SLN-VIZNLC-IOT-UG

SLN-VIZNLC-IOT User Guide

Rev. 0 — 20 February 2023 **User guide**

Document information

Information	Content
Keywords	Smart Lock, Smart Access, IoT
Abstract	This document describes the low-cost vision solution, also called SLN-VIZNLC-IOT, and its associated out of box features. The SLN-VIZNLC-IOT turnkey solution provides OEMs with a fully integrated, self-contained, software, and hardware solution

1 Introduction

The SLN-VIZNLC-IOT development kit implements NXP Edge Ready turnkey solution for face recognition-based access control, using an RGB+IR dual camera module. This kit includes the LPC845 low-power control, i.MX RT106F runtime library, and pre-integrated machine learning face recognition algorithms, as well as all required drivers for peripherals, such as memories, cameras, display, Bluetooth Low Energy (Bluetooth LE), and Wi-Fi (optional). This cost-effective, easy-to-use solution facilitates the deployment of highly accurate face recognition with robust liveness detection capability. By leveraging an MCU platform, this solution can deliver the low cost and low power consumption required for battery-powered consumer smart locks, combined with the quick inferencing, and short boot times required to deliver a great user experience.

Target applications:

- *Smart door locks*: For consumer and hospitality applications, including single family homes, multiple dwelling units, and hotels.
- *Access control*: For office and industrial smart-building applications.

1.1 Processor overview

The **i.MX RT106F** is an Edge Ready member of the i.MX RT1060 family of crossover processors, targeting low cost embedded face recognition applications. It features an advanced Arm Cortex-M7 core implementation from NXP that operates at up to 600 MHz to provide high CPU performance and the best real-time responses. This i.MX RT106F based solution enables system designers to add face recognition capabilities easily and inexpensively to a wide variety of smart appliances, smart homes, and smart industrial devices.

The i.MX RT106F processor is licensed to run NXP i.MX RT run-time library for face recognition which may include:

- Unified cross-platform framework.
- Camera drivers, image capture, and pre-processing.
- Face detection, tracking, alignment, recognition with quantified results and confidence measure, and liveness detection.
- Display drivers, 2D graphics accelerator supported.
- Built-in security, bootloader, and application validation.
- All drivers including Bluetooth LE and Wi-Fi.
- USB Mass Storage Device (MSD) updates.
- Factory automation scripts.
- Supported by an MCUXpresso SDK, IDE, and configuration tools.

Note: *The Wi-Fi feature is enabled in the second SW release.*

In addition to the i.MX RT106F, the **LPC845** is another Arm Cortex-M0+ core-based processor. The LPC845 is a low-cost, 32-bit MCU operating at frequencies of up to 30 MHz and supports up to 64 kB of flash memory and 16 kB of SRAM. It features exceptional power efficiency in the low-current mode, and includes rich peripheral complement I/O ports.

2 Recommended configuration

An up-to-date computer that can run MCUXpresso IDE version is required to modify and debug the SLN-VIZNLC-IOT example projects (11.6.1 or newer).

Table 1. Recommended computer configuration

Computer type	OS version	Terminal program
Apple	MAC OS	PuTTY
PC	Windows 7/10/11	PuTTY/Tera Term
PC	Linux	PuTTY

3 Hardware

The SLN-VIZNLC-IOT turnkey solution for face recognition comes with a cost and form-factor-optimized hardware reference designs and access to full software source code. In addition to the i.MX RT106F and LPC845 MCUs, rich peripherals are provided to help develop applications. Figure 1 shows the main hardware resources of the board.

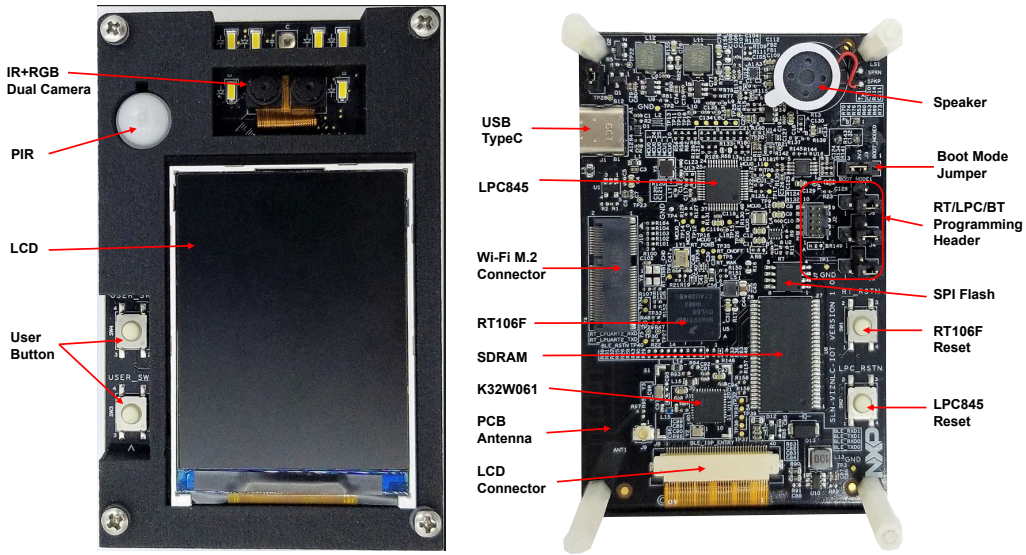

Figure 1. SLN-VIZNLC-IOT components

For more information about the hardware design of the SLN-VIZNLC-IOT, see the *SLN-VIZNLC-IOT Hardware Developer Guide* (document SLN-VIZNLC-IOT-HDG).

CAUTION: *Depending on the mode of operation, the SLN-VIZNLC-IOT kit can emit highly concentrated white or non-visible infrared light which can be hazardous to human eyes. Products which incorporate these devices must follow the safety precautions given in IEC 60825-1 and IEC 62471.*

3.1 MCU

In the SLN-VIZNLC-IOT design, the LPC845 manages the low-power control of the entire system and works as the host MCU. The i.MX RT106F is used to run camera preview, display, and machine learning algorithms.

The power supply of the i.MX RT106F part is controlled by the LPC845. However, by connecting the J11 jumper, an always-on power mode is enabled for easy debugging. See the box highlighted in green in Figure 6.

3.2 LCD

The SLN-VIZNLC-IOT kit, by default, uses a 2.4 inch TFT display (Rocktech RK024HH298) with 240 x 320 resolution, LED backlight, full viewing angle, and RGB interface.

