SAPSUG

Smart Access Platform Solution User Guide

Rev. 1 — 20 December 2022 User guide

Document information

Information	Content
Keywords	SAPSUG, Smart Access Platform, APK, LPC55S69, Matter, PIN pad, UWB, Fingerprint, Face recognition
Abstract	The purpose of this guide is to help users get familiar with the hardware, updating binaries, and exploring the out of box features

1 Introduction

Smart Access is a scalable platform solution showcasing the latest and renowned smart access technologies. This solution offers reference designs, software source code, one-stop-shop product support, and more in order to facilitate a quick time to market.

The objective of this guide is to assist users in becoming familiar with the hardware, updating binaries, and exploring the out of box features.

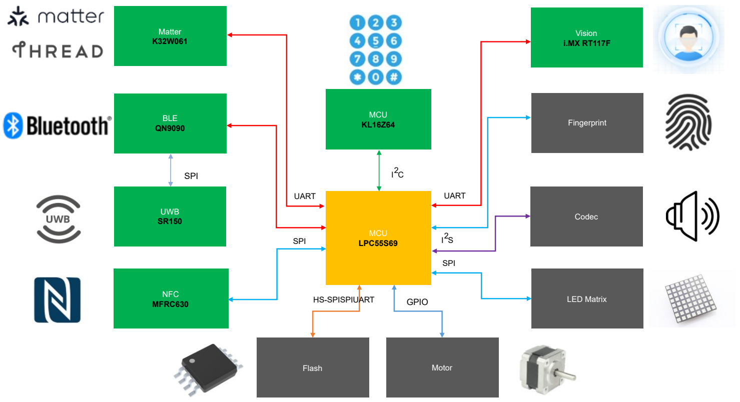


Figure 1. Smart Access Platform Solution block diagram

The Smart Access Platform includes five types of control systems:

- Fundamental Access Control - LPC55S69
  - NFC
  - PIN pad
  - Fingerprint
  - Motor control
  - Voice prompt
- Matter Access Control - K32W041/061:
  - Matter over the Thread Network
- Ultra-Wideband (UWB) Access Control - SR150
  - Based on UWB secure ranging
- Face Access Control - i.MX RT117F
  - Secure 3D face recognition plus liveness detection and anti-spoofing
  - Optional 2D secure and low-cost face recognition
- Bluetooth Low Energy (Bluetooth LE) Access Control - QN9090
  - Remote user management via Bluetooth LE

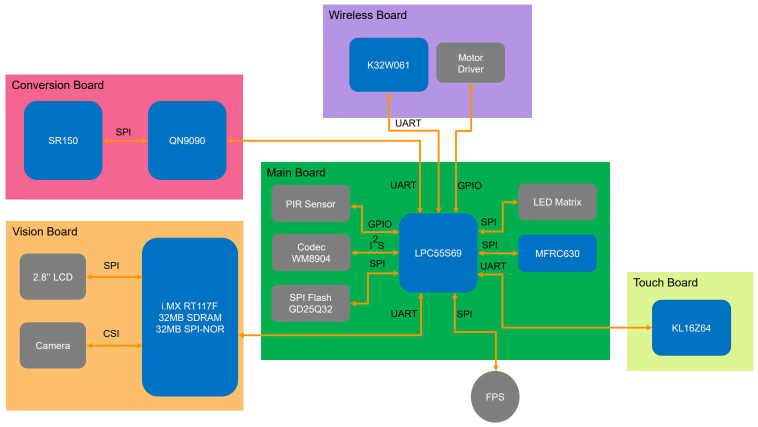


Figure 2. Smart Access Platform Solution hardware block diagram

The Smart Access Platform Solution development kit consists of five PCBAs: Main Board (LPC55S69), Touch Board (KL16Z64), Wireless Board (K32W061), Vision Board (i.MX RT117F), and Conversion Board (QN9090).

- Main Board includes:
  - LPC55S69 acting as the main controller of the whole system
  - MFRC630 acting as the NFC reader
  - GD25Q32 NOR SPI flash for audio files storage
  - WM8904 audio codec
  - BTL160 Fingerprint sensor
- Touch Board includes:
  - KL16Z64 capacitive touch IC which can support up to 16 buttons, by default, 12 buttons are connected (`0` ~ `9`, `*`, and `#`)
- Wireless Board includes:
  - K32W061 to support Matter functionality over Thread Network
  - DRV8837 acting as the motor driver
- Vision Board includes:
  - i.MX RT117F to provide MCU-based face recognition functionality, for more information, see *SLN-VIZN3D-IOT*.
- Conversion Board includes:
  - QN9090 to provide Bluetooth LE functionality
  - SR150 for UWB secure ranging functionality

Figure 3 shows the real PCBAs. As the schematic and design original files of each PCB are fully opened, the user can download them from NXP website. The detailed functions and connectors description of each PCB are introduced in the following sections.

