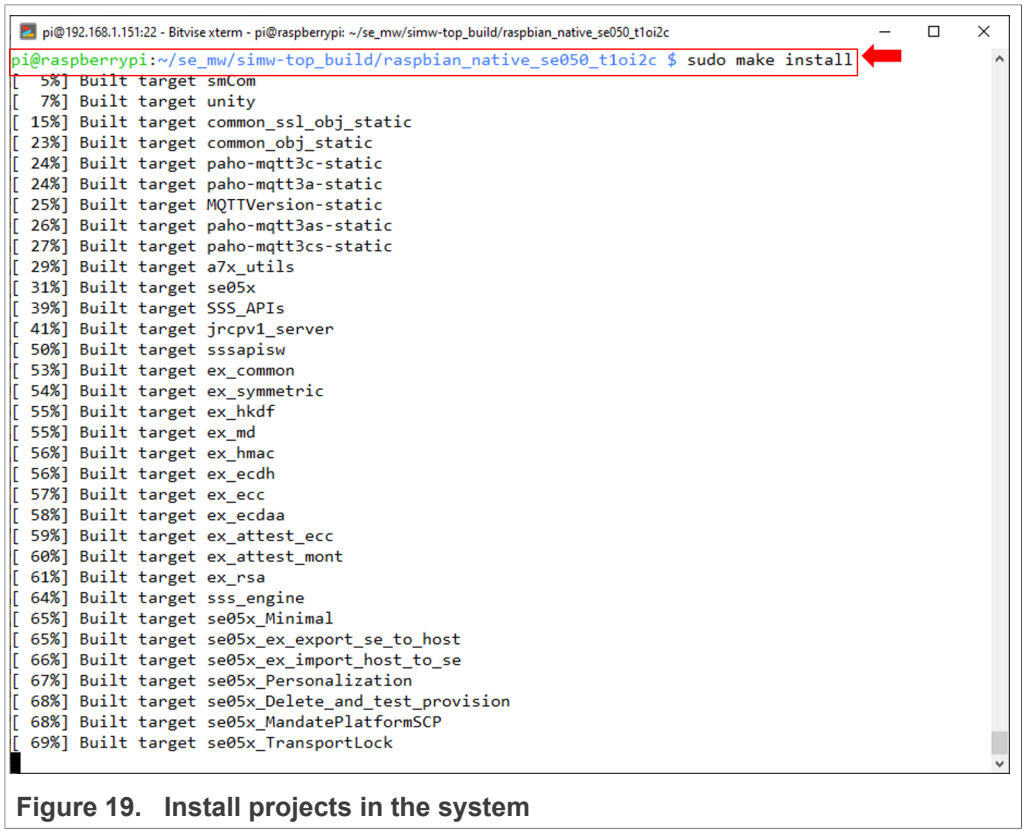

Figure 19. Install projects in the system

6. Update the cache to include the newly installed libraries as shown in Figure 20:
   `>> sudo ldconfig /usr/local/lib`

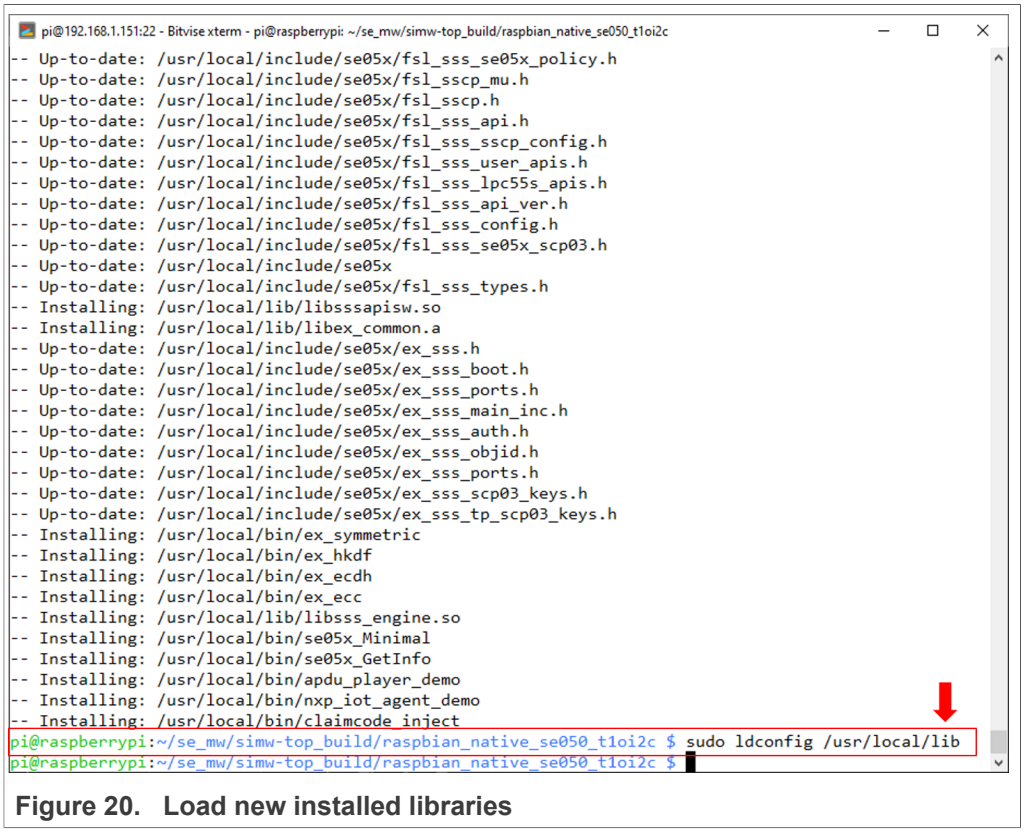

Figure 20. Load new installed libraries

3.4 Execute EdgeLock SE Plug & Trust Middleware test example

This section explains how to run the EdgeLock SE Plug & Trust Middleware test example called `se05x_minimal`. The `se05x_minimal` project outputs the memory left in the EdgeLock SE05x security IC. To execute the `se05x_minimal` test example follow these steps:

1. Connect the OM-SE05xARD board to the Raspberry Pi as described in Section 2.1.