3.3 Speaker

A GSPK1345PN-1M8R1W-L80 enclosed 8 Ω 1.0 W speaker is embedded in the SLN-VIZNLC-IOT kit.

3.4 Camera module

The SLN-VIZNLC-IOT kit uses the GC0308 IR+RGB dual camera module by default. The GC0308 features 640 V x 480 H resolution with 1/6.5-inch optical format, and 4-transistor pixel structure for high image quality and low noise variations. It delivers superior image quality by powerful on-chip design of a 10-bit ADC, and embedded image signal processor. The two GC0308 sensors share a single CSI-DVP interface.

3.5 Wireless radios

Usage condition

The following information is provided per Article 10.8 of the Radio Equipment Directive 2014/53/EU:

- Frequency bands in which the equipment operates.
- The maximum RF power transmitted.

Table 2. Bluetooth frequency and power

PN	RF technology	Frequency range	Maximum transmitted power
SLN-VIZNLC-IOT	Bluetooth	2402-2480 MHz	10 dBm

EUROPEAN DECLARATION of CONFORMITY (Simplified DoC per Article 10.9 of the Radio Equipment Directive 2014/53/EU)

This apparatus, namely SLN-VIZNLC-IOT, conforms to the Radio Equipment Directive 2014/53/EU. For the full EU Declaration of Conformity for this apparatus, see SLN-VIZNLC-IOT.

4 RT106F bootloader

The SLN-VIZNLC-IOT employs a multi-stage boot process to enhance the capabilities of the out-of-box firmware (FW) to include additional functionality. For instance, the ability to flash new firmware images remotely and without a debugging probe for the i.MX RT106F.

4.1 Normal boot

By default, if no boot flags are set during the boot phase, the Normal Boot mode is used. During Normal Boot, the bootloader boots into the "main" out-of-box demo application, meaning the bootloader has jumped to the flash address associated with the application.

4.2 Boot modes

The bootloader supports several different boot-up methods which augment the boot-up behavior. These methods include Normal Boot mode (default) and MSD mode for drag-and-drop flashing of new firmware images. The following sections describe the usage of each different Boot mode and how to enable them. A high-level overview of the purpose of each of these features is discussed in the following sections. For information regarding their usage, creating update payloads, and more, see *SLN-VIZNLC-IOT Software Developer Guide* (document SLN-VIZNLC-IOT-SDG).

4.3 Mass Storage Device

The MSD feature allows the SLN-VIZNLC-IOT to receive firmware updates without a debugging probe like a SEGGER J-Link. Instead, MSD uses USB to emulate an MSD interface like the one that is used for USB flash drives. This feature can be especially useful for marketers or engineers in the field without access to a dedicated debug probe tool. When the kit is powered on, hold down the **MSD pushbutton (SW3)** on the front of the kit to activate MSD mode.

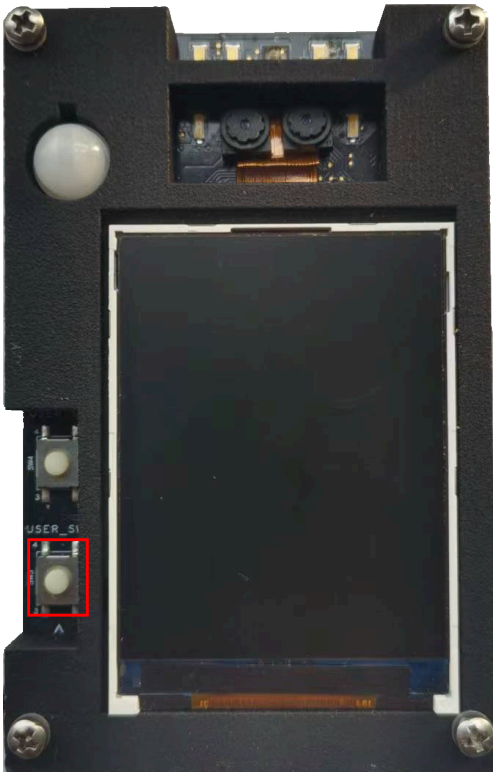

Figure 2. MSD pushbutton (SW3)

Once enabled, the kit enumerates as a USB Storage Device by the OS of your computer.

Figure 3. New USB drive for SLN-VIZNLC-IOT kit

To update the firmware image on your kit, drag and drop the new binary to the USB drive corresponding to your kit. Assuming the binary is properly generated, the bootloader automatically updates the firmware on your device. Flashing a new firmware image results in a pop-up window identical to the one used when copying files to a real USB flash drive device.

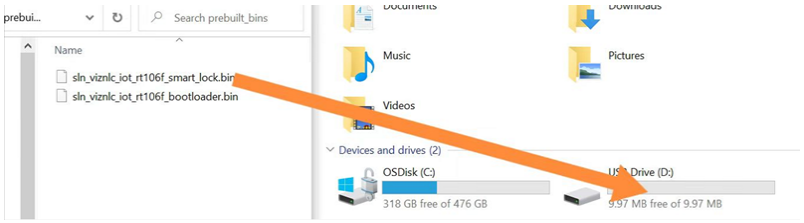

Figure 4. Copying new binary to the USB drive

Note:

- *Keep the i.MX RT106F in always-on power mode, when using MSD.*
- *Only the main application can be updated using MSD. The bootloader cannot be updated using MSD and requires the use of a SEGGER J-Link Debug Probe or the Factory Programming Flow. Instructions on MSD, J-Link-based updates, and the Factory Programming Flow can be found in the SLN-VIZNLC-IOT Software Developer Guide (document SLN-VIZNLC-IOT_SDG).*

For more information regarding MSD mode and its usage, and instructions on generating FW binaries compatible with MSD mode, see the *SLN-VIZNLC-IOT Software Developer Guide* (document SLN-VIZNLC-IOT-SDG).

5 Out-of-box demo application

5.1 Overview

The SLN-VIZNLC-IOT supports **Smart Lock** (default) and **Smart Access** applications. These example applications are built to showcase the complex machine vision, voice prompt, and graphical UI capabilities the kit supports. They also provide a base software platform for rapid integration of unique customer applications and requirements.

The **Smart Lock** application presents an example of a potential smart lock use case. Here, a smart lock device provides custom user experiences using face recognition.

The **Smart Access** application presents an example of a potential smart access use case. Here, a smart access device provides custom user experiences using face recognition.

