AN14238

Get started with EdgeLock A30 secure authenticator support package

Rev. 1.0 — 15 January 2025

Application note

Document information

Information	Content
Keywords	EdgeLock A30 secure authenticator, NX Middleware
Abstract	This document is the entry point for getting familiar with EdgeLock A30 support package contents and how to get started with them.

1 About EdgeLock A30 secure authenticator

EdgeLock A30 is a secure authentication IC for IoT platforms, electronic accessories and consumable devices such as home electronic devices, mobile accessories and medical supplies.

EdgeLock A30 supports on-chip ECC key generation to make sure that private keys are never exposed outside the IC. It performs cryptographic operations for security critical communication and control functions. EdgeLock A30 is Common Criteria EAL 6+ security certified with AVA_VAN.5 on product level and supports a generic Crypto API providing AES, ECDSA, ECDH, SHA, HMAC and HKDF cryptographic functionality.

- Asymmetric cryptography features support 256-bit ECC over the NIST P-256 and brainpool P256r1 curves.
- Symmetric cryptography features support both AES-128 and AES-256.
- PKI-based mutual authentication based on the Sigma-I protocol.
- Symmetric three pass Mutual Authentication protocol compatible with NTAG42x and MIFARE DesFire EV2, DesFire EV3 and DesFire Light.
- Secure messaging channel using either AES-128 or AES-256 session encryption/decryption and MAC.

The Common Criteria security certification ensures that the IC security measures and protection mechanisms have been evaluated against sophisticated noninvasive and invasive attack scenarios.

- A30 supports an I^{2}C contact interface and has two additional GPIOs.
- A30 supports a low-power design, and consumes only 5 µA at Deep-Power-Down mode when an external VDD is supplied.

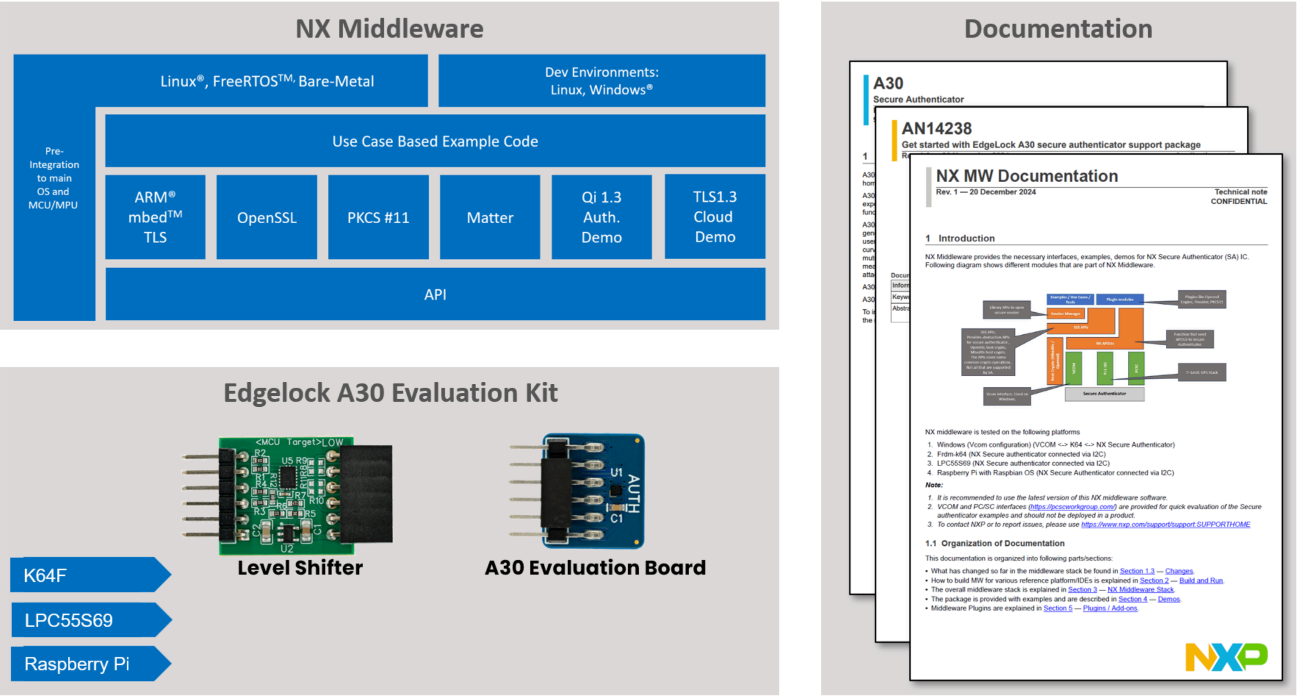

NX Middleware
Linux®, FreeRTOS™, Bare-Metal
Dev Environments: Linux, Windows®
Pre-Integration to main OS and MCU/MPU
Use Case Based Example Code
ARM® mbed™ TLS
OpenSSL
PKCS #11
Matter
Qi 1.3 Auth. Demo
TLS1.3 Cloud Demo
API
Edgelock A30 Evaluation Kit
K64F
LPC55S69
Raspberry Pi
Level Shifter
A30 Evaluation Board
Documentation
A30
Secure Authenticator
AN14238
Get started with EdgeLock A30 secure authenticator support package
NX MW Documentation

Figure 1. EdgeLock A30 support package overview

Delivered as a ready-to-use solution, the EdgeLock A30 includes a complete product support package that simplifies design-in and reduces time to market. The EdgeLock A30 support package offers:

- EdgeLock A30 evaluation kit
- NX Middleware
  - Software enablement for MCUs and MPUs.
  - Integration with the most common cryptographic libraries like OpenSSL, Mbed TLS and PKCS #11.
  - Multi-platform software enablement targeting freeRTOS and Linux as well as Windows as evaluation platform.
  - Sample code for major IoT and secure authentication use cases.
- Documentation

This document lists the existing material within EdgeLock A30 support package, organized in the following sections:

- Section 2 EdgeLock A30 evaluation kit
- Section 3 Supported MCU/MPU boards
- Section 4 NX Middleware
- Section 6 Supported EdgeLock A30 documentation

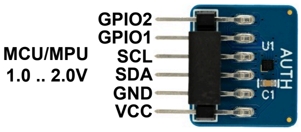
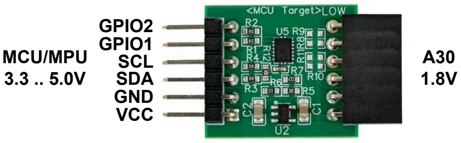
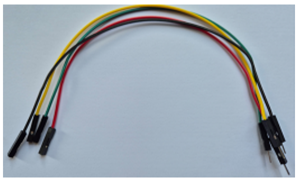
2 EdgeLock A30 evaluation kit

The EdgeLock A30 secure authenticator is supported by an A30 evaluation kit including:

- EdgeLock A30 evaluation boards
- Level shifter board
- Jumper wires

Table 1 summarizes the contents of the evaluation kit.

Table 1. EdgeLock A30 evaluation kit A30-EVAL

Part number	12NC	Number of pieces	Content	Picture
A30-EVAL	9355050 94598	3	A30 evaluation board	 MCU/MPU 1.0 .. 2.0V GPIO2 GPIO1 SCL SDA GND VCC U1 AUTH C1
		1	Level shifter board	 MCU/MPU 3.3 .. 5.0V GPIO2 GPIO1 SCL SDA GND VCC <MCU Target>LOW A30 1.8V
		6	Jumper wires	

EdgeLock A30 is designed for battery-operated applications and for MCU/MPUs with a supply voltage of 1.8 V. Therefore, the operating supply voltage range of EdgeLock A30 is specified from 1.0 V to 2.0 V.