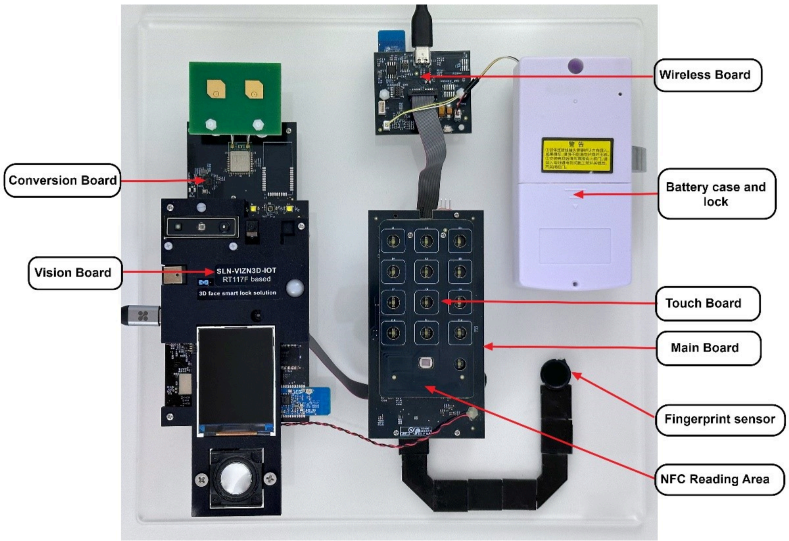


Figure 3. Smart Access Platform Solution PCBAs

2 Features overview

The Smart Access Solution provides various access options as follows:

- To control the door lock smartly, such as PIN pad password input.
- Face ID registration and recognition.
- MIFARE (NFC) card detection.
- Moreover, the user can configure Smart Access Platform Solution system by Android Bluetooth LE APK, which can be found in smart_access_platform.

2.1 APK Installation

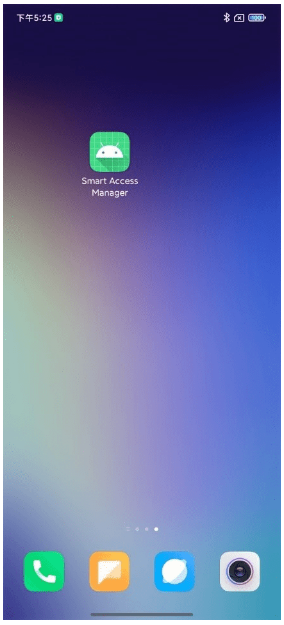


Figure 4. Smart Access Manager

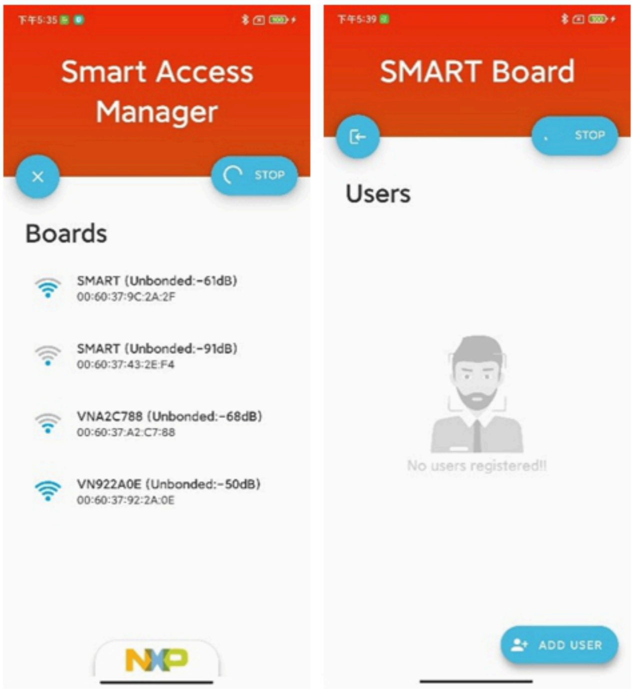
Users can communicate wirelessly to the Smart Access board via Bluetooth LE by installing the “Smart Access Manager” APK on Android smartphone (v8.0 and up) or tablet devices.

- Connect your phone to the computer with a USB cable, download the provided `.apk` file, and allow file transfer.
- Click and drag the `.apk` file from your computer in a folder inside the internal storage of the phone.
- To find that folder, use a file explorer application on the phone, then click the `.apk` file to install it.
- If a security warning appears, click "Settings", and enable the option to install from unknown sources.

The APK is used to create a customized “Smart Access profile” based on the core technologies enabled by the solution. User can select the technologies they are interested in and then create a custom profile with their own PIN code, biometric data, and so on.

2.2 Connect the board

- Open the APK.
- APK scans for the Smart Access Platforms automatically.
- Select the correct device (naming “SMART”) by touching it.
  The selected board is connected and the previously created users are shown Figure 5



SMART (Unbonded:-61dB)
00:60:37:9C:2A:2F

SMART (Unbonded:-91dB)
00:60:37:43:2E:F4

VNA2C788 (Unbonded:-68dB)
00:60:37:A2:C7:88

VN922A0E (Unbonded:-50dB)
00:60:37:92:2A:0E

No users registered!!

Figure 5. Connect the board

2.3 Create a new user with a password

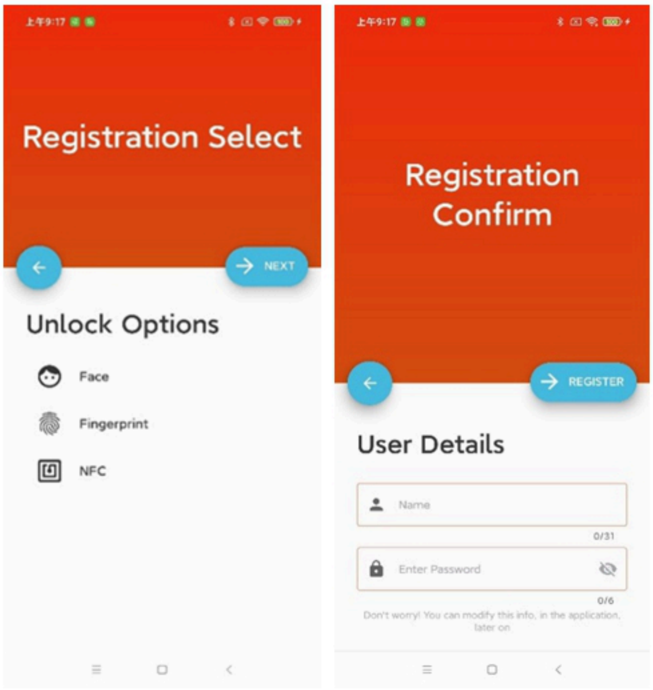
To create a new user:

- Press **ADD USER** button on the bottom-right corner of the screen.