2. Open a Terminal window and follow the steps as shown in Figure 21:
   a. Move to the directory containing the examples binaries:
      (1) `>> cd /home/pi/se_mw/simw-top_build/raspbian_native_se050_t1oi2c/bin/`
   b. Run the `se05x_minimal` example:
      (2) `>> ./se05x_Minimal`
      (3) You should see the EdgeLock SE05x IC available memory (in this case, 32767)

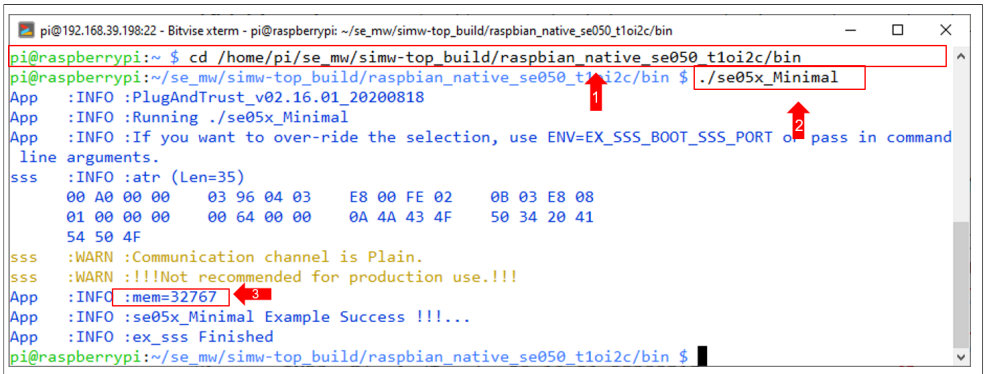

Figure 21. Run se05x_minimal example

4 Appendix A: Using the ssscli tool

EdgeLock SE Plug & Trust Middleware also provides the `ssscli` tool. This tool can be used to interact with the EdgeLock SE05x security IC without having to write any code.