Although current MCU families typically support 1.8 V operation voltage, many MCU evaluation kits still operate with 3.3V or even 5V. To support rapid prototyping, the EdgeLock A30 evaluation kit includes a level shifter which translates the voltage level accordingly if needed.

Figure 2 shows how to connect the Level Shifter and A30 board.

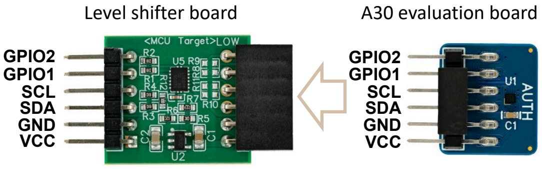


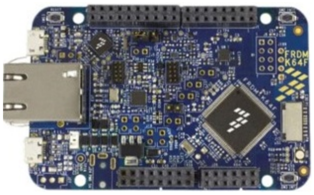
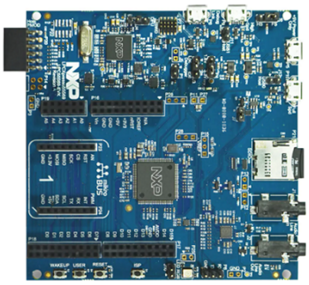
Figure 2. Connecting A30 evaluation board with level shifter board

3 Supported MCU/MPU boards

The EdgeLock A30 secure authenticator IC is designed to be used as a part of an IoT system. It works as an auxiliary security authenticator device attached to a host controller (MCU or MPU board). The host controller communicates with EdgeLock A30 through an I^2C interface with the host controller being the controller and the EdgeLock A30 being the target.

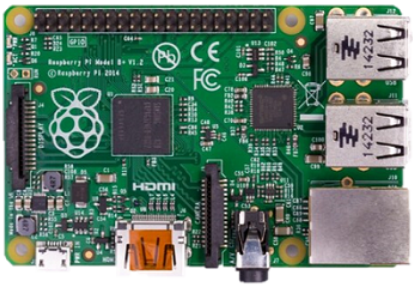
The EdgeLock A30 can be connected to any MCU/MPU on the market supporting the I^2C interface. To enable easy evaluation of the EdgeLock A30, the NX Middleware supports the NXP FRDM-K64F and the LPCXpresso 55S69 demo board as an MCU reference platform.

Table 2. FRDM-K64F details

Part number	12NC	Content	Picture
FRDM-K64F	935326293598	Freedom development platform for Kinetis K64, K63 and K24 MCUs	
LPC55S69-EVK	935377412598	LPCXpresso55S69 development board	

The Raspberry Pi is used to demonstrate the embedded Linux enablement of A30. The middleware supports all different Raspberry Pi board versions and was tested on Raspberry Pi 4 Model B.

Table 3. Raspberry Pi

Part number	Content	Picture
Raspberry Pi	Raspberry Pi model	

4 NX Middleware

4.1 Overview

The NX Middleware is a single software stack designed to facilitate the integration of EdgeLock A30 secure authenticator IC into your MCU or MPU software. The NX Middleware abstracts the commands and communication interface exposed by EdgeLock A30. It is directly accessible from stacks like mbedTLS, OpenSSL and PKCS #11. In addition, it includes code examples for quick integration of features and use cases such as TLS and AWS cloud service onboarding. It also comes with support for reference MCU/MPU platforms and can be ported to multiple host platforms and host operating systems.

Figure 3 is a simplified representation of the layers and components of NX Middleware:

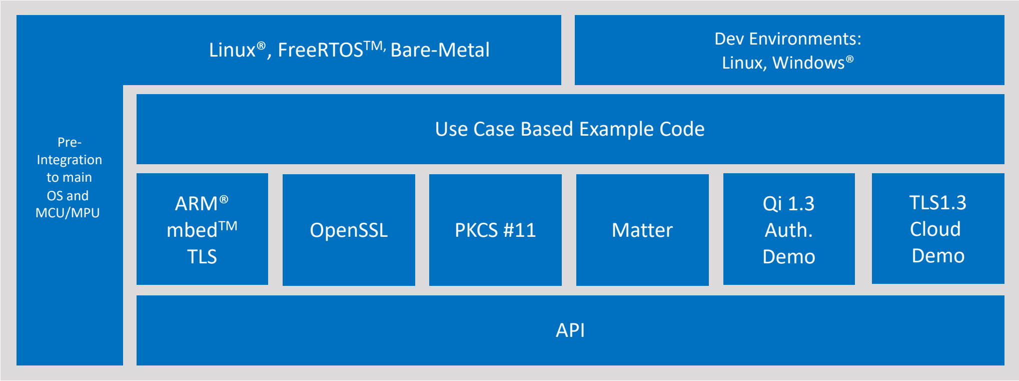

Linux®, FreeRTOS™, Bare-Metal
Dev Environments: Linux, Windows®
Pre-Integration to main OS and MCU/MPU
Use Case Based Example Code
ARM® mbed™ TLS
OpenSSL
PKCS #11
Matter
Qi 1.3 Auth. Demo
TLS1.3 Cloud Demo
API

Figure 3. NX Middleware block diagram

The NX Middleware is delivered with CMake files that include the set of directives and instructions describing the project's source files and targets. The CMake files allow developers to build NX Middleware in their target platform, enable or disable features or change setting flags, among others.

The CMake based compilation option is provided as a convenient way for developers to run a project example on different target platforms:

- Windows/Linux PC for evaluation purpose
- MCU boards
- MPU boards

The NX Middleware has built-in cryptographic and abstracts the commands as well the communication interface exposed by NXP EdgeLock A30 secure authenticator IC. The NX Middleware is directly accessible form the following crypto software stacks:

- ARM mbedTLS
- OpenSSL
- PKCS #11

The NX Middleware can be downloaded via GitHub https://github.com/NXP/nxmw.

Note: *Currently only the Linux platform can be downloaded from GitHub. The Windows, the FRDM-K64F and LPC55S69-EVK MCU platform releases are currently provided as a .zip package and can be downloaded from www.nxp.com/A30. These platforms will be added to GitHub in subsequent releases and will replace the zip package thereafter.*

4.2 Architecture overview

Figure 4 gives a brief overview of the NX Middleware.