- Press **Next** without any additional unlock option selected.
- Press the **Name** field and type the desired name.
- Press the **Enter Password** field and type the desired password (for simplicity keep the password 123456)
- Press **Register**, the new user is created and appears in the **Users** list.

User can unlock the door in following ways:

- Unlocking the door through APK directly:
  - Select the user from the **Users** list by touching it.
  - Press the **Unlock device** option.
  - Select **Password**.
  - Enter the password correctly (123456) and press the **Unlock** icon.
  - Door lock is opened and audio feedback is sent through the speaker of the board.
- Unlocking the door through PinPad:
  - Enter the right password by touching the corresponding button in the PinPad.
  - After entering the password, tap the confirmation button.
  - Door lock is opened and audio feedback is sent through the speaker of the board.



Don't worry! You can modify this info. in the application, later on

Figure 6. Create a new user with a password

The KL16 implements the PinPad with 12 capacitive touch buttons. The software for the input supports anti-peeping virtual length password.

To delete the previous number, press **E10**.

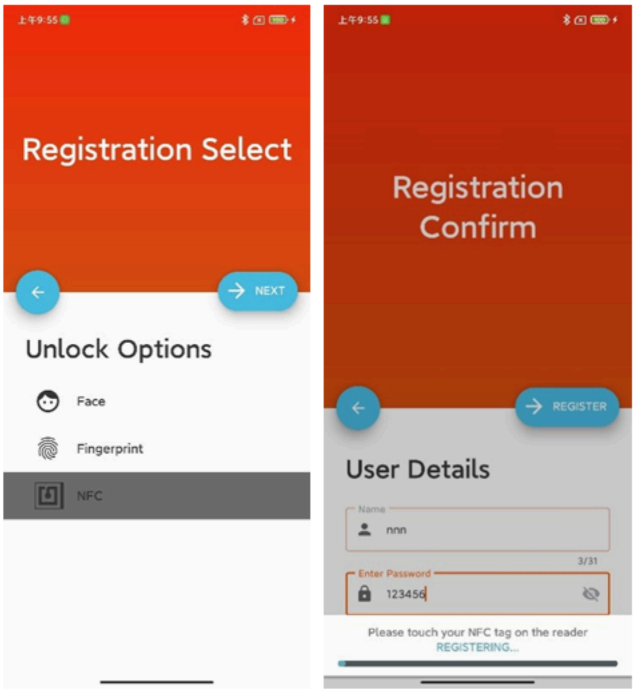
To confirm, press **E11**.

Once user clicks the confirmation button, LPC55S69 starts to compare input characters with recorded passwords. If any recorded passwords match with the input, the LPC55S69 controls the motor to unlock the door. The **alarm** button on the back of the

Main Board, can be quickly clicked to change the motor behavior between **forward first** (the default), **backward first**, and **no action**.

2.4 Create a new user with an NFC card

- Press **ADD USER** button on the bottom-right corner of the screen.
- Select **NFC** from **Unlock Options** and press **NEXT**.
- The phone displays the message **Please touch your NFC tag on the reader**.
- The board prompts the message **Recording card**.
- User must approach an NFC card reader on the Touch Board which is located directly under the **0** key.
- If successfully registered, audio feedback plays **Record card success**.
- New user is shown in the **Users** list.
- To unlock the door, the user must approach the card to the sensor.
- On success, door lock opens and audio feedback is played.



Name: nnn

3/31

Enter Password: 123456

Please touch your NFC tag on the reader

REGISTERING...

Figure 7. Create a new user with an NFC card

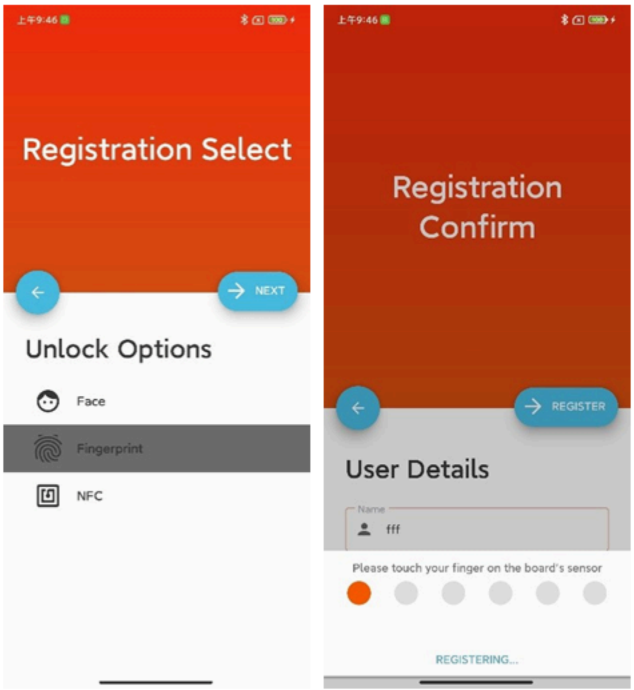
2.5 Create a new user with a fingerprint

- Press **ADD USER** button on the bottom-right corner of the screen.
- Select **Fingerprint** from **Unlock Options** and press **NEXT**.
- Press the **Name** field and type the desired name.
- Press the **Enter Password** field and type the desired password (for example, 123456).
- The phone displays the message **Please touch your finger on the board's sensor**.
- The board prompts the message **Enrolling fingerprint, click the sensor**.
- User must press finger on the Fingerprint six times. User must be persistent, hold the finger for 2-3 seconds, then wait for audio feedback to lift it from the fingerprint sensor.