For installing the ssscli tool follow the steps below shown in Figure 22:

1. Move to the user directory
   >> `cd /home/pi`
2. Ensure PYTHON 3 is installed
   `>> sudo apt-get install python3-pip`
3. Ensure python3-pip and libffi-dev are installed:
   >> `sudo apt-get install libffi-dev`
   ***Note**: In this case, the packages were already installed*

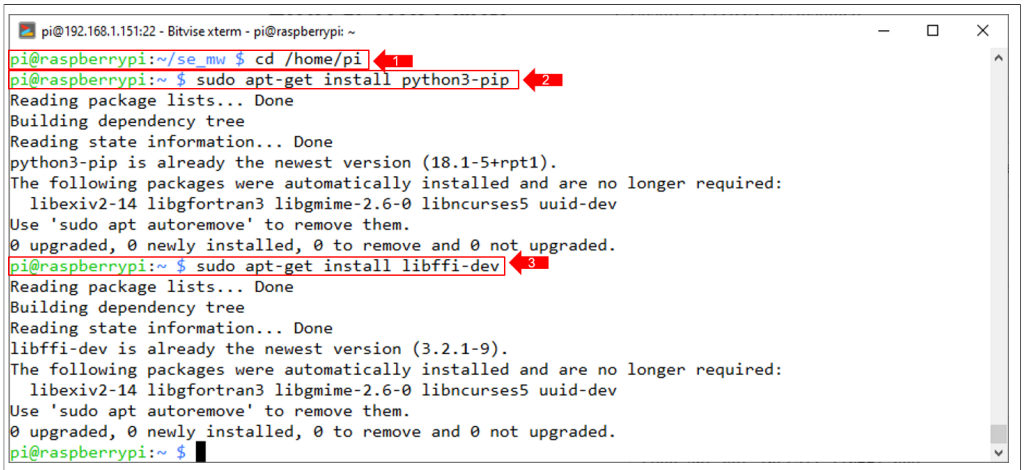

Figure 22. Install python and libffi-dev

Make sure you have cmake installed and configured for the Raspbian Host as done in Section 3.3.

4. Ensure click, cryptography and func-timeout modules are installed. Figure 23 shows how to install these modules, change directory to:
   >> `cd /home/pi/se_mw/simw-top/pycli`
5. and run the following command:
   >> `pip3 install -r requirements.txt`

6.