The main difference between the two applications is the images used for face recognition. Face recognition uses IR images for smart lock applications and RGB images for smart access applications.

If you want to build the smart access application, change the symbol definition from "SMART_LOCK_2D" to "SMART_ACCESS_2D" in the project settings.

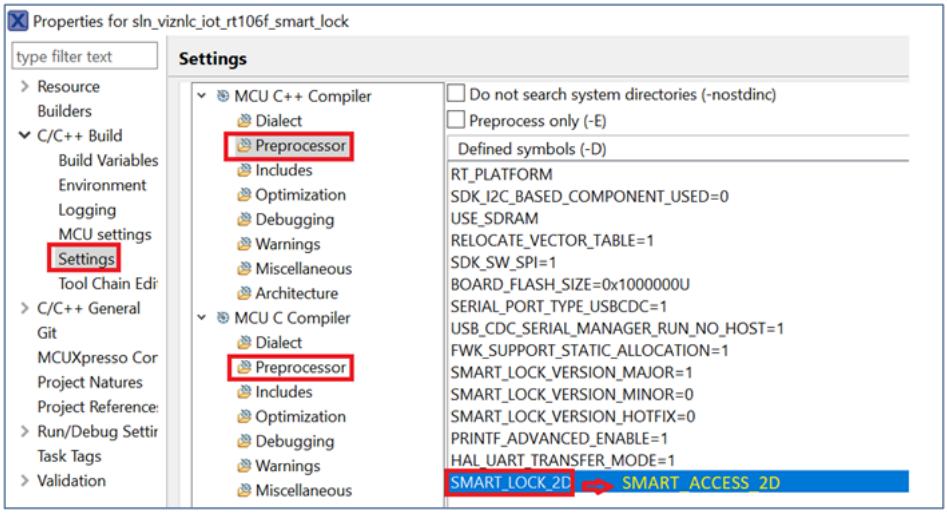

Figure 5. How to build Smart Access application

5.2 Smart Lock

The following sections describe the out-of-box features of smart lock in default. It also applies to smart access application, except for few GUI display.

5.2.1 Power on

Take the USB-A > USB-C cable provided inside the kit. Plug the USB-A end into the USB port on your computer and the USB-C end into the USB port of the kit.

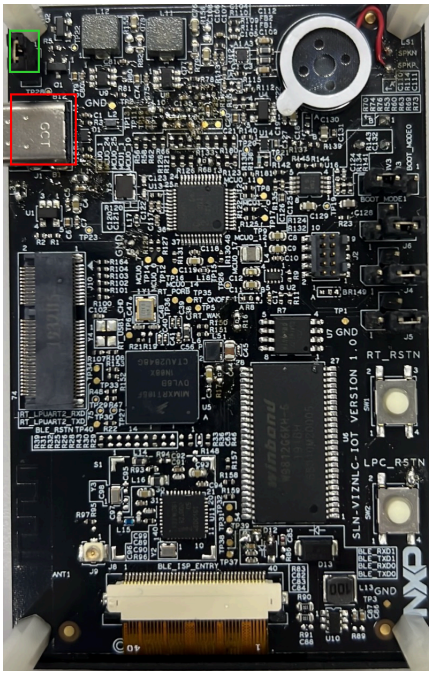

Figure 6. Power on the SLN-VIZNLC-IOT kit

Note: *LPC845 controls the power supply of i.MX RT106F and K32W061. However, an always-on power mode is supported for easy debugging by connecting J11 jumper as shown in the box highlighted in green in Figure 6.*

When powered on, the onboard TFT screen streams video directly from the RGB camera alongside a GUI overlay, providing information such as:

- Locked/Unlocked status whether a face is recognized.
- Current app type (Smart Lock/Access).
- ON/OFF status of Wi-Fi and Bluetooth LE.
- Number of registered users.

Figure 7. The screen with video preview

When J11 is not connected and no PIR event is triggered after a 30 s timeout, the entire system enters the low-power mode. Now, the screen is off and the power supply of i.MX RT106F is cut off. When new PIR event is triggered, the system wakes up immediately.

When J11 is connected, the screen is always on. The i.MX RT106F is powered on all the time, and face recognition does not stop working.

5.2.2 Register a face

To begin registering a new face, press the **Manual Registration button (SW4)** on the kit or use shell command (`add username`). For shell commands, see the description later.

Figure 8. Manual registration button (SW4)

Once pressed, a message indicating registration is taking place pops up at the top of the screen. The speaker plays an audio message confirming that the registration has started.

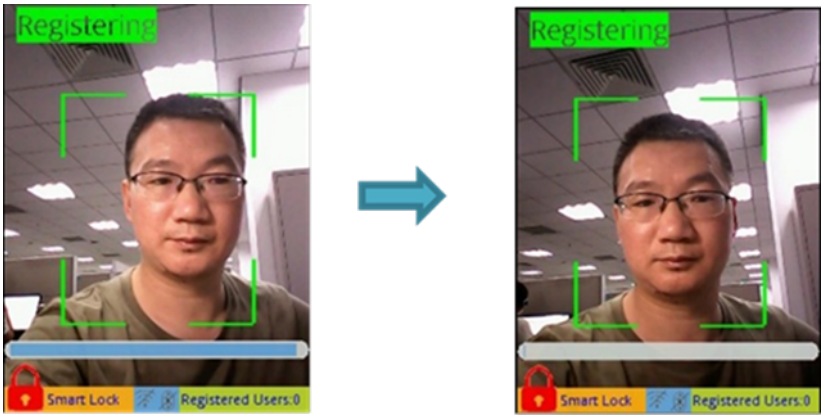

Figure 9. Registering screen

Figure 9 shows that while registration is taking place, the GUI displays:

- A “Registering” message.
- Face alignment guidelines.
- A countdown timer bar.

The guidelines help you align your face correctly during registration, and the countdown timer indicates how much longer it takes until the registration procedure times out and fails.

Figure 10. Registration Timeout

As an additional measure to aid in registering your face, the kit even plays a warning audio prompt, saying "Look at Camera," until your face is properly pointed toward the camera, if too much of the side of your face is exposed during the registration process.

Should your face fail to register, simply press the **SW4** button again to retry.

Once your face is successfully registered, the kit displays the message "Registration Successful", and a unique identifier is assigned to your face. The number of registered users is also updated automatically.