All information provided in this document is subject to legal disclaimers.

Each time user receives audio feedback from the board: **Enroll fingerprint success, click the sensor again** and progress feedback from the APK.

- The sixth time the user receives audio feedback **Enroll fingerprint success** and the list of users is updated.
- If user touches fingerprint sensor again, the door lock opens, and audio feedback plays through the speaker of the board.



Name: fff

Please touch your finger on the board's sensor

Figure 8. Create new user with a Fingerprint

2.6 Create a new user with a face

- Press **ADD USER** button on the bottom-right corner of the screen.
- Select **Face** from **Unlock Options** and press **NEXT**.
- Press the **Name** field and type the desired name.
- Press the **Enter Password** field and type the desired password.
- The phone displays the message **Please look at the board camera**.
- While face detection is running, the board displays a message that says, **Registering**, with a green background.
- User must approach camera with a Face to complete registration.
- The list in the phone updates and user shows up in the list of users.
- If user is approaching the camera of the board, the recognition is successful. The door lock opens and audio feedback is sent through the speaker of the board.

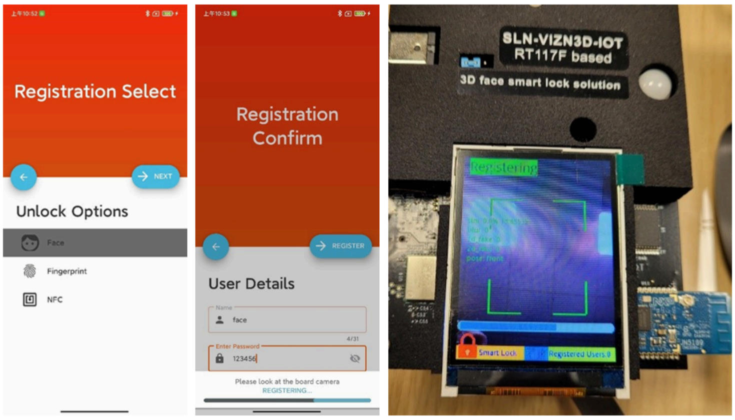


Figure 9. Create a new user with a Face

2.7 Update user name

- Press a user from the **Users** list.
- Press **Update Name**.
- Type in the new **Name** and press **Update**.
- **Users** list should be updated with the new name for the user selected.

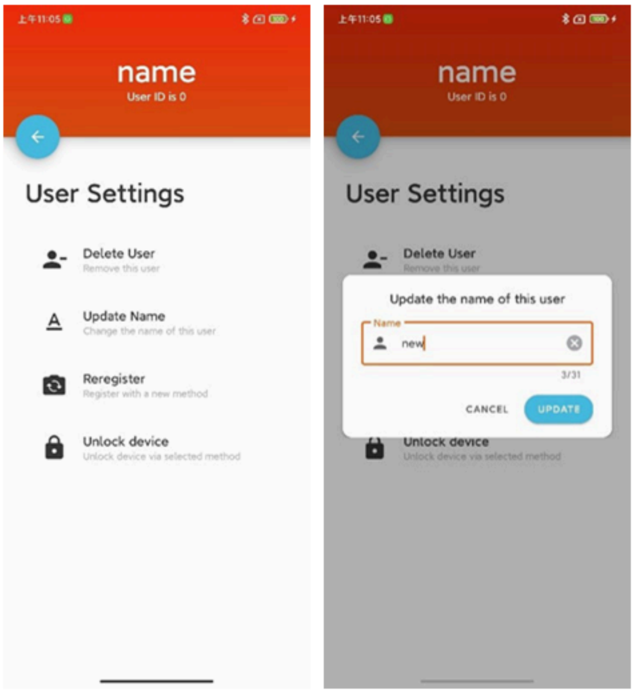
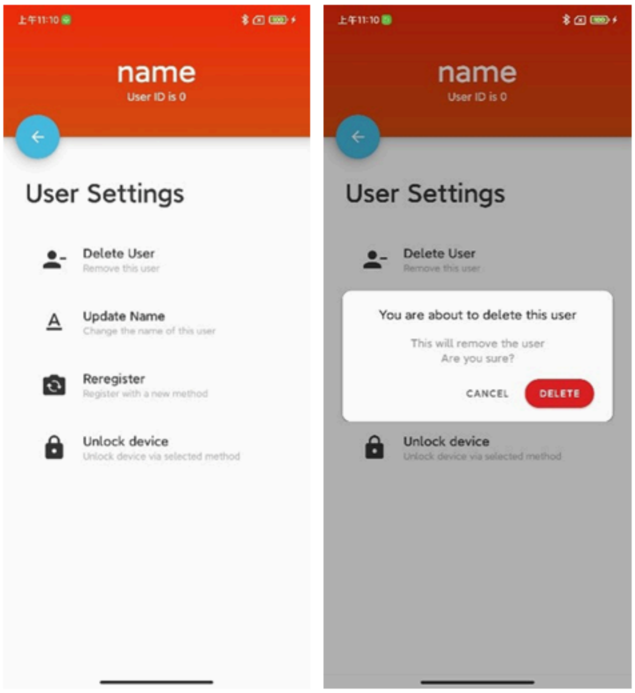

name
User ID is 0
User Settings
Delete User
Remove this user
Update Name
Change the name of this user
Reregister
Register with a new method
Unlock device
Unlock device via selected method
Update the name of this user
Name
new
3/31
CANCEL
UPDATE

Figure 10. Update user name

2.8 Delete a user

- Select a user from the **Users** list.
- Press the **Delete User** option.
- Press **Confirm.** The **Users** list should be updated automatically.



