AN12397 EdgeLockTM SE050 Quick start guide with i.MX6UltraLite Rev. 1.2 — 17 December 2019 Application note 534512

Document information

Information	Content
Keywords	EdgeLock SE050, EdgeLock Plug & Trust middleware, i.MX6UltraLite
Abstract	This document explains how to get started with the OM-SE050ARD board and i.MX6UltraLite board. This guide provides detailed instructions for connecting the boards, installing the software, running the EdgeLock SE050 Plug & Trust project examples and executing the pySSSCLI tool.



Revision history

Revision his	story	
Revision number	Date	Description
1.0	2019-06-08	First document release.
1.1	2019-06-20	Update board figures
1.2	2019-12-17	Corrected OM-SE050ARD J14 jumper setting.

1 Read this first

The hardware used in this document is the following:

1.1 Required hardware

1. OM-SE050ARD development kit:

Table 1.	OM-SE050AR	D deve	lopment	kit deta	ails

Part number	12NC	Content	Picture
OM-SE050ARD	935383282598	EdgeLock SE050 development board	

2. i.MX6Ultralite board

Table 2. i.MX6Ultralite	•		
Part number	12NC	Content	Picture
MCIMX6UL-EVKB	935328353598	i.MX6UltraLite evaluation kit	

2 Hardware setup

The hardware setup consists of two steps:

- 1. Mounting the boards, as described in Section 2.1
- 2. Configuring OM-SE050ARD jumpers, as described in Section 2.2

2.1 Mounting the boards

1. Connect the OM-SE050ARD board on top of the i.MX6UltraLite board using the Arduino connectors as shown in <u>Figure 1</u>



Note: In case the i.MX6UltraLite board does not come with the Arduino headers assembled by default, they can be easily soldered in the dedicated mounting holes.

2.2 Jumper configuration

1. Make sure the jumper settings in your OM-SE050ARD board are configured as shown in <u>Figure 2</u>



EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite

For more information about the OM-SE050ARD jumper settings, refer to <u>AN12395 OM-SE050ARD hardware overview</u> document.

3 Software setup

The software setup consists of:

- 1. Preparing a micro-SD card with the pre-compiled Linux image for i.MX6UltraLite board, as described in <u>Section 3.1</u>.
- 2. Installing the USB to UART Bridge VCOM driver in your laptop, as described in <u>Section 3.2</u>.
- 3. Installing TeraTerm terminal application, as described in <u>Section 3.3</u>.
- 4. Booting the i.MX6UltraLite board, as described in <u>Section 3.4</u>.

3.1 Micro-SD card preparation

To prepare the micro-sd card with the pre-compiled Linux image that includes the EdgeLock SE050 Plug & Trust middleware, you need to:

- Download from <u>www.nxp.com/se050</u> the EdgeLock SE050 Plug & Trust middleware SD Card Image. This image contains the EdgeLock SE050 Plug & Trust middleware pre-installed on a bootable IMX6UL-EVK SD Card Image.
- 2. Download and install <u>Win32 Disk Imager</u> software. Win32 Disk Imager is a Windows open source program to format SD card images. Instead of Win 32 Disk Imager, you could also use any other software for this operation.
- 3. Plug your micro-SD card in your laptop.
- Open Win 32 Disk Imager, (1) select from your file system the pre-compiled Linux image you downloaded from the website and (2) click the *Write* button as shown in <u>Figure 3</u>.



3.2 Drivers

To install the i.MX6UltraLite drivers, follow these steps:

1. Plug the power supply and connect the USB cable to your laptop as shown in <u>Figure 4</u>.

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite



- 2. Download the <u>USB to UART Bridge VCOM driver</u> for your processor (either 32 or 64 bits). Install the driver by following the setup wizard until it is finished.
- 3. Unplug and plug your board.
- 4. Go to your Device Manager, and check that your board is recognized and assigned to a port number (COMxx). Write down the assigned port number (COMxx) as it is needed in the next steps. Your Device Manager should look like Figure 5

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite



3.3 Terminal setup

We need to install a terminal application, for instance TeraTerm, to communicate and view the serial output of the i.MX6UltraLite board from our laptop. To setup TeraTerm application:

- 1. Download <u>TeraTerm</u> and run the installer.
- 2. Launch TeraTerm, click **Serial** option and select from the drop down list the COM port number assigned to your i.MX6UltraLite board as shown in <u>Figure 6</u>. If the serial option is not enabled for you, your i.MX6UltraLite board might not be recognized. In that case, please repeat the driver installation described in <u>Section 3.2</u>.