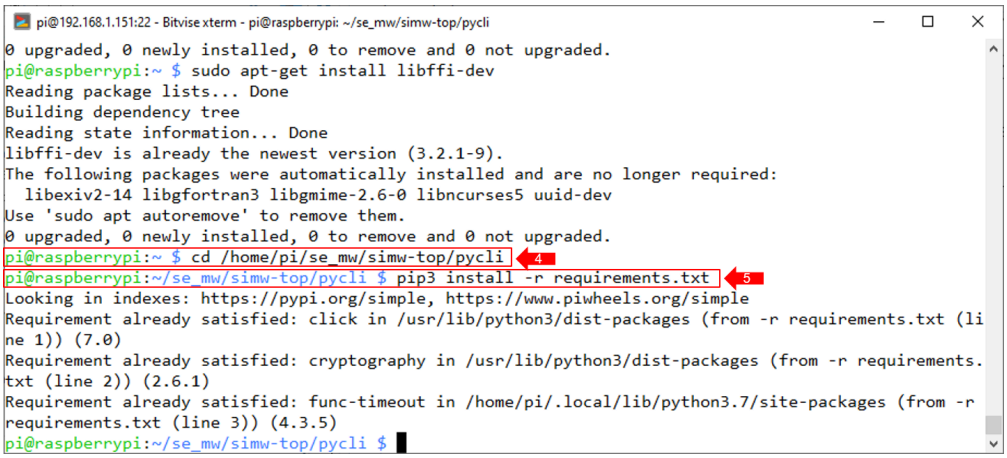

Figure 23. Install required modules

7. Install the `ssscli` tool as Figure 24 shows:
   >> `cd src`
   >> `sudo python3 setup.py develop`

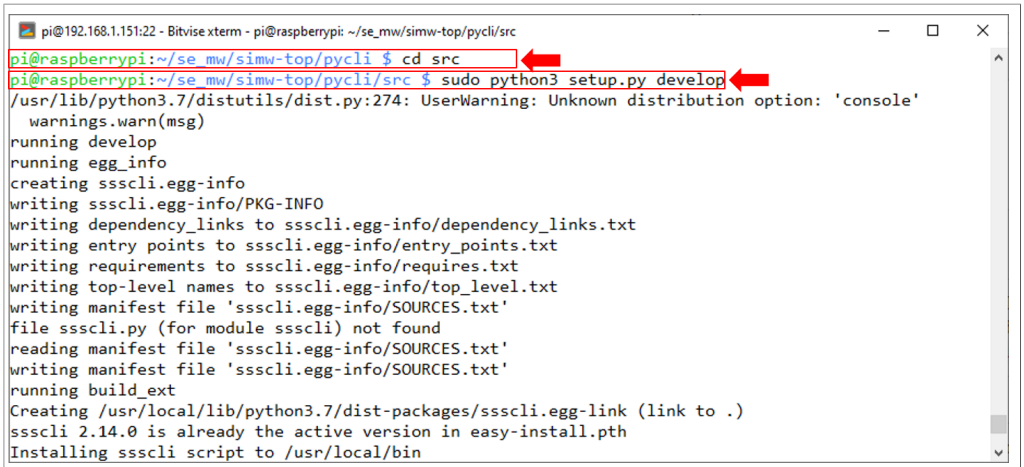

Figure 24. Install ssscli tool

To start the ssscli tool, send the commands shown in Figure 25:

1. Move to the user directory:
   >> `cd /home/pi`
2. Open the connection
   >> `ssscli connect se050 t1oi2c none`

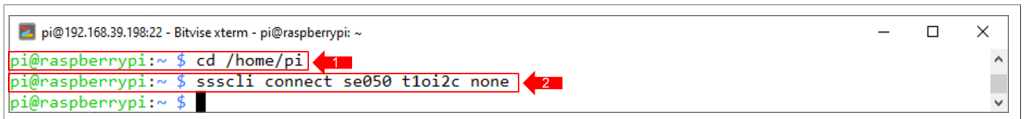

Figure 25. Start ssscli tool

The SE05x ssscli tool supports several operations. To check which commands are supported by the ssscli tool (Figure 26):

```
>> ssscli --help
```