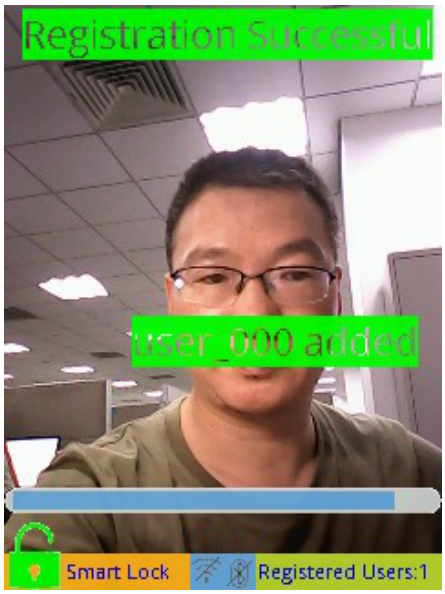

Figure 11. Registration Successful

5.2.3 Recognize a face

Once registered, the kit displays the message "Recognition Successful" and plays a corresponding audio file when a recognized face is detected.

Figure 12. Recognition Successful

5.2.4 Deregister

If the application recognizes a face, the user may delete it using **Manual Deregistration button (SW3)**.

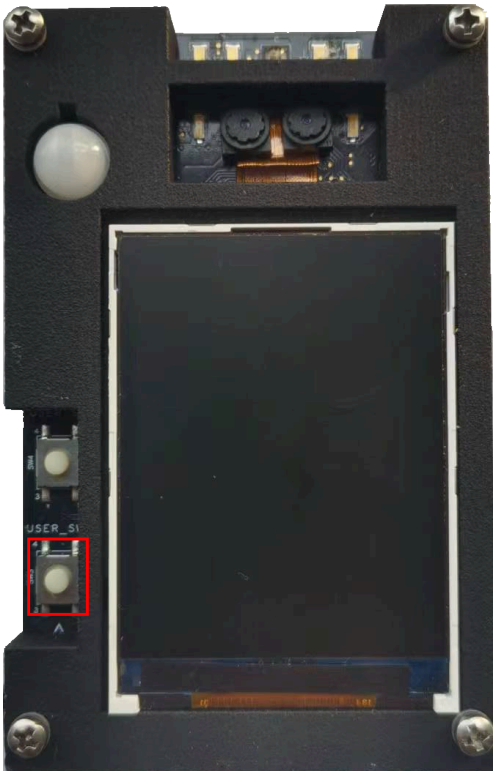

Figure 13. Manual Deregistration Button (SW3)

This process permanently deletes the face.

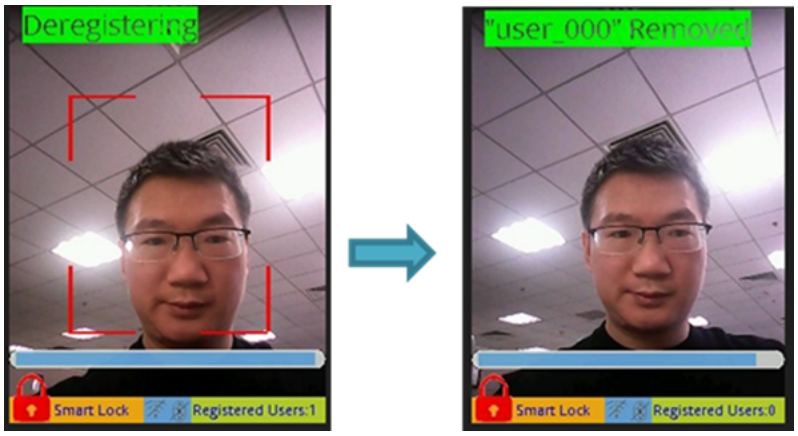

Figure 14. Deregistering Screen

5.2.5 Liveness detection and anti-spoofing

The Liveness detection and anti-spoofing features of the SLN-VIZNLC-IOT are switched on by default. Therefore, enabling the system to distinguish between your actual face and a printout or phone display image of your face.

This feature helps to defend against some of the most frequent face recognition "spoof" attacks. One such spoof attack is when a malicious actor uses a picture of someone to gain access to their face-protected materials. The malicious actor does this spoof by requiring an actual face of the user to unlock the system rather than simply a picture of their face.

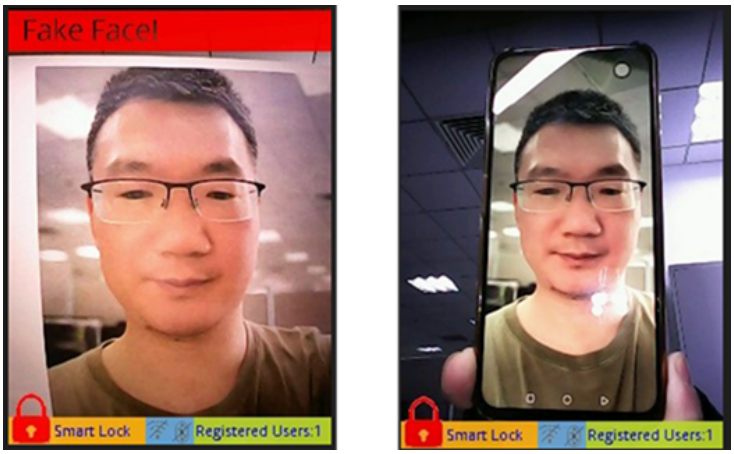

Figure 15. Printed picture and phone display spoof attack

As shown in the Figure 15, using a phone display or a printed picture of a face does not trigger the “Recognition Successful” message.

5.2.6 Shell commands

The smart lock/access out-of-box FW provides additional configuration options via a shell interface hosted over a USB virtual COM connection.

To connect to the shell interface, use a serial terminal emulator program like PuTTY, Tera Term, or Minicom. Configure the serial connection settings as follows and make sure to use the COM port corresponding to your kit:

- Speed: 115200
- Data: 8 bit
- Parity: None
- Stop bits: 1 bit
- Flow control: None

The shell commands for the smart lock/access application are listed in Table 3.