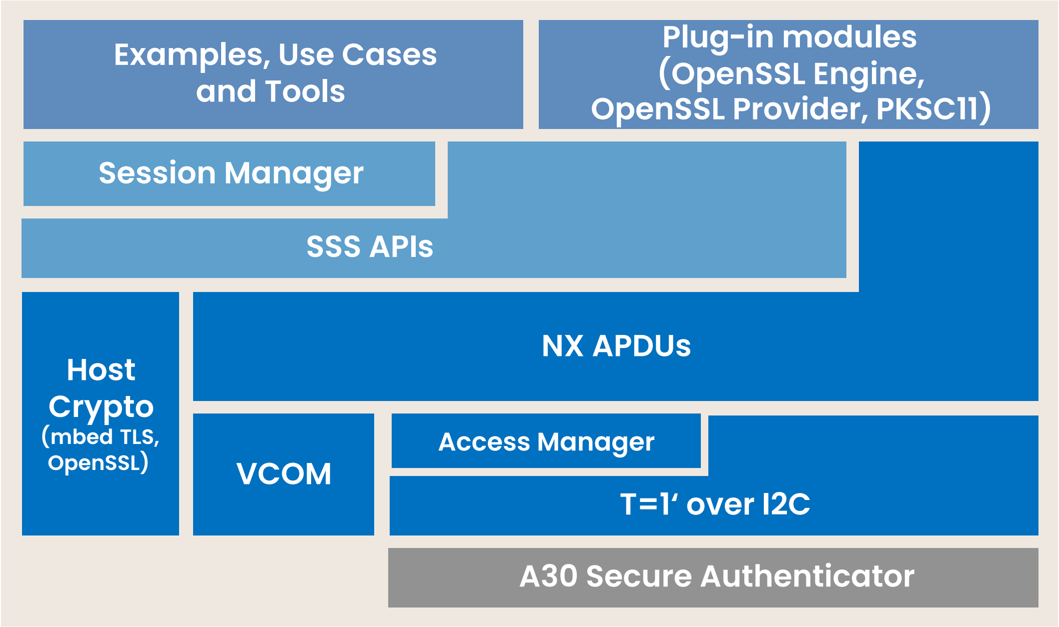

Examples, Use Cases and Tools
Plug-in modules (OpenSSL Engine, OpenSSL Provider, PKSC11)
Session Manager
SSS APIs
Host Crypto (mbed TLS, OpenSSL)
NX APDUs
VCOM
Access Manager
T=1' over I2C
A30 Secure Authenticator

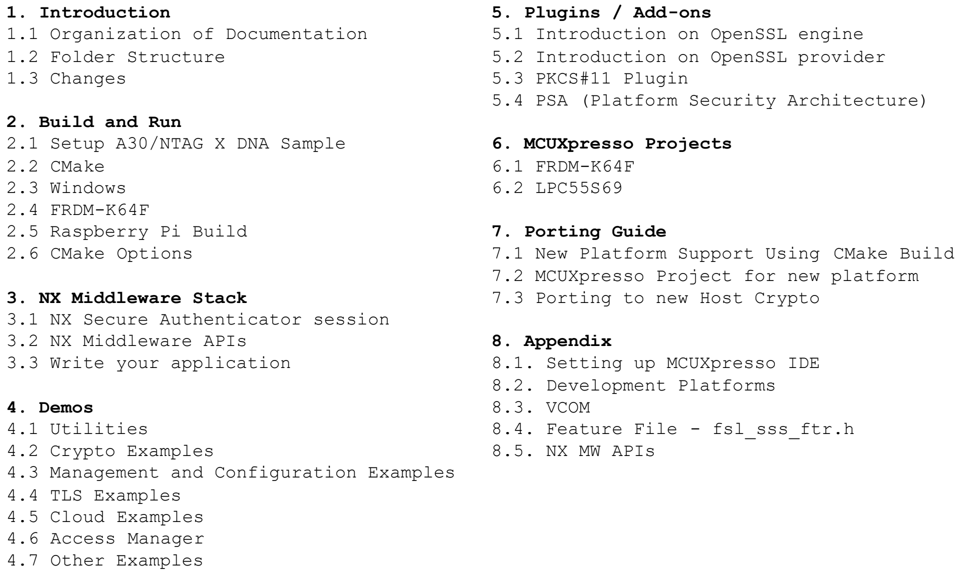
Figure 4. NX Middleware architecture

- Session Manager
  - APIs to open a session. The following sessions are supported:
    - Plain session
    - PKI based asymmetric Mutual Authentication (Sigma-I-Verifier or Sigma-I-Prover)
    - AES-based Symmetric Mutual Authentication
  - Note: Both mutual authentication methods initiate a MIFARE DESFire compatible EV2 secure messaging channel (authenticated session).
- SSS APIs
  - Provides abstraction APIs for EdgeLock A30, OpenSSL and mbedTLS host crypto.
  - SSS APIs are supporting common crypto operations.
- NX APDUs
  - Implements the EdgeLock A30 authenticator commands (APDUs)
- Access Manager
  - Manage access from multiple Linux processes to EdgeLock A30. Client processes connect over the JRCPv1 protocol to the Access Manager.

T=1‘ over I^2C communication protocol according to Global Platform.

4.3 Code documentation

The code documentation provided as part of NX Middleware package in PDF format and as a part of the GitHub release. The primary audience are programmers, developers, system architects and system designers. Figure 5 gives an overview of the PDF document contents.



1. Introduction
1.1 Organization of Documentation
1.2 Folder Structure
1.3 Changes

2. Build and Run
2.1 Setup A30/NTAG X DNA Sample
2.2 CMake
2.3 Windows
2.4 FRDM-K64F
2.5 Raspberry Pi Build
2.6 CMake Options

3. NX Middleware Stack
3.1 NX Secure Authenticator session
3.2 NX Middleware APIs
3.3 Write your application

4. Demos
4.1 Utilities
4.2 Crypto Examples
4.3 Management and Configuration Examples
4.4 TLS Examples
4.5 Cloud Examples
4.6 Access Manager
4.7 Other Examples

5. Plugins / Add-ons
5.1 Introduction on OpenSSL engine
5.2 Introduction on OpenSSL provider
5.3 PKCS#11 Plugin
5.4 PSA (Platform Security Architecture)

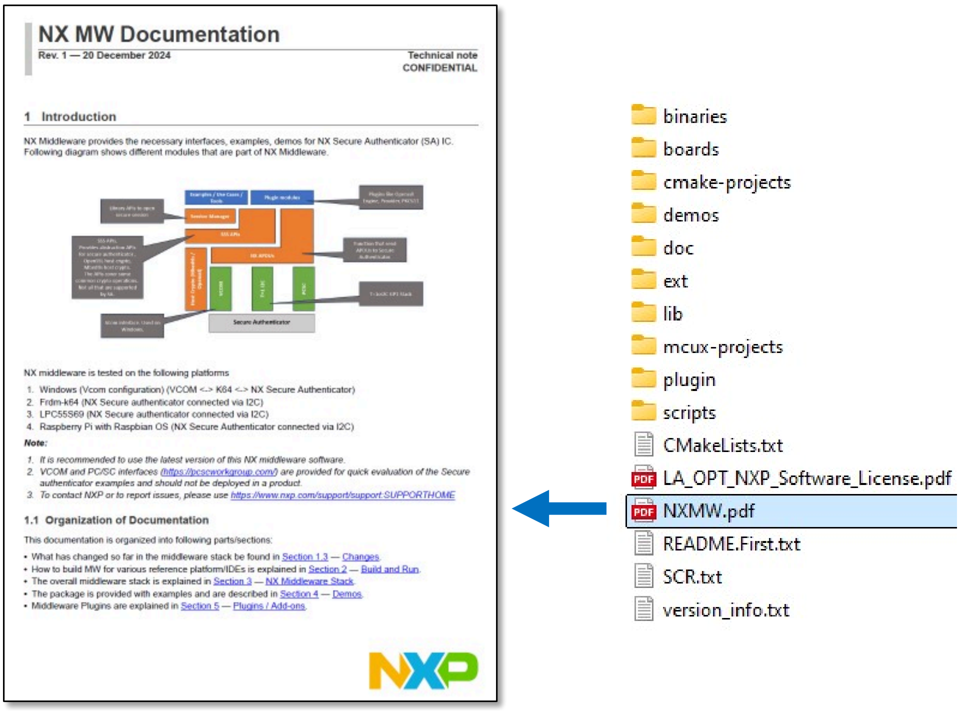
6. MCUXpresso Projects
6.1 FRDM-K64F
6.2 LPC55S69

7. Porting Guide
7.1 New Platform Support Using CMake Build
7.2 MCUXpresso Project for new platform
7.3 Porting to new Host Crypto

8. Appendix
8.1. Setting up MCUXpresso IDE
8.2. Development Platforms
8.3. VCOM
8.4. Feature File - fsl_sss_ftr.h
8.5. NX MW APIs

Figure 5. NX Middleware contents

The PDF version of the NX Middleware documenation (`NXMW.pdf`) is located in the `simw-top\` folder as shown in Figure 6:



NX MW Documentation

Rev. 1 — 20 December 2024

Technical note
CONFIDENTIAL

1 Introduction

NX Middleware provides the necessary interfaces, examples, demos for NX Secure Authenticator (SA) IC. Following diagram shows different modules that are part of NX Middleware.