You are about to delete this user

This will remove the user
Are you sure?

Figure 11. Delete User

2.9 Reregister a user

- Press on a user from the **Users** list.
- Press the **Reregister** button and select the option you want to reregister.
- For Password, you must enter both the old password and the new password.
- For NFC, you must approach a new NFC card to the reader.
- For Fingerprint, you must approach finger to the sensor.

•

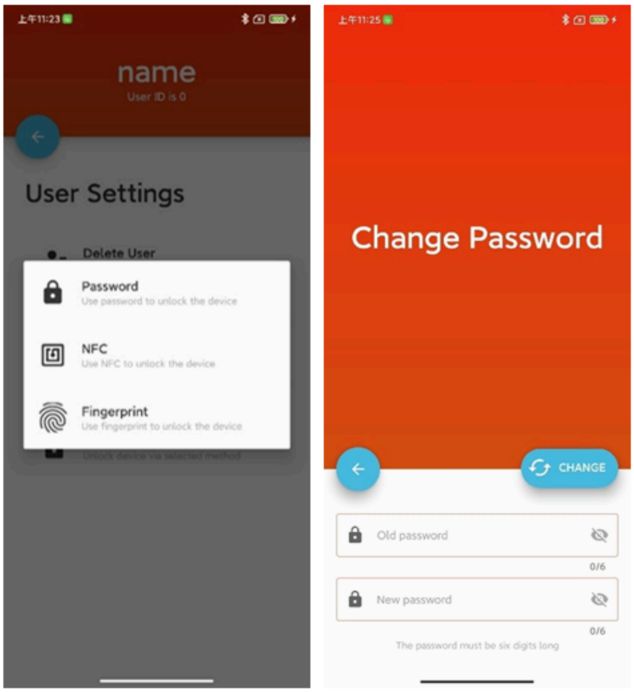

上午11:23
name
User ID is 0
User Settings
Delete User
Password
Use password to unlock the device
NFC
Use NFC to unlock the device
Fingerprint
Use fingerprint to unlock the device
Unlock device via selected method
上午11:25
Change Password
CHANGE
Old password
0/6
New password
0/6
The password must be six digits long

Figure 12. Reregister user with Password

2.10 Control door lock with UWB

Ultra-Wideband (UWB) provides the user with secure precise ranging. The UWB module uses the distance values to compute the logic for which the smart lock is actuated.

The UWB setup on Smart Access Platform consists of Conversion Board (SR150 UWB Transceiver + QN9090 Bluetooth LE Microcontroller). The interacting devices can either be an iOS or an Android phone. The Conversion Board is part of the whole Smart Access board and the others (phones) are used for interaction.

The prerequisites for the iOS phone are:

- iPhone 11 or later.
  Note: *Starting with iPhone 11, Apple phones come with the U1 Ultra-Wideband chip.*
- NXP Trimensions AR from Apple store.
  Note: *Requires iOS 15.0 or later.*
- For further information about iOS UWB capabilities, see Nearby Interaction with UWB.

The prerequisites for the Android phone are:

- Samsung Galaxy S21+, S21 Ultra, S22+.
- Basic UWB demo APK, which can be downloaded from smart_access_platform.
- Android 12 or later with Jetpack UWB library.

Note: *Xiaomi Mi Mix4 with MIUI 13 (Android 12.x) can also work, but does not support Augmented Reality (AR) core.*

The whole point of the Smart Access modularity is to keep the data computing away from the LPC55S69 MCU as much as possible. Therefore, for UWB the whole computing and locking algorithm is based on the QN9090 MCU.

The Generic Access Profile (GAP) from the Bluetooth LE stack is used because the Conversion Board and phone connection are initially established over Bluetooth LE. The GAP has the role of handling device discovery and device connection. The Conversion Board is the peripheral device which sends advertisements (data through which the device can show its identity). The phone is regarded as the central device, which sends the connection request on the same RF channel with different parameters to keep the connection synchronized and persistent. After the connection has been established, the Conversion Board acts as the slave, and the phone is the master. Notice that on the Smart Access Platform there are two Bluetooth LE services (qpps and wireless_uart). To be able to advertise using both services, use the advertising scan and the scan response structures with different UUIDs.

We receive ranging data through the SPI connection between SR150 and QN9090 per iteration. We only send the AT (AT+UWBLOCK and AT+UWBUNLOCK) command through UART to LPC MCU if there is a change of state. As a result, the UART is not overloaded with useless data from its perspective; instead, it only must determine whether to send the locking or unlocking signal to the lock.

The use of both apps is straightforward:

- Open either "NXP UWB" on iOS or "Basic UWB demo" on Android.
- Accept the required permissions.
- Keep the phone oriented with its camera toward the Smart Access board.
  Note: *Keep the phone oriented in the range of -60 degrees to 60 degrees.*
- The phones use their cameras to provide an AR view which targets the UWB board, based on the ranging data.