Table 3. Shell commands

Shell command	Meaning
help	List all the registered commands
exit	Exit program
version oasis	Get the version of the current oasis library
version	Get the version of the current software
reset	Reset the board
save	Save all registered users to flash
add *username*	Add user
del -n <*username*>	Delete user by user name
del -i <*id*>	Delete user specified by id
del -a	Delete all users
rename <*id*>*new name*	Rename user based on id
list	Prints a list of all users currently saved in the face database
list -c	Print the number of users currently saved in the face database
log_level <*none/error/debug/info/verbose*>	Set the log level
log_level	Get the log level
display_output <*UVC/panel*>	Set the display device
display_output	Get display device
display_output source <*RGB/2DIR*>	Set display source
display_output source	Get display source
ir_pwm <*value*>	Set PWM pulse width for IR LED, value should be between 0 (inactive) and 100 (max)
white_pwm <*value*>	Set PWM pulse width for white LED, value should be between 0 (inactive) and 100 (max)
volume <*value*>	Set volume of the speaker,value should be between 0 (muted) and 100 (max)
oasis <*start/stop*>	Start/stop oasis
oasis info	Get the state of oasis
facerec_threshold	Show the current face recognition threshold
facerec_threshold <*value*>	Set the face recognition threshold

5.2.7 Remote registration

The Smart Lock/Access application allows you to register and de-register faces locally using the onboard pushbuttons or serial commands. This application also supports remote face management over Bluetooth LE using an Android phone/tablet application. The **Smart Lock Manager** app for Android smartphones and tablets provides a user-friendly interface where you may remotely register new faces and manage faces that are already registered in the SLN-VIZNLC-IOT local face database. This section describes some major features provided by this dedicated Android app.

5.2.8 Installing the Smart Lock Android app manually

The pre-compiled APK and the complete source code for the Smart Lock Manager app are available on the SLN-VIZNLC-IOT under the Software and Tools section. They can also be obtained from GitHub repository.

To install the Smart Lock Manager app on your Android device, store the `Smart_Lock_Manager.apk` file on your smart device. First, download it directly from the web browser of your device or by transferring it from your computer to your device. Ensure that the third-party apps are allowed on your Android device before you install it. Search for the APK file location on your Android device using the **Files** app. Tap it to authorize installation from the file manager, and then wait for the installation to complete.

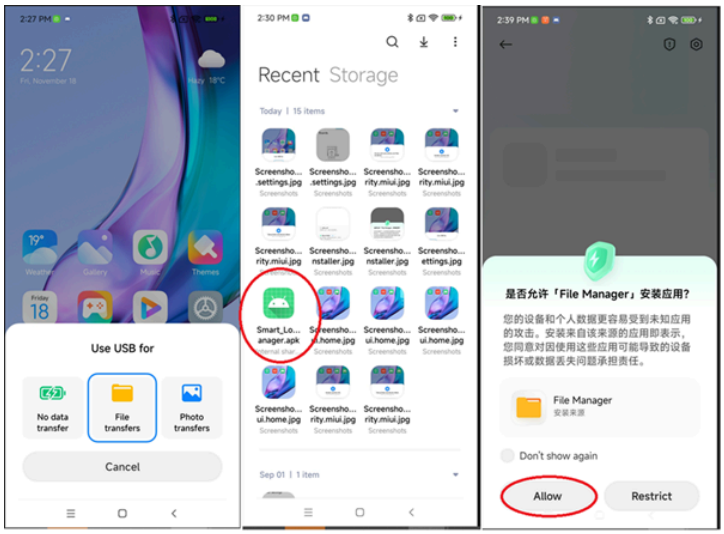

Figure 16. Installing the Smart Lock Manager app for Android

After launching the Smart Lock Manager app for the first time, you are prompted to authorize the app to access the camera of your smart device, your location to enable Bluetooth, and your photographs. It is important that you approve those services to connect new kits or register new faces.

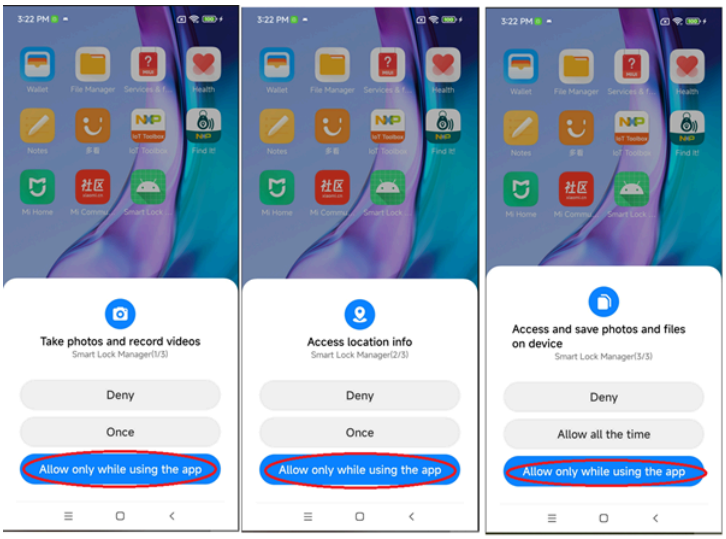

Figure 17. Allowing camera, location, and photograph access

If Bluetooth radio is off, the app prompts you to enable it on your Android device. To pair your kit with the Smart Lock Manager app and remotely manage the registered faces stored in the SLN-VIZNLC-IOT local database, Bluetooth connectivity is required.

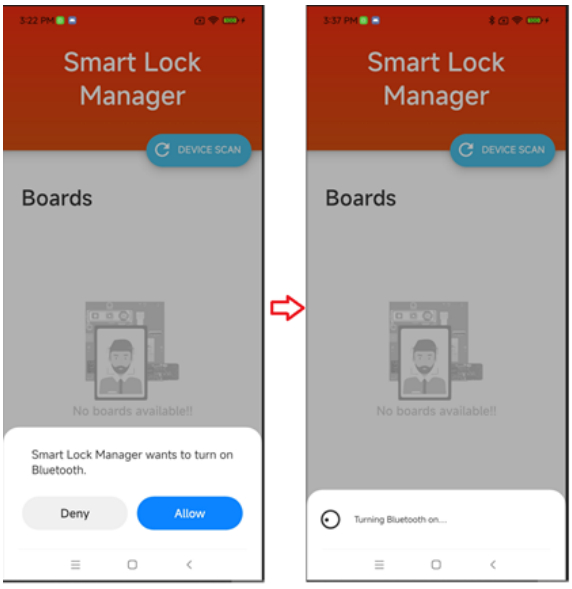

Figure 18. Enabling Bluetooth

Note: *The Smart Lock Manager app is intended for use as an evaluation tool and as a reference/boilerplate upon which a customized smartphone/tablet companion application is built.*

5.2.9 Managing kits

To interact with your SLN-VIZNLC-IOT kit, pair your kit with the Smart Lock Manager app which can be done from the main menu of the app. To detect the VIZNLC devices that are within the Bluetooth range of your Android device, press the "DEVICE SCAN" button.