NX middleware is tested on the following platforms

1. Windows (Vcom configuration) (VCOM <-> K64 <-> NX Secure Authenticator)
2. Frdm-k64 (NX Secure authenticator connected via I2C)
3. LPC55S69 (NX Secure authenticator connected via I2C)
4. Raspberry Pi with Raspbian OS (NX Secure Authenticator connected via I2C)

Note:

1. *It is recommended to use the latest version of this NX middleware software.*
2. *VCOM and PC/SC interfaces (https://pcscworkgroup.com/) are provided for quick evaluation of the Secure authenticator examples and should not be deployed in a product.*
3. *To contact NXP or to report issues, please use https://www.nxp.com/support/support:SUPPORTHOME*

1.1 Organization of Documentation

This documentation is organized into following parts/sections:

- What has changed so far in the middleware stack be found in Section 1.3 — Changes.
- How to build MW for various reference platform/IDEs is explained in Section 2 — Build and Run.
- The overall middleware stack is explained in Section 3 — NX Middleware Stack.
- The package is provided with examples and are described in Section 4 — Demos.
- Middleware Plugins are explained in Section 5 — Plugins / Add-ons.

binaries
boards
cmake-projects
demos
doc
ext
lib
mcux-projects
plugin
scripts
CMakeLists.txt
LA_OPT_NXP_Software_License.pdf
NXMW.pdf
README.First.txt
SCR.txt
version_info.txt

Figure 6. NX Middleware PDF documentation

4.4 Evaluation using a Windows PC

For rapid evaluation and prototyping, the NX Middleware supports building and running the stack on a Windows PC without the need to port to the final target MCU/MPU platform. To connect the EdgeLock A30 evaluation board to a Windows PC, an NXP FRDM-K64 board with the pre-compiled firmware *nx_vcom-T1oI2C_GP1_0-frdmk64f.bin* is required. The FRDM-K64 board must be connected to a Windows PC via USB (K64 USB port - see Figure 8). The EdgeLock A30 and the level shifter board must be connected as shown in Figure 8.

When the NX Middleware is compiled for the Windows platform, all low-level EdgeLock A30 APDU commands and responses are transmitted over a VCOM interface instead of the T=1 over I^{2}C protocol. The *nx_vcom-T1oI2C_GP1_0-frdmk64f.bin* firmware acts as a bridge between the PC VCOM interface and the EdgeLock A30 secure authenticator I^{2}C interface. The *nx_vcom-T1oI2C_GP1_0-frdmk64f .bin* firmware performs the complete T=1 communication over I^{2}C.

To avoid the need of installing MCUXpresso development tools, NX Middleware provides the FRDM-K64 *nx_vcom-T1oI2C_GP1_0-frdmk64f.bin* firmware as a pre-compiled binary. The FRDM-K64 CPU supports flashing the firmware via a USB mass storage device (see Figure 7). Therefore, flashing a firmware binary to the FRDM-K64 MCU can be easily done by drag and drop the firmware binary into the FRDM-K64 USB mass storage folder.

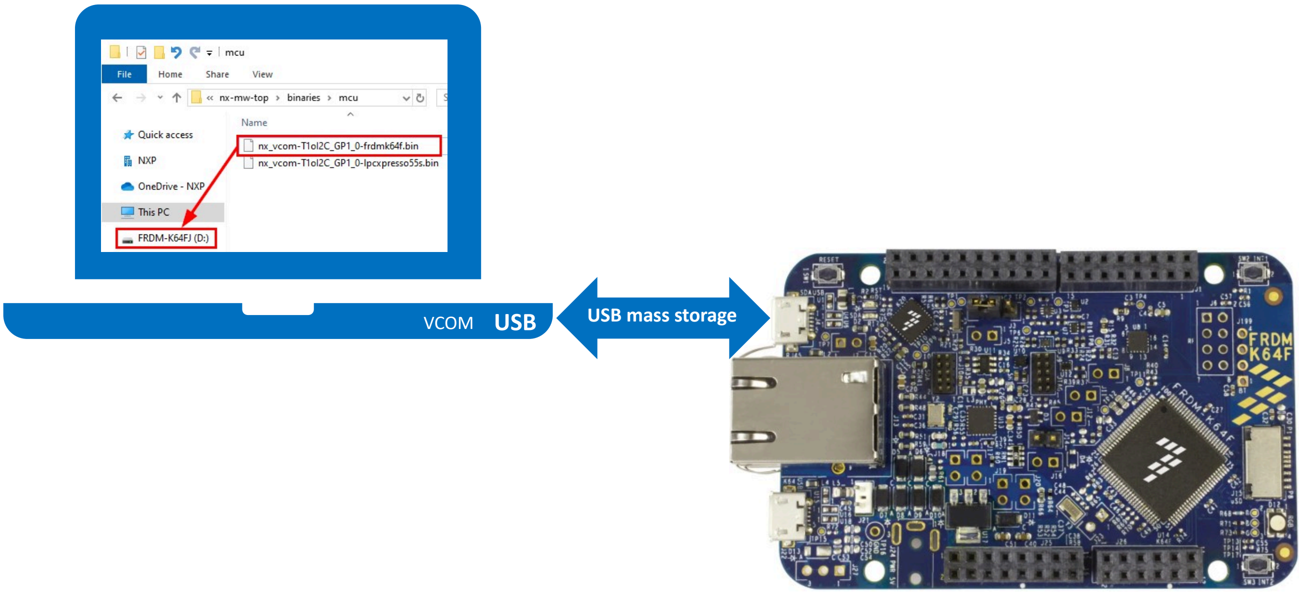


Figure 7. Flashing the pre-compiled FW binary *nx_vcom-T1oI2C_GP1_0-frdmk64f.bin*