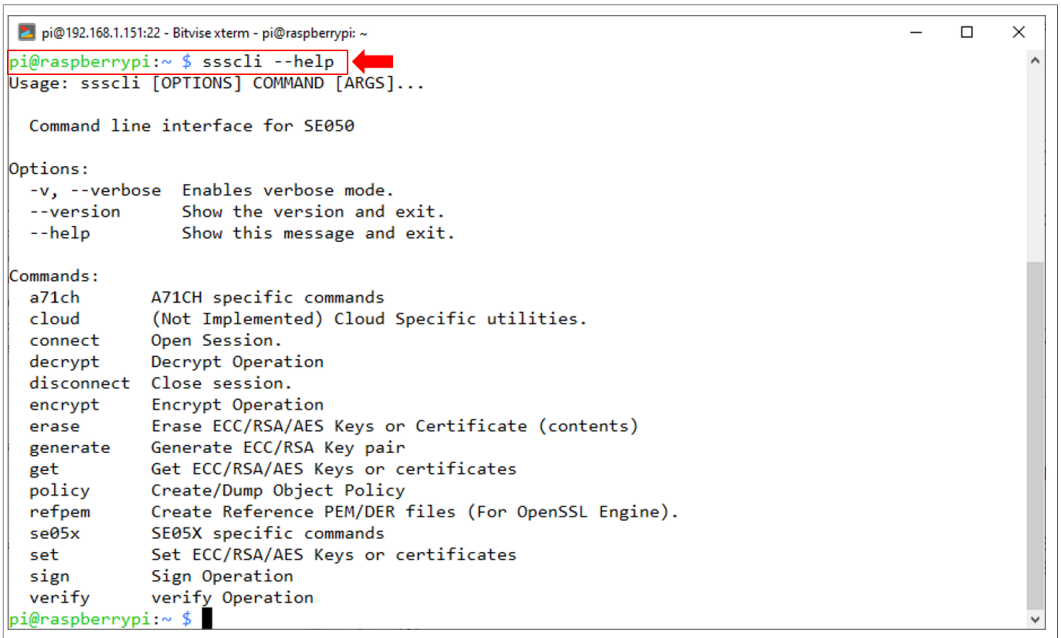

Figure 26. ssscli tool help menu

Each of these options provides information about the syntax used for each specific command. For instance, the se05x option:

```
>> ssscli se05x
```

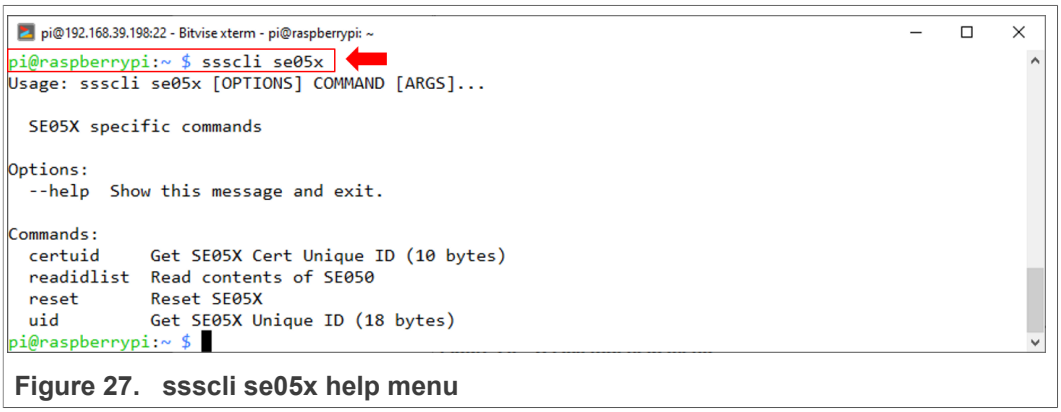

Figure 27. ssscli se05x help menu

To read the credentials and secure objects stored in the EdgeLock SE05x, you can send the following command (Figure 28):

```
>> ssscli se05x readidlist
```