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite

⊖ TCP <u>/I</u> P	Hos <u>t</u> :	myhost.exa	mple.com	
		⊠ Hist <u>o</u> ry		
	Service:	⊖ Te <u>l</u> net	TCP por	t#: 22
) <u>s</u> sh	SSH version:	SSH2
		O Other	Proto <u>c</u> ol:	UNSPEC
● S <u>e</u> rial	Po <u>r</u> t:	COM6: Silic	on Labs CP210×	: USB to l
	ОК	Cancel	Help	

3. Go to Setup > Serial Port and configure the terminal to *115200 baud rate*, *8 data bits, no parity* and *1 stop bit* and click **OK** as shown in Figure 7

Tampinal	Help			Port:	COM6 \sim	OK
Window				Baud rate:	115200 ~	on
Font				Data:	8 bit 🗸	Cancel
Keyboard				Parity.	none v	
Serial port				Tanty.	none +	Help
Proxy				Stop:	1 bit v	neih
SSH				Flow control:	none v	
SSH Authentication						
SSH Forwarding				Transmit dela	iy	
SSH KeyGenerator				0 mse	c/char 0 ms	sec/line
TCP/IP						
General						
Additional settings						
Save setup			~			
Restore setup						
Setup directory						
Load key man						
Additional settings Save setup Restore setup Setup directory			v			

3.4 Booting the i.MX6UltraLite

To boot the i.MX6UltraLite, please do the following:

1. Insert the micro-SD card with the pre-compiled Linux image into the card slot as shown in Figure 8

EdgeLockTM SE050 Quick start guide with i.MX6UltraLite



2. Configure the board switches as follows

- SW601 (Boot Device Select Switch): OFF, ON, OFF, OFF (from 4-1 bit)
- SW602 (Boot Mode Select Switch): ON, OFF (from 1-2 bit)
- 3. Make sure the i.MX6UltraLite switches are set as shown in Figure 9



Figure 9. Configure i.MX6UltraLite board switches

- 4. Make sure your board is connected to the power supply and to your laptop using a USB cable and TeraTerm serial port configured (see <u>Section 3.3</u>).
- 5. Turn on the power supply switch to boot up the board. The power supply button is shown in Figure 10.

AN12331	
Application	note

.....

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite



- 6. During the boot process, the operating system status information will be prompted on the TeraTerm as shown in <u>Figure 11</u>. When the process is complete, the user can login with the following credentials
 - Account name: root
 - Password: not required

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite



4 Run EdgeLock SE050 Plug & Trust middlewaretest examples

The EdgeLock SE050 Plug & Trust middleware comes with several test examples used to verify atomic EdgeLock SE050 security IC features. This section explains how to run the EdgeLock SE050 Plug & Trust middleware test example called $se05x_minimal$.

1. Go to se050_mw_vXX.XX.XX_build/imx_native_se050_t1oi2c/bin directory as shown in Figure 12, where vXX.XX.XX corresponds to the EdgeLock SE050 Plug & Trust middleware version number. At the moment of writing, the latest version was v02.09.00_20190605_115623

Send > cd se050_mw_vvXX.XX.build/imx_native_se050_t1oi2c/bin.



2. Execute the $se05x_{minimal}$ test example. This test example outputs the memory left in EdgeLock SE050 security IC.

Send > ./se05x minimal.