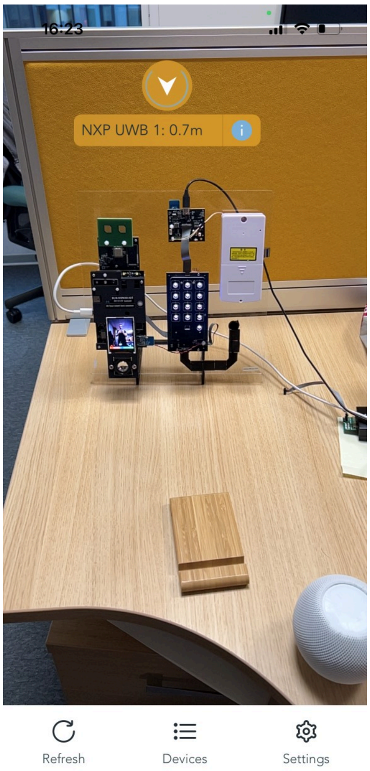


Figure 13. iOS UWB app

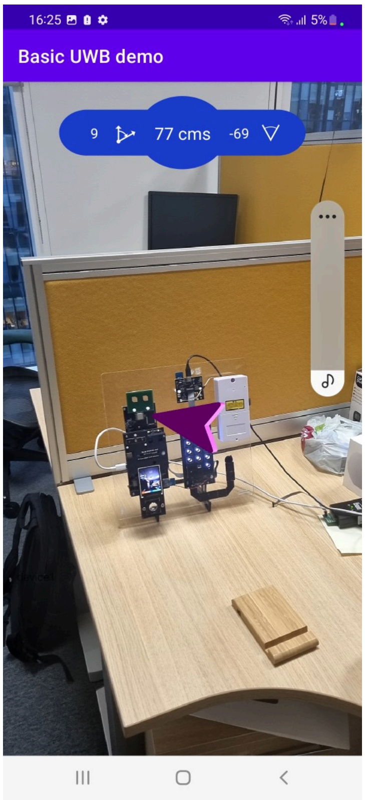


Figure 14. Android UWB app

User can use the UWB phones as follows:

- If user approaches phone within range (~80 cm), door opens.
- If user moves phone further away (~120 cm), door lock closes.
- Furthermore, for data loss connection or screen off, if the lock is in the unlock position, a counter initializes and increases at every consecutive iteration, making the lock to go eventually into the lock position.

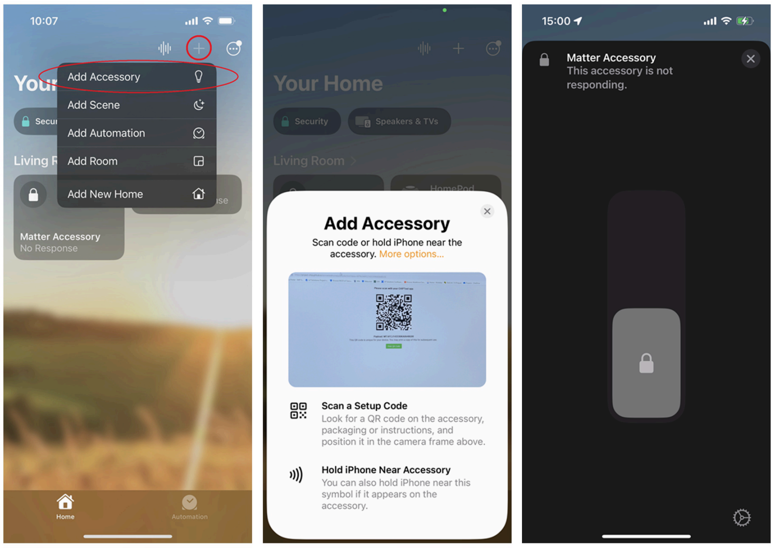
2.11 Control door lock with Matter

To enable Matter capabilities, the Smart Access Platform uses the K32W chip with Thread functionality, in order to achieve a host-less/standalone node. Additionally, Open Thread Border Router (OTBR) and Radio Co-Processor (RCP) are needed, but not supplied by our default accessories.

This guide shows how to set up Apple HomePod as Border Router. This enables commissioning the K32W node and toggling lock and unlock commands via Apple Home application and using voice commands.

- First, do the initial setup of the Apple HomePod according to the official guide by Apple.
- Make sure that the HomePod is version 16.1. Follow the Update HomePod to update.
- Have the Apple Home application installed, connect phone to an Internet enabled network.
- From the Apple Home application, connect the HomePod to the same network.
- With the Smart Access board powered up, make sure that MATTER-3840 shows in Bluetooth devices.

- On the Apple Home application, press the **+** sign in the upper right corner, then press **Add Accessory** to begin commissioning of the K32W.
- When asked for a QR code, scan **connectedhomeip**.
- After device adding succeeds, the K32W Matter accessory can be locked and unlocked via the graphical interface of the application and using voice commands.



Scan code or hold iPhone near the accessory. More options...

Look for a QR code on the accessory, packaging or instructions, and position it in the camera frame above.

You can also hold iPhone near this symbol if it appears on the accessory.

This accessory is not responding.

Figure 15. Apple Home control lock

Official guides on how to add an accessory and how to control them can be found here:

- https://support.apple.com/en-us/HT204893
- https://support.apple.com/guide/iphone/control-accessories-iph0a717a8fd/ios

Note: *The network of the HomePod must not contain other border routers, because the commissioning fails. A mobile hotspot is recommended.*

Note: *To change Wi-Fi network on the HomePod, it must be factory reset.*

To reset the K32W chip in order to pair it with another Apple HomePod, long press the alarm button on the Main Board, and power reset the board. This erases the commissioning keys stored in the K32W flash and also erase the user list on the Main Board.