Note: *The Bluetooth LE feature of the SLN-VIZNLC-IOT is enabled by default, so the app automatically discovers the kit shortly after powering up.*

Any VIZNLC kits found while the search is in progress are shown in the "Device" list. Select the device that you want to add to your list of supported smart locks.

Note: *For easy identification, each kit transmits a distinct Bluetooth SSID that begins with VN and includes its serial number.*

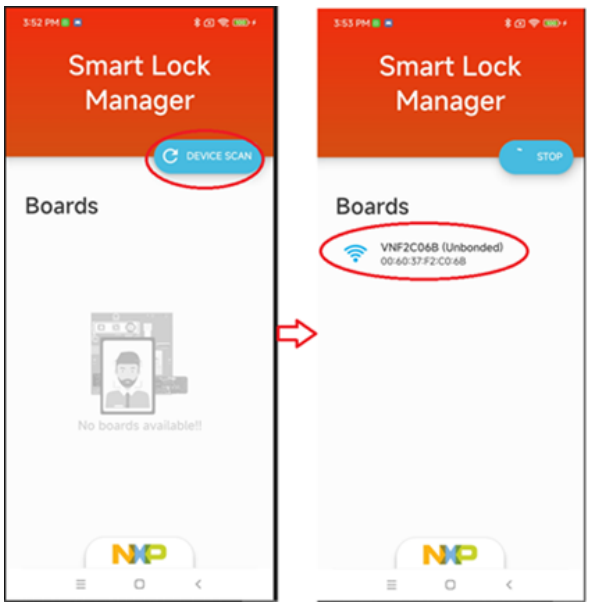

Figure 19. Pairing with a new board

To secure the connection between your Android device and the SLN-VIZNLC-IOT kit that you want to access, enter a password before logging in to your device. This password is set to `000000` by default.

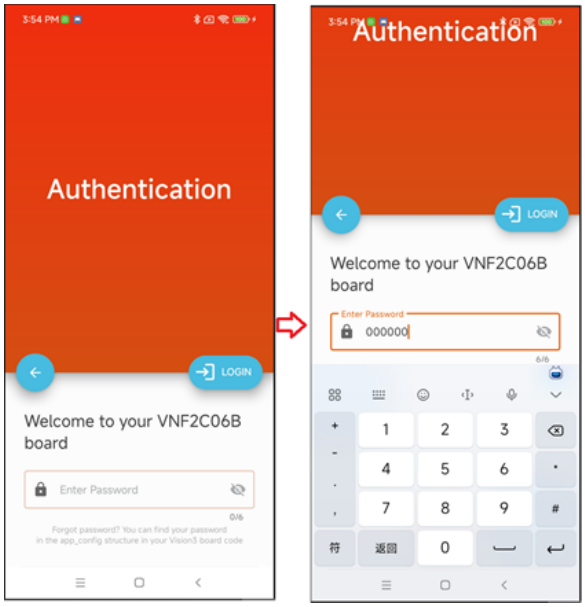

Figure 20. Smart lock password screen

The Android app displays a list of users who are currently registered in the kit local face database when securely connected with the VIZNLC device.

Note: *Only one device can be connected and controlled at a time.*

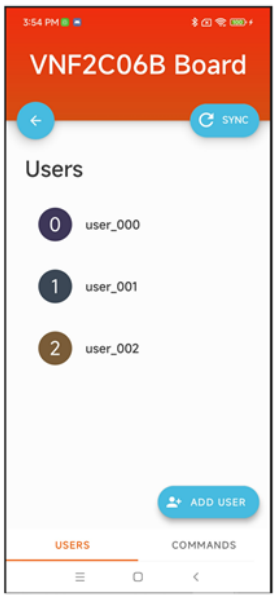

Figure 21. Smart lock list of users currently registered

By selecting the “Change Password” command, you can modify the password previously registered to secure the Bluetooth connection with the smart lock device. Enter the old password and the new password and click “Change”. The app automatically returns to the previous "Smart Lock Control" menu. A message is displayed in green at the bottom of the screen to confirm that the new password is successfully pushed to the device.

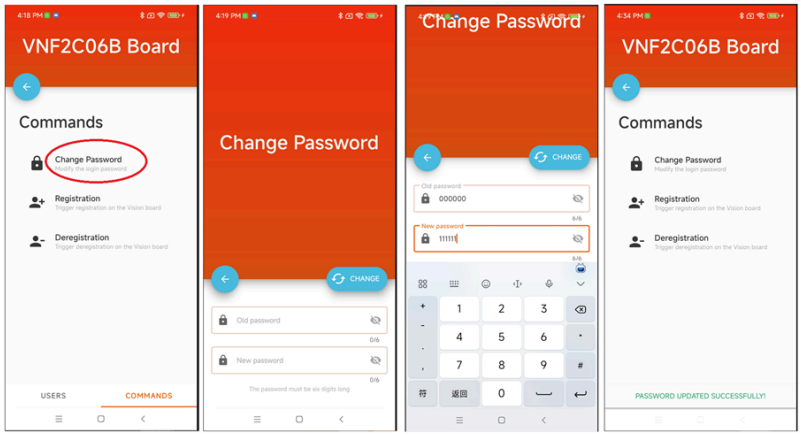

Figure 22. Changing smart lock password

5.2.10 Managing users

5.2.10.1 Adding users

One of the key features of the Smart Lock Manager app is registering new faces remotely from any Android device and uploading them to the VIZNLC device via Bluetooth. To start the remote registration process, tap the “ADD USER” button, as shown in Figure 23.

The Smart Lock Manager app automatically displays the live view of the front camera of your Android device. A green bounding box appears when your face is detected. To register your face, click the shutter icon at the bottom of the camera view while the box around your face is green.

The app asks you to type a name of the new face. Tap the blue checkmark icon and select “REGISTER” to finalize the registration.