The TeraTerm logs should indicate the available memory in EdgeLock SE050 security IC as can be seen in Figure 13 (in this case, 592).

bin# ./	/se05x_minimal pp:INFO :PlugAndTrust_v02.09.00 21	ð190605	100_00000_01010
Aj	pp:INFO :Running ./se05x_minimal		TH 000 D007 000
PORT on	pp:INFU : If you want to over-ride	the selection, use ENV=	EX_222_B001_222
SS SS	ss:INFO :atr (Len=35)		
	00 00 0A 00	03 96 04 03	E8 00 FE
2	0B 03 E8 08		
		00 64 00 00	ØA 4A 43
F	50 34 20 41 E4 E0 4P		
	ss:WARN :Communication channel is	Plain	
SS	ss:WARN :!!!Not recommended for p	roduction use.!!!	
(A)	pp:INFO :mem=592		
A)	pp:INFO :ex_sss Finished		
otCimx	5ulevk:~/se050_mw_v02.09.00_20190	505_115623_build/imx_nat	ive_se050_t1oi2

The execution of the se05x_minimal project is shown as an example. The steps detailed in this section can be replicated to run any other test example included as part of the EdgeLock SE050 Plug & Trust middleware. To get the list of test examples:

1. Send the ls command as shown in Figure 14

Send > 1s -1

root@imx60 c/bin# 1s total 9604 -rwxr-xr-x	lleuk: ~/ -1 1 root 1 root	<pre>/se050 ; root; root; ; root; root; ; root;</pre>	_mu_u02 548508 576764 576808 576292 576492 576492 576492 572456 572456 578196 572816 103984 775180 583292 572456 572216 572216 572216 119060	.09 .0 Mayy Maayy Maayy Maayy Maayy Maayy Maayy Maayy Maayy Maayy	0_2 77777777777777777777777777777	01906 2019 2019 2019 2019 2019 2019 2019 2019	apdu_player ex_ecc ex_hkdf ex_md ex_policy ex_rsa ex_se05x_WiFiKDF_derive ex_se05x_WiFiKDF_inject ex_se05x_WiFiKDF_inject ex_symmetric generate_certificate generate_certificate_key jrcpu1_server nxp_iot_agent_demo nxp_iot_agent_e2e se05x_Delete_and_test_pp se05x_Cet_UID se05x_minimal simple_server	ve_se	050_t1 ion	012
---	---	---	---	---	--------------------------------------	---	--	-------	---------------	-----

5 Using SE050 ssscli tool

In <u>Section 2</u> and <u>Section 3</u> we have prepared the hardware setup and the software setup respectively. To validate that the whole process was done correctly and that your setup is fully operational, we are going to run the <code>ssscli</code> tool. To start the <code>ssscli</code> tool, send the commands shown in <u>Figure 15</u>:

- 1. Open the connection: Send: >ssscli connect se050 tloi2c none
- 2. Send the reset command: Send: >ssscli se05x reset

🛄 COM6 - 1	Tera Term VT		- 1		×
File Edit Se	etup Control Window Help				
1 root@imx6u root@imx6u	levk:~# ssscli connect se050 t1 levk:~# ssscli se05x reset	oi2c none			
S SSS	:INFO :atr (Len=35) 00 A0 00 00	03 96 04	03		00 FE
4F	08 03 E8 08 01 00 00 00 50 34 20 41	00 64 00	00	ØA	4A 43
sss sss rootCimx6u	:WARM :???Not recommended for p levk:~# ■	production use.??	*		

Note: If you see the following message: WARNING:sss.connect:Session already open, close current session first message as shown in Figure 16, it means that you have a session open. To close it, send: (1) > ssscli disconnect and then send once again (2) > ssscli connect se050 vcom <COM_NUMBER> and later (3) > ssscli se05x reset.