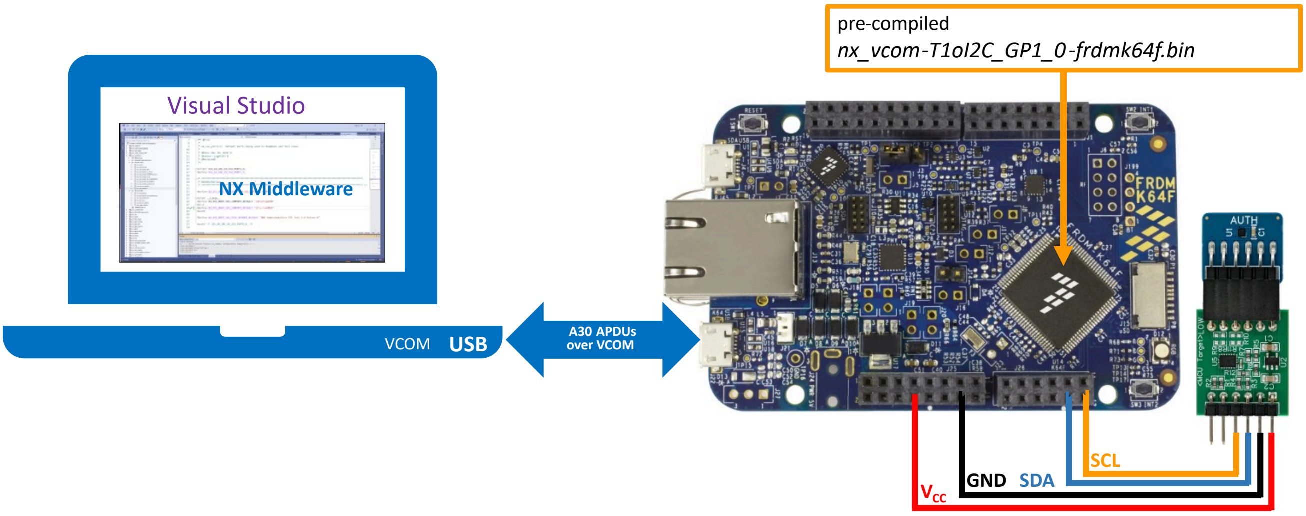


Figure 8. NX Middleware evaluation using a Windows PC

For further details please refer to NX Middleware documentation chapter 2.2 Build and Run Windows.

The NX Middleware also provides a pre-compiled binary for the LPC55S69-EVK. The *nx_vcom-T1oI2C_GP1_0-lpcxpresso55s.bin* file can be loaded, for example using the GUI Flash Tool integrated in MCUXpresso IDE. For further details please refer to MCUXpresso IDE User Guide chapter 17.1.3 Advanced GUI Flash Tool programming an arbitrary binary.

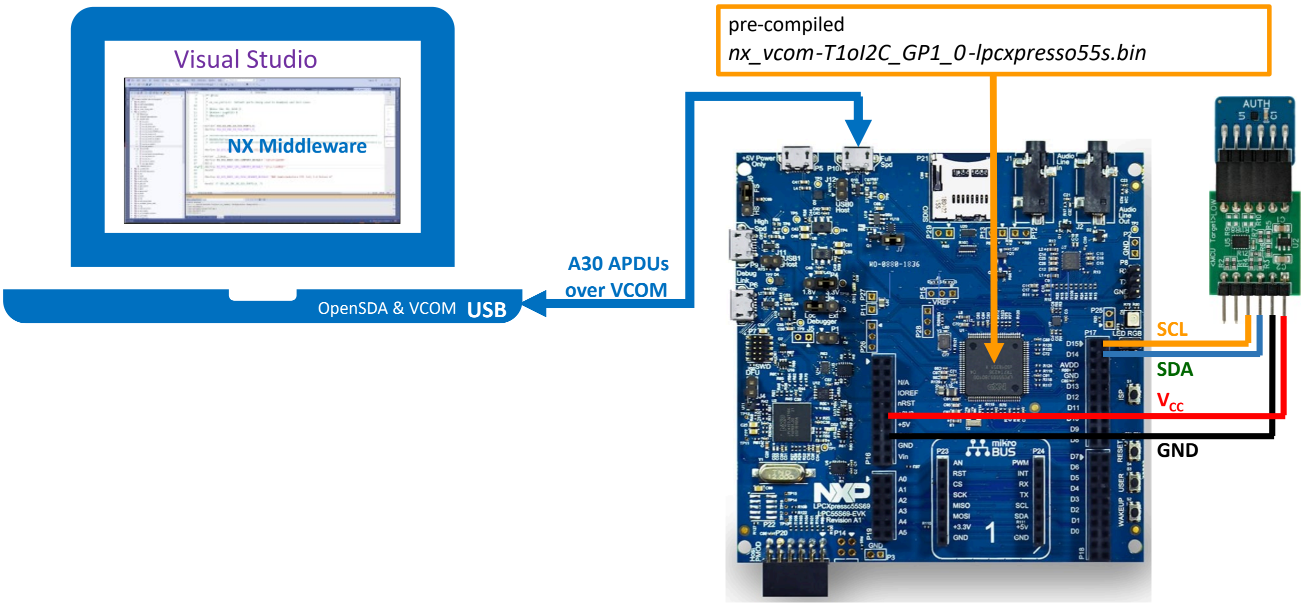


Figure 9. NX Middleware evaluation using a Windows PC

4.5 Evaluation using a MCU board

The NX Middleware includes a set of MCU examples that demonstrate the use of A30 in the latest authenticator security use cases. The FRDM-K64F and LPC55S69-EVK boards are used as a reference MCU platform and MCUXpresso as a reference development IDE. The MW stack was designed to allow easy porting to other MCU/MPU platforms. For further details please refer to the MW documentation chapter 7. Porting Guide.

FRDM-K64/LPC55S69 project examples can be either imported into MCUXpresso as:

- A standalone MCUXpresso projects (see MW document chapter 6 MCUXpresso Projects)
- A CMake project (see MW document chapter 2.4. FRDM-K64F and chapter 8.2.1. Freedom K64F with MCUXPresso IDE)

These project examples offer a quick way to evaluate EdgeLock A30 features, and its source code can be re-used for customer specific implementations. To execute the code, the FRDM-K64F board must be connected to a Windows PC via USB (Open SDA USB port - see Figure 10). The EdgeLock A30 and the level shifter board must be connected as shown in Figure 10.

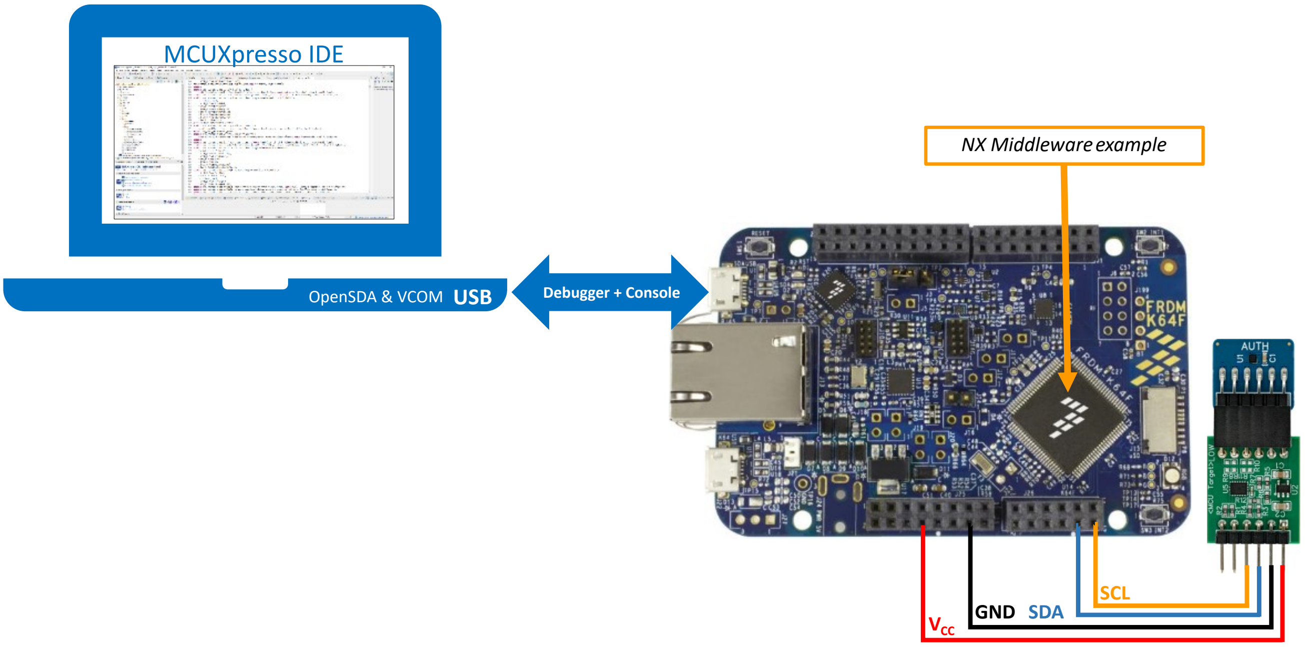


Figure 10. NX Middleware evaluation using a FRDM-K64F MCU board

Figure 11 shows the setup using a LPC55S69-EVK.