2.12 Timeout mechanism

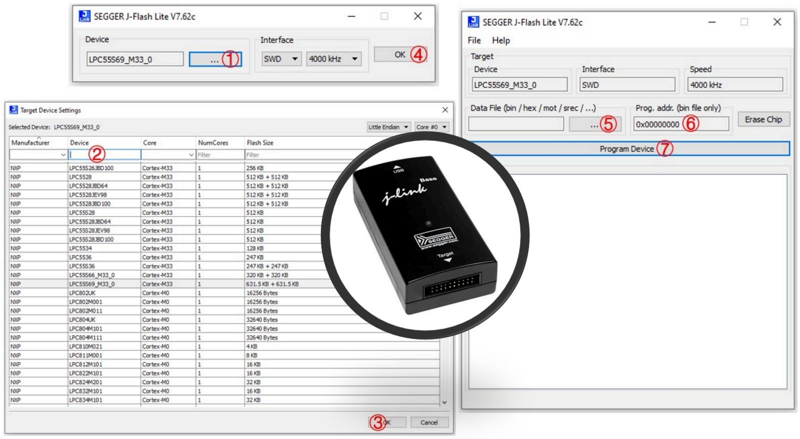
The Smart Access Manager is designed with a timeout feature:

- If user stays idle for 3 minutes while being connected, the application disconnects from the board automatically.
- All the registration methods have a timeout of 2 minutes before automatically returning to the menu and deleting the created user.

3 Update binaries

All MCU firmware programs fully integrated with Arm Serial Wire Debug (SWD) interface, and all the mentioned binaries can be found in smart_access_platform. It is always recommended to update firmware with the latest release for better user experience.

3.1 How to update firmware



SEGGER J-Flash Lite V7.62c

Device: LPC55S69_M33_0 | ... ①

Interface: SWD | 4000 kHz

OK ④

Target Device Settings

Selected Device: LPC55S69_M33_0

Little Endian | Core #0

Manufacturer	Device ②	Core	NumCores	Flash Size
NXP	LPC55S26JBD100	Cortex-M33	1	256 KB
NXP	LPC5528	Cortex-M33	1	512 KB + 512 KB
NXP	LPC5528JBD64	Cortex-M33	1	512 KB + 512 KB
NXP	LPC5528JEV98	Cortex-M33	1	512 KB + 512 KB
NXP	LPC5528JBD100	Cortex-M33	1	512 KB + 512 KB
NXP	LPC55S28	Cortex-M33	1	512 KB
NXP	LPC55S28JBD64	Cortex-M33	1	512 KB
NXP	LPC55S28JEV98	Cortex-M33	1	512 KB
NXP	LPC55S28JBD100	Cortex-M33	1	512 KB
NXP	LPC5534	Cortex-M33	1	128 KB
NXP	LPC5536	Cortex-M33	1	247 KB
NXP	LPC55S36	Cortex-M33	1	247 KB + 247 KB
NXP	LPC55S66_M33_0	Cortex-M33	1	320 KB + 320 KB
NXP	LPC55S69_M33_0	Cortex-M33	1	631.5 KB + 631.5 KB
NXP	LPC802UK	Cortex-M0	1	16256 Bytes
NXP	LPC802M001	Cortex-M0	1	16256 Bytes
NXP	LPC802M011	Cortex-M0	1	16256 Bytes
NXP	LPC804UK	Cortex-M0	1	32640 Bytes
NXP	LPC804M101	Cortex-M0	1	32640 Bytes
NXP	LPC804M111	Cortex-M0	1	32640 Bytes
NXP	LPC810M021	Cortex-M0	1	4 KB
NXP	LPC811M001	Cortex-M0	1	8 KB
NXP	LPC812M101	Cortex-M0	1	16 KB
NXP	LPC822M101	Cortex-M0	1	16 KB
NXP	LPC824M201	Cortex-M0	1	32 KB
NXP	LPC832M101	Cortex-M0	1	16 KB
NXP	LPC834M101	Cortex-M0	1	32 KB

③ OK | Cancel

SEGGER J-Flash Lite V7.62c

File Help

Target

Device: LPC55S69_M33_0

Interface: SWD

Speed: 4000 kHz

Data File (bin / hex / mot / srec / ...): ... ⑤

Prog. addr. (bin file only): 0x00000000 ⑥

Erase Chip

Program Device ⑦

Figure 16. J-Flash Lite update

The firmware update is based on SEGGER J-Link debugger and J-Flash Lite Tool.

1. Open J-Flash Lite Tool.
2. Click **Device** selection button.
3. Enter the device name and to select the correct MCU, click the corresponding row.
4. Click **OK** button to continue.
5. Click file selection button.
6. Choose the corresponding firmware file, either `.bin` or `.hex` format.
   Note: *Input the correct program address for `.bin` files, skip this action for others.*
7. To execute the programing, click **Program Device** button.

3.2 Update LPC55S69 firmware

LPC55S69 contains two firmwares: `LPC55S69_Bootloader_Debug.hex` and `LPC55S69_Application_Debug.hex`.

User can program them through J2 on back side of the Main Board. The device name is `LPC55S69_M33_0`, the program address are `0x00000000` and `0x00008000` separately.

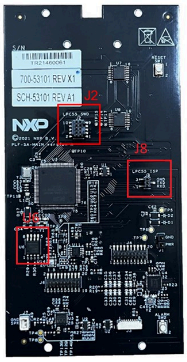


Figure 17. Main Board

3.3 Update LPC55S69 voice files

The default voice files (MP3 format) and python script (`py_generate_eng.py`) used for update are available in GitHub-Audio-Files and GitHub-Python-Script. Ensure that Python 3.7 or newer versions are installed along with `pip` option on PC. Also ensure to install `pyserial` and `pydub` modules via `python3 -m pip install pyserial pydub` command running within the terminal. The bootloader firmware must be programed first.