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite

File Edit Setup Control Window Help root@inx6ulevk:~# ssscli connect se050 tloi2c none MARNING:sss.connect:Session already open, close current session floi2c root@inx6ulevk:~# ssscli disconnect session floi2c none root@inx6ulevk:~# ssscli session session floi2c none root@inx6ulevk:~# ssscli session session floi2c none sss:INFO :atr (Len=35) 00 00 03 96 04 03 02 0B 03 E8 08 00 00 64 00	first			^
root@imx6ulevk:~# ssscli connect se050 t1oi2c none WARNING:sss.connect:Session already open, close current session f root@imx6ulevk:~# ssscli disconnect root@imx6ulevk:~# ssscli connect se050 t1oi2c none root@imx6ulevk:~# ssscli se05x reset andom: crng init done sss:INF0 :atr (Len=35) 00 A0 00 00 03 96 04 03 02 0B 03 E8 08 01 00 00 00 00 64 00 00 00 64 00 00	first			^
<pre>4F 50 34 20 41 54 50 4F sss:WARN :Communication channel is Plain. sss:WARN :!!!Not recommended for production use.!!! root@imx6ulevk:~#</pre>	E	1 41	0 FE A 43	

 The SE050 ssscli tool supports several operations. To check which commands support the SE050 ssscli tool: (Figure 17) Send: > ssscli

🔟 COM6 - Tera Term VT	-0	×
File Edit Setup Control Window Help		
root@imx6ulevk:~# ssscli Jsage: ssscli [OPTIONS] COMMAND [ARGS]		^
Command line interface for SE050		
Options: -v,verbose Enables verbose mode. 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 se05x SE05X specific commands set Set ECC/RSA/AES Keys or certificates sign Sign Operation verify verify Operation root@imx6ulevk:~#		~

4. Once you are done using the ssscli tool, close the session with SE050 security IC: (Figure 18) Send: > ssscli disconnect

EdgeLock[™] SE050 Quick start guide with i.MX6UltraLite



If you have reached this point, the $\tt ssscli$ tool is working as expected in your machine.

EdgeLockTM SE050 Quick start guide with i.MX6UltraLite

6 Legal information

6.1 Definitions

Draft — The document is a draft version only. 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 herein and shall have no liability for the consequences of use of such information.

6.2 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 products products products applications and products product sole 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). 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 — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

6.3 Trademarks

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

EdgeLockTM SE050 Quick start guide with i.MX6UltraLite

Tables

Tab. 1.	OM-SE050ARD development kit details3	Tab. 2.	i.MX6Ultralite
	•		

NXP Semiconductors

AN12397

EdgeLockTM SE050 Quick start guide with i.MX6UltraLite

Figures

Fig. 1.	Arduino connectors of OM-SE050ARD and
Fig. 2.	Jumper configuration for i.MX6UltraLite
-	board
Fig. 3.	Micro-SD card preparation with Win32 Disk
	Imager software6
Fig. 4.	Plug the power supply and connect the USB
	cable to your laptop7
Fig. 5.	Check i.MX6UltraLite board is recoginized in
	Device Manager8
Fig. 6.	Open a TeraTerm serial connection9
Fig. 7.	Configure TeraTerm serial port connection9
Fig. 8.	Insert the Micro-SD card

Configure i.MX6UltraLite board switches 10
Turn on the board11
Sign in the OS 12
Go to the EdgeLock SE050 Plug & Trust
middleware test example directory13
Run se05x_minimal test example
List EdgeLock SE050 Plug & Trust
middleware test examples14
Start the ssscli tool15
Close an already openned session
ssscli info16
ssscli disconnect 17

NXP Semiconductors

AN12397

EdgeLockTM SE050 Quick start guide with i.MX6UltraLite

Contents

1	Read this first	3
1.1	Required hardware	3
2	Hardware setup	4
2.1	Mounting the boards	4
2.2	Jumper configuration	4
3	Software setup	6
3.1	Micro-SD card preparation	6
3.2	Drivers	6
3.3	Terminal setup	8
3.4	Booting the i.MX6UltraLite	9
4	Run EdgeLock SE050 Plug & Trust	
	middlewaretest examples	13
5	Using SE050 ssscli tool	. 15
6	Legal information	18

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2019.

All rights reserved.

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

Date of release: 17 December 2019 Document identifier: AN12397 Document number: 534512