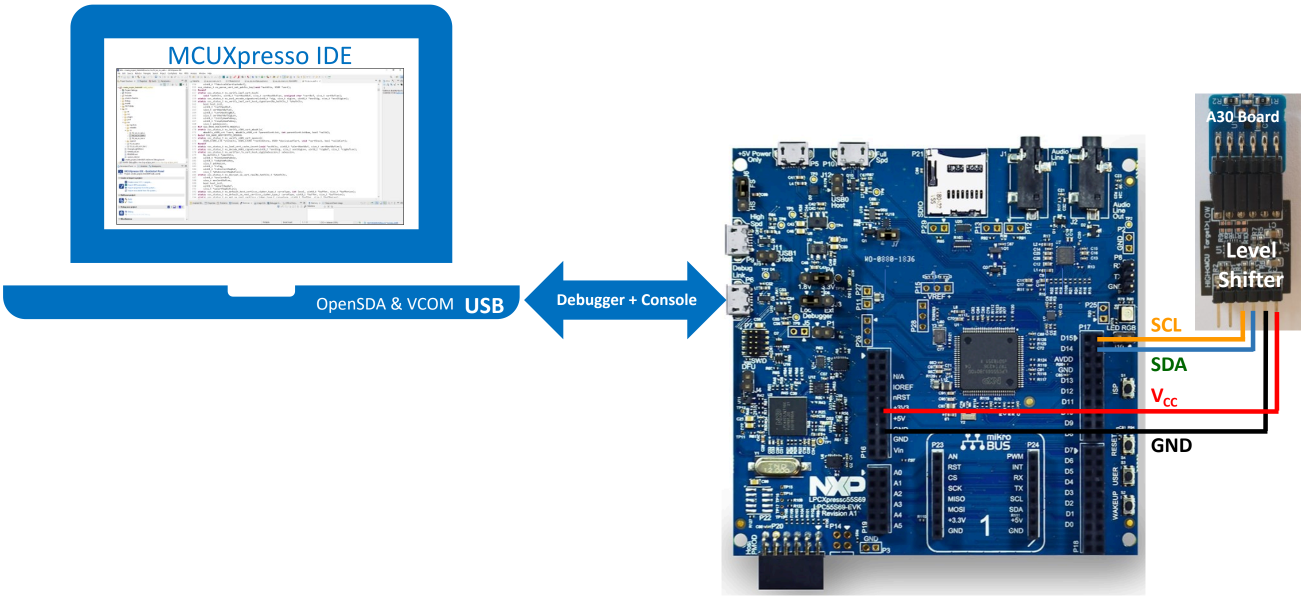


Figure 11. NX Middleware evaluation using a LPC55S69-EVK

4.6 Evaluation using Raspberry Pi

The NX Middleware offers several components and example code to implement and verify EdgeLock A30 on devices running an embedded Linux distribution:

- OpenSSL engine compatible with OpenSSL versions 1.1.1
- OpenSSL provider compatible with OpenSSL versions 3.0
- PKCS#11 Plugin
- SSS API

The Raspberry Pi was selected as a reference MPU platform running embedded Linux. For further details refer to the following chapters in the MW documentation:

- 2.4. Raspberry Pi Build
- 4.4.1. OpenSSL Engine: TLS Client example
- 4.5.2. AWS Demo for Raspberry Pi
- 4.6 Access Manager
- 5.1. Introduction on OpenSSL engine
- 5.2. Introduction on OpenSSL provider
- 5.3. PKCS#11 Plugin

Note:

If several Linux processes want to access EdgeLock A30 at the same time, it is necessary to use the Access Manager. The Access Manager manages the simultaneous access of several Linux processes to EdgeLock A30. Linux client processes are connected to the Access Manager via the JRCPv1 protocol.

Figure 12 shows the principal hardware setup. Please refer to the MW documentation chapter 2.4.2. Connecting NX Secure Authenticator with RaspberryPi for more details

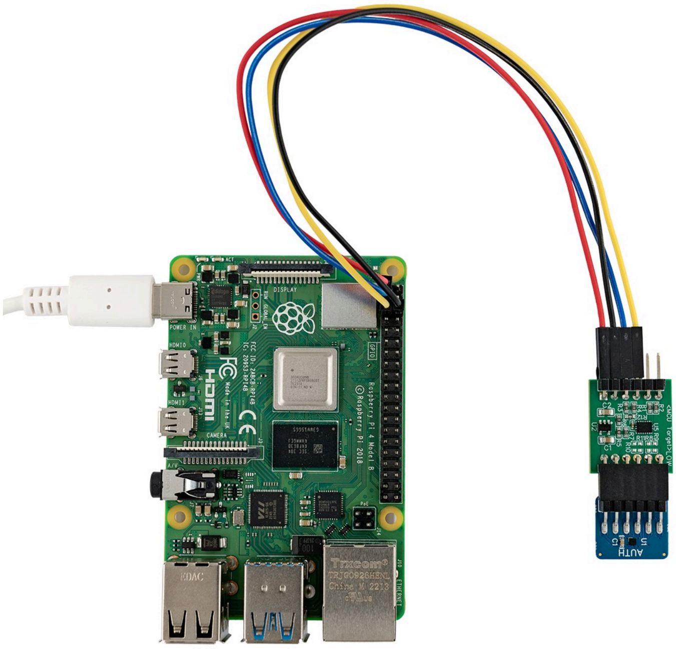


Figure 12. NX Middleware evaluation using a Raspberry Pi 4 Model B board

Figure 13 and Table 4 are showing the detailed connection of the EdgeLock A30 to the Raspberry Pi:

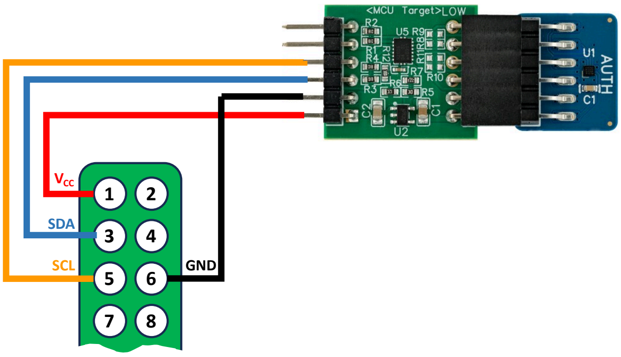


Figure 13. EdgeLock A30 wiring to a Raspberry Pi 4 Model B

Table 4. EdgeLock A30 wiring to a Raspberry Pi 4 Model B board

Raspberry Pi 4 Model B (# jumper - # pin)	Level Shifter Board (# jumper - # pin)
J8-P5 (SCL)	SCL (HIGH<MCU)
J8-P3 (SDA)	SDA (HIGH<MCU)
J8-P6 (GND)	GND (HIGH<MCU)
J8-P1 (3V3)	VCC (HIGH<MCU)