User can update voice files through J8 on MCU Base Board via UART interface. The user must short (for instance, using tweezers) the pin #1 (CS) and pin #4 (GND) of U6 (external SPI Flash) in order to enter the Update mode. This procedure must be done during the power-on reset of LPC.

Then find the UART port number on PC side (check the list of "Ports" in "Device Manager") and modify the `ser.port` (COMx value) within the Python script (such as line #71) accordingly.

To program 34 voice files into SPI NOR flash, execute the script through the command `python py_generate_eng.py`. The script stops automatically once the audio files are successfully loaded. Then to restart LPC, press the **reset** button.

3.4 Update QN9090 firmware

User can program QN9090 firmware `QN9090_SR150_Debug.hex` through J5 (2x5 header) on back side of Conversion Board. The device name is `QN9090`, the program address is `0x00000000`.

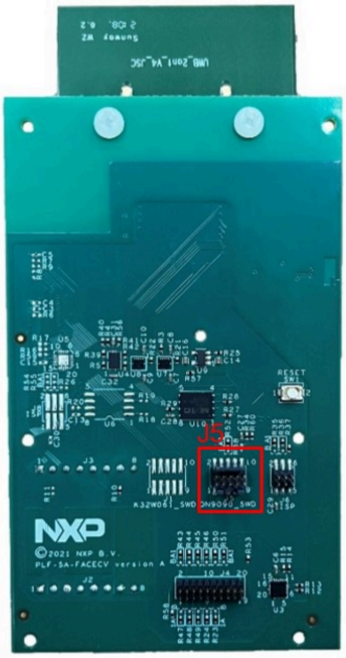


Figure 18. Conversion Board

3.5 Update KL16 firmware

User can program KL16 firmware `kl16_touch.hex` through J1 on back of Touch Board. The device name is `MKL16Z64xxx4`, the program address is `0x00000000`.

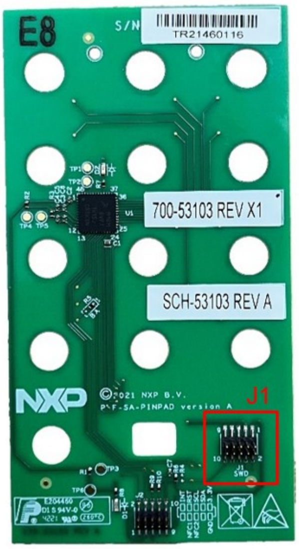


Figure 19. Touch Board

3.6 Update K32W firmware

User can program K32W firmware `K32W061_Debug.bin` through J2 on front side of Wireless Board. The device name is `K32W061`, the program address is `0x00000000`.

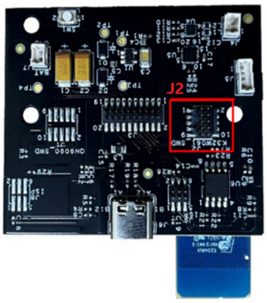


Figure 20. Wireless Board

3.7 Update RT117F firmware

RT117F contains two firmwares: `RT117F_Bootloader_Debug.hex` and `RT117F_Application_Debug.hex`.

User can program them through J204 on back side of Vision Board. The device name is `MIMXRT1172xxxA_M7`, the program addresses are `0x30000000` and `0x30100000` separately.

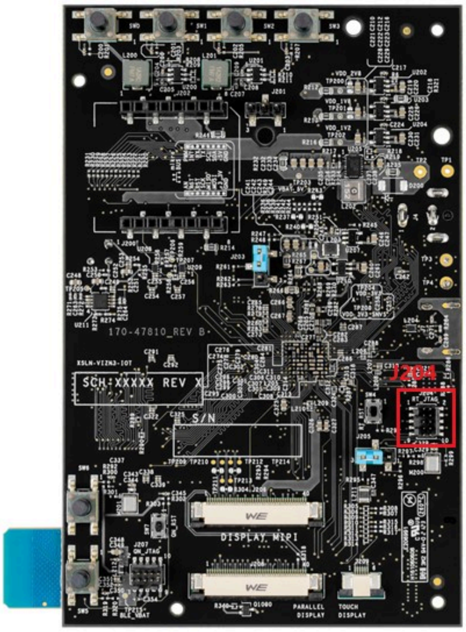


Figure 21. Vision Board

4 Reference

The following references are available to supplement this document. Some of the documents listed below may be available only under a Non-Disclosure Agreement (NDA). To request access to these documents, contact your local NXP Field Applications Engineer (FAE) or sales representative.

- *LPC55S6x data sheet* (document: LPC55S6x)
- *Kinetis KL16 Sub-Family)* (document KL16P64M48SF4)
- *QN9090(T)/QN9030(T) data sheet* (document QN9090(T)/QN9030(T))
- *MFRC630 data sheet* (document MFRC630)
- *K32W061/K32W041 data sheet* (document K32W061/K32W041)
- *Ultra-Wideband Transceiver* (document SR150)

5 Revision history

The Revision history lists the substantive changes done to this document since the initial release.

Table 1. Revision history

Revision number	Date	Substantive changes
0	16 May 2022	Initial revision
1	20 December 2022	• Multiple editorial changes throughout the document • Updated list of Figures, title of figures • Added Legal information • Added and updated Revision history section

6 Legal information

6.1 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.

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 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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that 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 vulnerabilities or may support established security standards or specifications with known limitations. 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.

6.3 Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile — are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

Apple — is a registered trademark of Apple Inc.

Bluetooth — the Bluetooth wordmark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by NXP Semiconductors is under license.

Kinetis — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

Contents

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

For more information, please visit: http://www.nxp.com

Date of release: 20 December 2022
Document identifier: SAPSUG