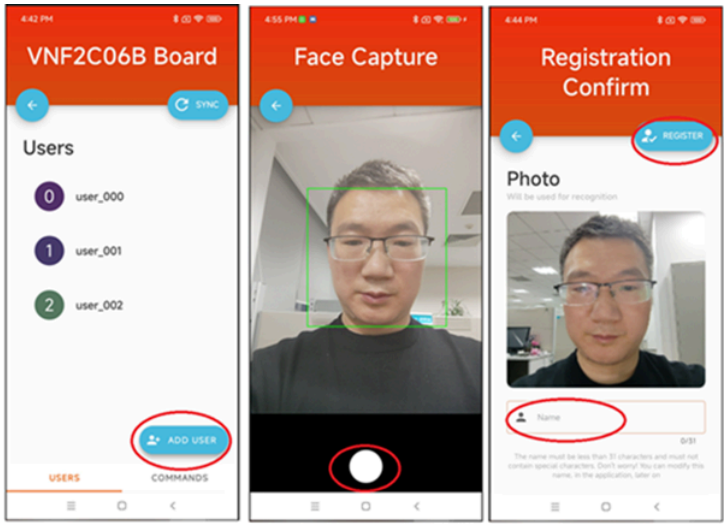

Figure 23. Registering a new face remotely

The app automatically returns to the list of registered users for the selected smart lock device, where the recently added face has been added via the Android device.

To trigger a local registration remotely, go to the "Commands" menu and choose the "Registration" option. It has the same effect as pressing the local **Registration button (SW4)** on the kit.

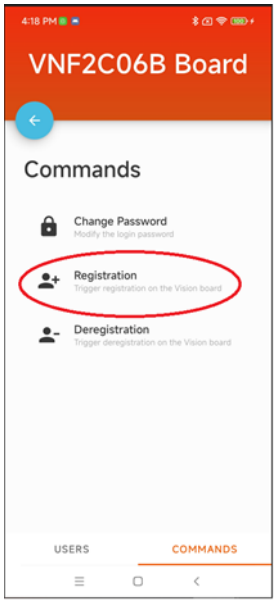

Figure 24. Trigger a local registration remotely

Note: *If you locally register, update, or delete a face using the smart lock device, select the “Sync” option in the app. This option alerts the Android device of any modifications made locally on the kit for users. A sync is automatically performed when you connect to a board.*

Figure 25. Sync option to update the face databases in the Android app and the kit

5.2.10.2 Modifying users

The Smart Lock Manager app also enables you to modify registered users. From the list of the Smart Lock registered users, select the user that you want to modify. The available options are "Delete User", "Update Name", and "Reregister".

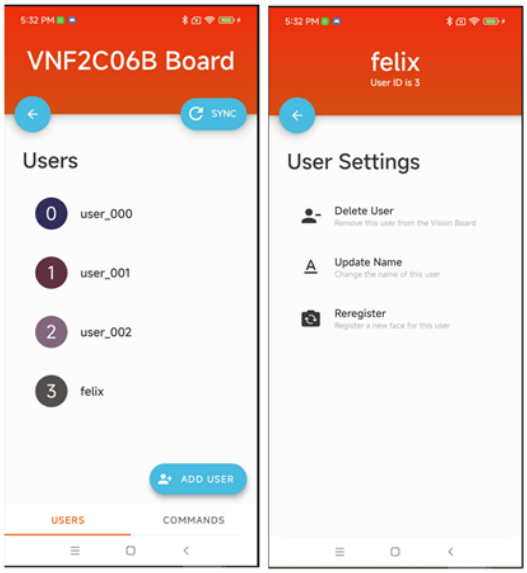

Figure 26. Managing registered users

To modify a name of the user, choose "Update Name", type the new user name, and select "Update" to save the information.

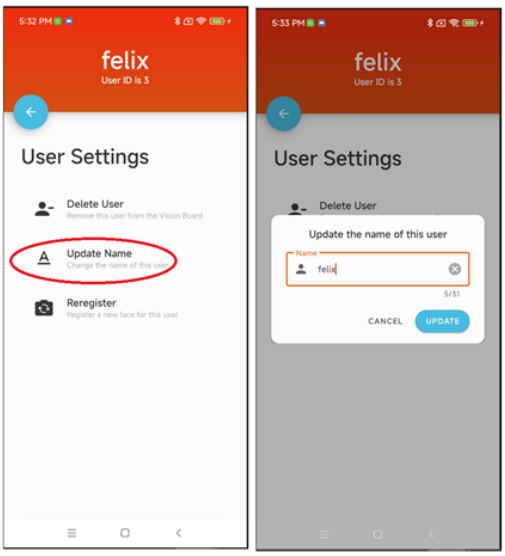

Figure 27. Renaming a registered user

Note: *If you locally register, update, or delete a face using the smart lock device, select the "Sync" option in the app. This option alerts the Android device of any modifications made locally on the kit for users. A sync is automatically performed when you connect to a board.*

5.2.10.3 Deleting users

In addition to adding and modifying registered users, the Smart Lock Manager app also allows you to delete registered users. From the list of the Smart Lock registered users, select the user that you want to delete. To delete the user, select the "Delete User" option, and confirm by selecting "DELETE" to remove the user.

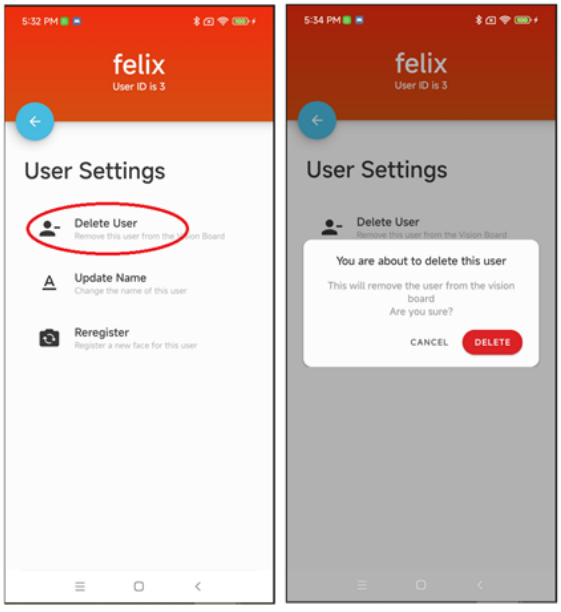

Figure 28. Remote deletion screen

To trigger a local deregistration remotely, go to the "Commands" menu and choose the "Registration" option. It has the same effect as pressing the **Deregistration button (SW3)** on the board.