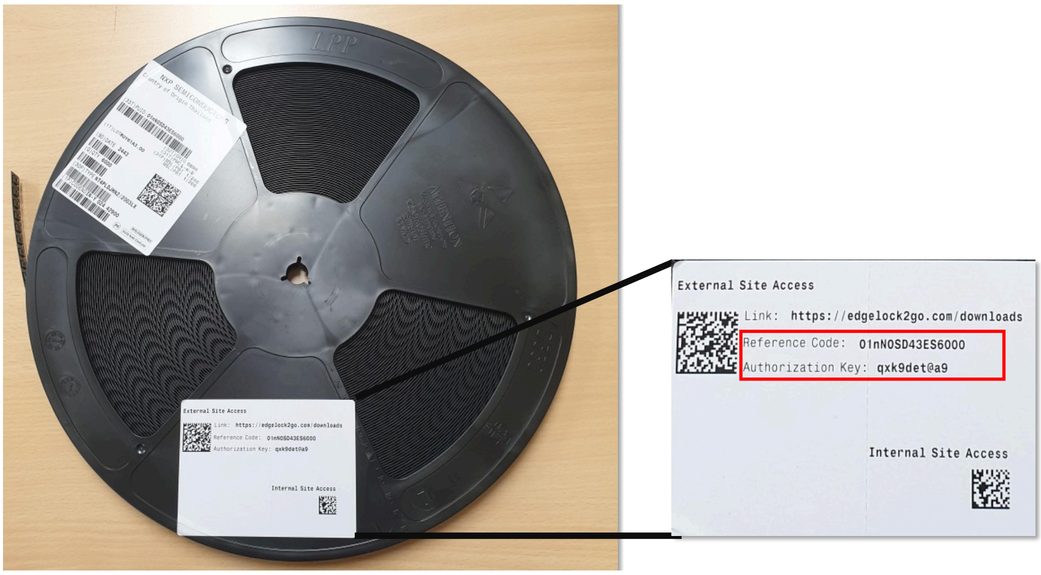
5 EdgeLock 2 Go service for EdgeLock A30

5.1 Overview

EdgeLock A30 products are delivered with an NXP trust-provisioned device unique application private EC key and application X.509 certificate containing the corresponding public EC key. The EdgeLock A30 application credentials can be used for Sigma-I Authentication.

To simplify the OEMs products process and reduce the production cost the EdgeLock A30 device UID and the application X.509 certificate can be downloaded via the EdgeLock 2 Go service. This eliminates the need for OEMs to read the credential from each individual EdgeLock A30 device.

EdgeLock A30 reels are shipped with a label containing an access code (reference code and authorization key).



External Site Access

Link: https://edgelock2go.com/downloads

Reference Code: 01nNOSD43ES6000

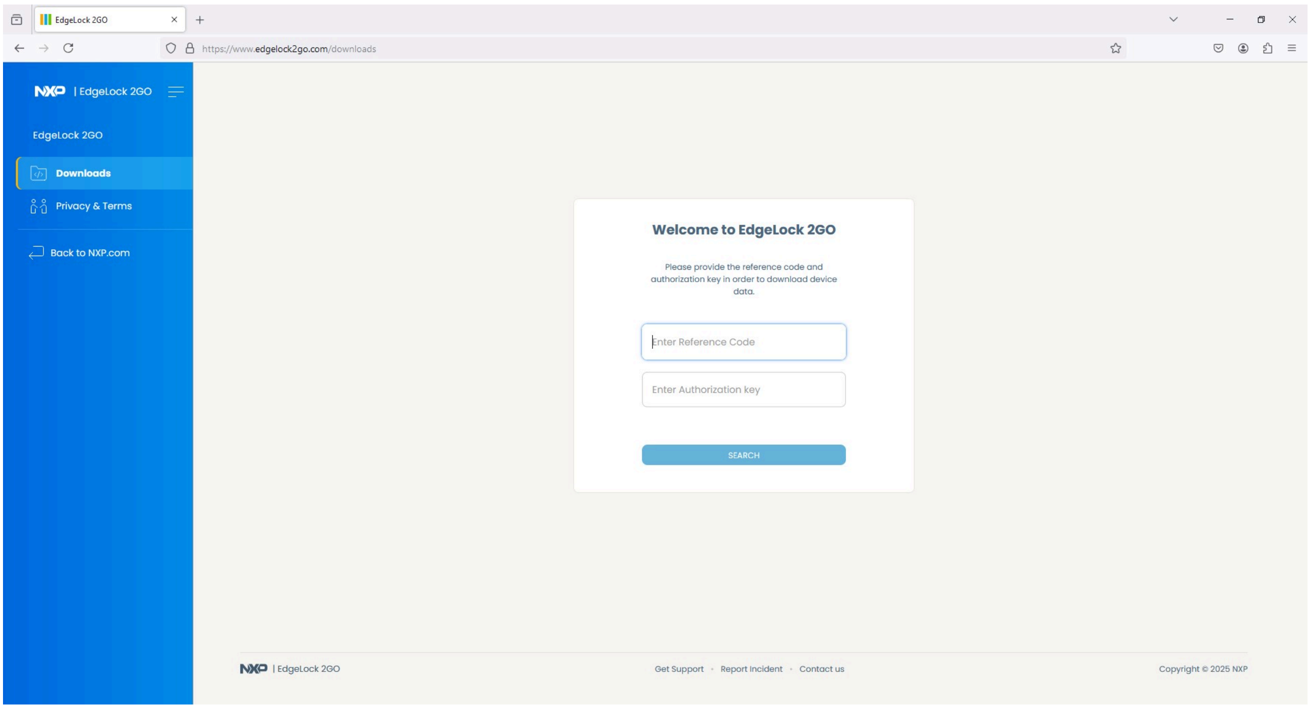
Authorization Key: qxk9det@a9

Internal Site Access

Figure 14. EdgeLock A30 reel

To download the EdgeLock A30 UIDs and application certificates can be simple done by the following steps:

- Go to https://www.edgelock2go.com/downloads and enter the reference code and authorization key.
- After successful registration, the Wafer Map, Device UIDs and the application X.509 certificates can be downloaded.