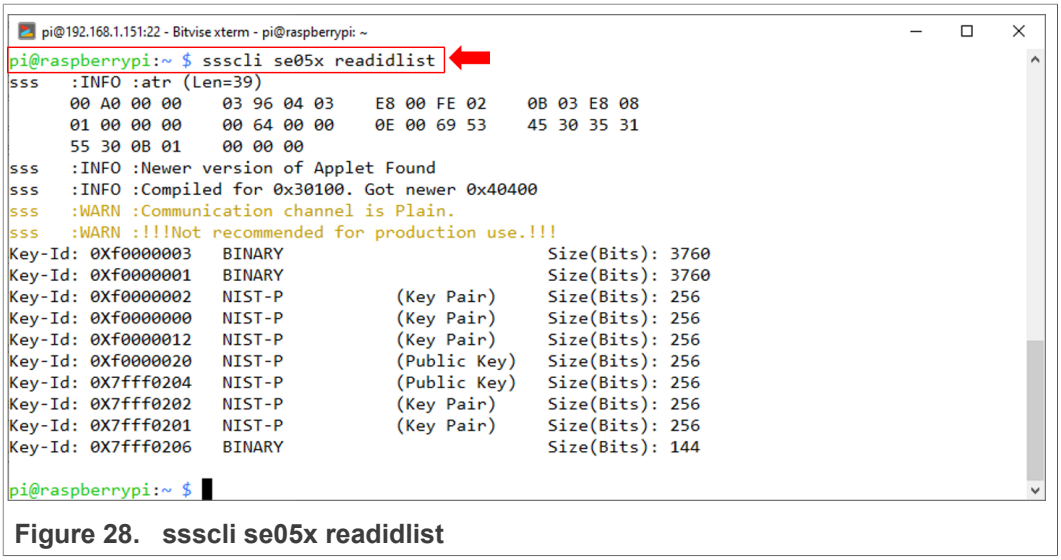

Figure 28. ssscli se05x readidlist

5 Legal information

5.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

5.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

5.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Tables

Tab. 1. EdgeLock SE05x development boards. 3
Tab. 2. OM-SE050RPI adapter board details 3
Tab. 3. Raspberry Pi 4
Tab. 4. OM-SE05xARD wiring to the Raspberry Pi board 6

Figures

Fig. 1. OM-SE05xARD jumper configuration 5
Fig. 2. OM-SE05xARD connection to the Raspberry Pi using the OM-SE05xRPI adapter board 6
Fig. 3. OM-SE05xARD wiring to the Raspberry Pi board 6
Fig. 4. Install build tools 8
Fig. 5. List I2C interfaces 8
Fig. 6. Open the Raspberry Pi software configuration tool 8
Fig. 7. Enable I2C interface 9
Fig. 8. Enable I2C interface 9
Fig. 9. Enable I2C interface 10
Fig. 10. Close the Raspberry Pi sofware configuration tool 10
Fig. 11. List I2C interfaces 11
Fig. 12. Create se050_middleware folder 12
Fig. 13. simw-top folder content 12
Fig. 14. Build EdgeLock SE Plug & Trust Middleware middleware 13
Fig. 15. EdgeLock SE05x middleware project structure 13
Fig. 16. Open CMake configuaration interface 14
Fig. 17. Review build configuration 15
Fig. 18. Build project examples 16
Fig. 19. Install projects in the system 17
Fig. 20. Load new installed libraries 18
Fig. 21. Run se05x_minimal example 19
Fig. 22. Install python and libffi-dev 20
Fig. 23. Install required modules 21
Fig. 24. Install ssscli tool 21
Fig. 25. Start ssscli tool 21
Fig. 26. ssscli tool help menu 22
Fig. 27. ssscli se05x help menu 22
Fig. 28. ssscli se05x readidlist 23

Contents

1 Required hardware 3
1.1 Required hardware 3
2 Prepare your Raspberry Pi 5
2.1 Hardware setup 5
2.1.1 Jumper configuration 5
2.1.2 Connecting the OM-SE05xARD to the Raspberry Pi 5
2.1.2.1 Using the OM-SE05xRPI adapter board 5
2.1.2.2 Connecting the OM-SE05xARD with wires 6
2.2 Software setup 6
2.2.1 Install Raspbian 7
2.2.2 Install build tools 7
2.2.3 Enable the I2C interface 8
3 Run EdgeLock SE Plug & Trust Middleware test examples 12
3.1 Download EdgeLock SE Plug & Trust Middleware 12
3.2 Build EdgeLock SE Plug & Trust Middleware 13
3.3 Build EdgeLock SE Plug & Trust Middleware test examples 14
3.4 Execute EdgeLock SE Plug & Trust Middleware test example 18
4 Appendix A: Using the ssscli tool 20
5 Legal information 24

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 22 January 2021
Document identifier: AN12570
Document number: 565813