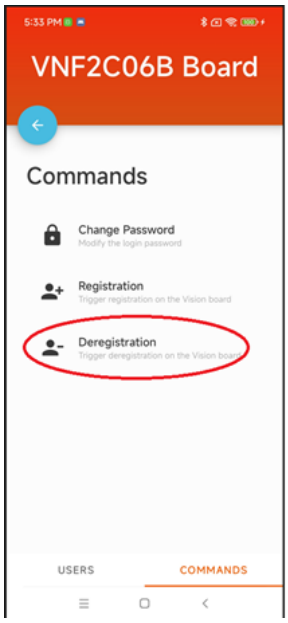

Figure 29. Triggering a local deregistration remotely

Note: *If you locally register, update, or delete a face using the smart lock device, select the "Sync" option in the app. This option alerts the Android device of any modifications made locally on the kit for users. A sync is automatically performed when you connect to a board.*

6 Troubleshooting

6.1 Unable to register

This section describes the steps that can be taken to help debug potential points of failure when attempting to perform face registration and recognition. If after following these steps you are still unable to determine the root of the problem, head over to the NXP forum dedicated to SLN-VIZNLC-IOT kit section to request for more help.

6.2 Adjust face proximity and position

It is crucial that the cameras can see the *face identifiers* since face recognition uses these identifiers to determine the face being looked at. Often, an improper face angle and/or the proximity to the camera can cause registration to fail. Figure 30 shows a few examples of improper usage.

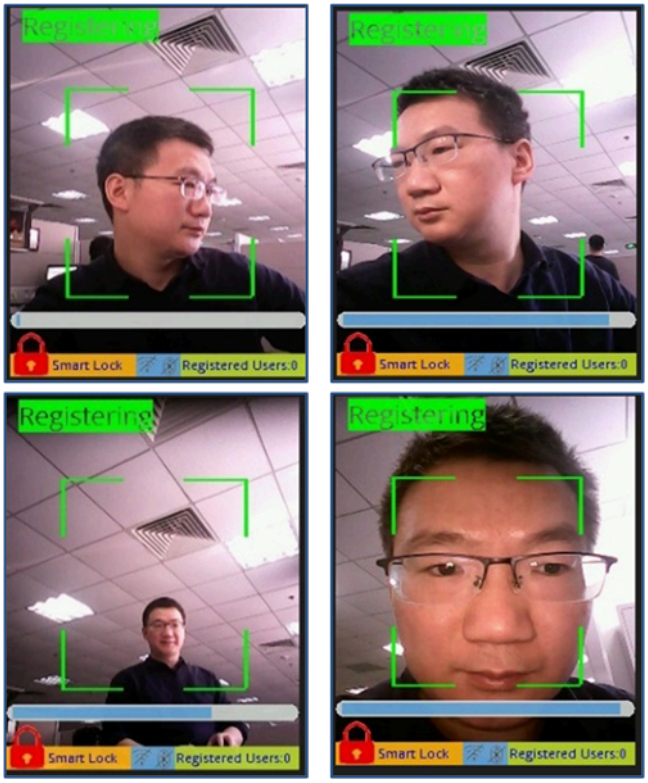

Figure 30. Improper face angle and proximity

To detect your face correctly, the face must:

- Take up most of the bounding box.
- Be centered inside the bounding box.
- Stare straight at the camera.
- Move slowly from left to right and up to down to ensure the proper face angle.
- Be under proper lighting conditions.

The dual camera module is calibrated to scan a face properly between 0.3 m and 1.0 m. If the face of the user is positioned closer or further away, the application does not generate a "Recognition Successful" or “Registration Successful” message.

6.3 Debug using log messages

Log messages can provide useful information when debugging registration issues, especially when it comes to debugging issues with liveness detection. The onscreen indicators can be helpful in identifying what is going wrong during the registration.

Connect the debug UART as shown in Figure 31, if necessary.

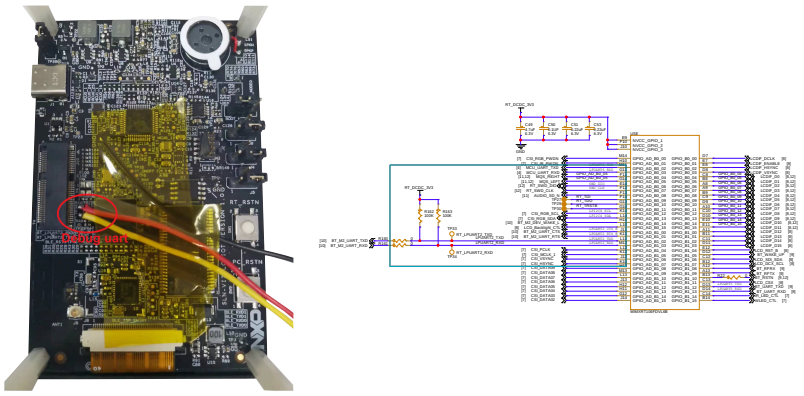

Figure 31. RT106F debug UART on LPUART2

Table 4. Debug using log messages

Message	Meaning	Solution
OK	A face is detected	N/A
No Face	No face is detected	N/A
Small Face	Face is too far away	Come closer to the camera
Light Face	Face is too bright	Adjust environment brightness
Dark Face	Face is too dark	Adjust environment brightness
Blurry Face	Face is out of focus	Hold still when looking at camera
Side Face	Face is improperly angled	Look directly at the camera

7 References

The Table 5 lists the references that 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 Application Engineer (FAE) or sales representative.

Table 5. References

Links	Description
MCUXpresso IDE for NXP MCUs	MCUXpresso IDE Download
MCUXpresso IDE User Guide	MCUXpresso IDE User Guide
SLN-VIZNLC-IOT-SDG	SLN-VIZNLC-IOT Software Developer Guide
SLN-VIZNLC-IOT	SLN-VIZNLC-IOT Home Page
https://github.com/NXP/mcu-viznlc	SLN-VIZNLC-IOT GitHub

8 Acronyms

Table 6 lists the acronyms used in this document.

Table 6. Acronyms

Acronym	Definition
TFT	Thin Film Transistor

Table 6. Acronyms...*continued*

Acronym	Definition
DVP	Digital Video Port
HAL	Hardware Abstraction Layer
OoBE	Out of Box Experience
MSD	Mass Storage Device
VIZNLC	Vision low cost
FW	Firmware
SW	Software
HW	Hardware
PIR	Passive InfraRed
IR	InfraRed
GUI	Graphical User Interface

9 Revision history

The Table 7 lists the substantive changes done to this document since the initial release.

Table 7. Revision history

Revision history	Date	Substantive Changes
0	20 February 2023	Initial release

10 Legal information

10.1 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.

10.2 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.

10.3 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 and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) 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.

Contents

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

Date of release: 20 February 2023
Document identifier: SLN-VIZNLC-IOT-UG