Welcome to EdgeLock 2GO

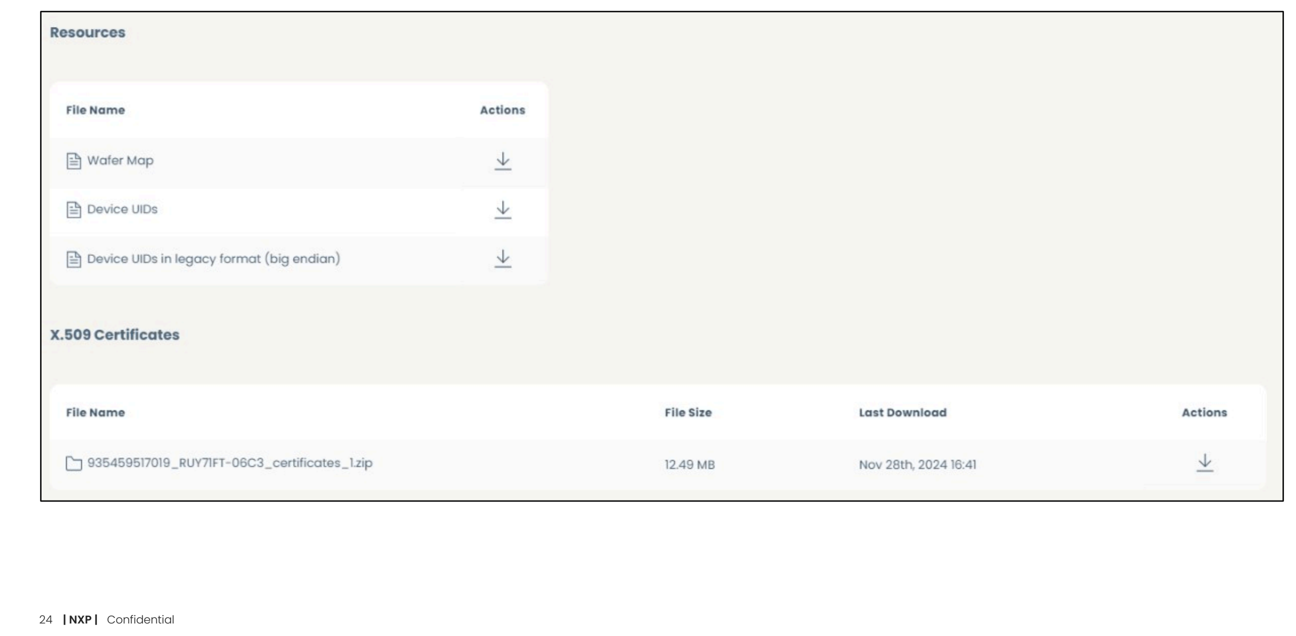
Please provide the reference code and authorization key in order to download device data.

Enter Reference Code

Enter Authorization key

SEARCH

Figure 15. EdgeLock2Go web portal



Resources

File Name	Actions
Wafer Map	⤓
Device UIDs	⤓
Device UIDs in legacy format (big endian)	⤓

X.509 Certificates

File Name	File Size	Last Download	Actions
935459517019_RUY71FT-06C3_certificates_1.zip	12.49 MB	Nov 28th, 2024 16:41	⤓

Figure 16. UID and certificate download via EdgeLock2Go

6 Supported EdgeLock A30 documentation

Table 5 summarizes the EdgeLock A30 dedicated documents.

Note: *Click on the hyperlink in the app note numbers to download the document, or click on the hyperlink in the app note title to navigate through the specific app note section*

Table 5. Dedicated EdgeLock A30 documentation

Documentation number	Title
DS9767xx	Edgelock A30 Secure Authenticator data sheet
AD9772xx	Edgelock A30 Delivery specification
AN14559	Migration Guide from EdgeLock A5000 to EdgeLock A30
Global Platform	GlobalPlatform Technology- APDU Transport over SPI / I^{2}C Version 1.0, January 2020
UM10204	I^{2}C-bus specification and user manual

7 Appendix

7.1 EdgeLock A30 application circuit diagram

Figure 17 shows an application circuit diagram with the following design considerations:

- Power-On-Reset
  - It is recommended that the hostcontroller can perform a Power-On-Reset by controlling V_{CC}.
  - It is possible to supply A30 via the MCU/MPU GPIO. The GPIO shall be able to deliver current up to 15 mA.
- A30 triggers a Reset via T=1‘ over I^2C protocol
  - Using a proprietary NXP S-Blocks chip reset request/response.
- A30 enables Deep Power Down via T=1‘ over I^2C protocol
  - Using a proprietary NXP S-Block Deep Power Down request/response.

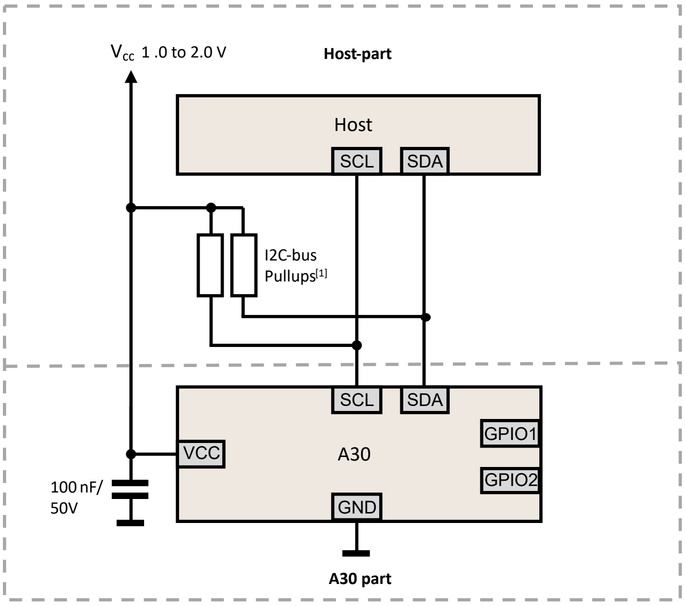


Figure 17. evaluation board schematic

Note: *[1] .. According UM10204 I^2C-bus specification and user manual Rev 7, chapter 7.1 Pull-up resistor sizing*

7.2 EdgeLock A30 evaluation board schematic

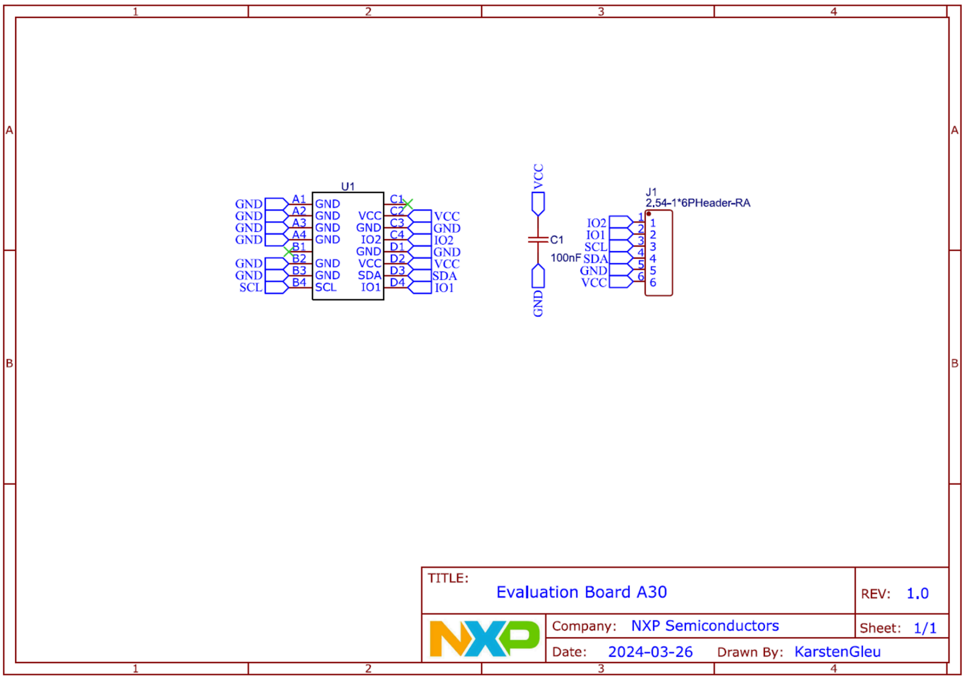


Figure 18. evaluation board schematic

7.3 Level shifter board schematic

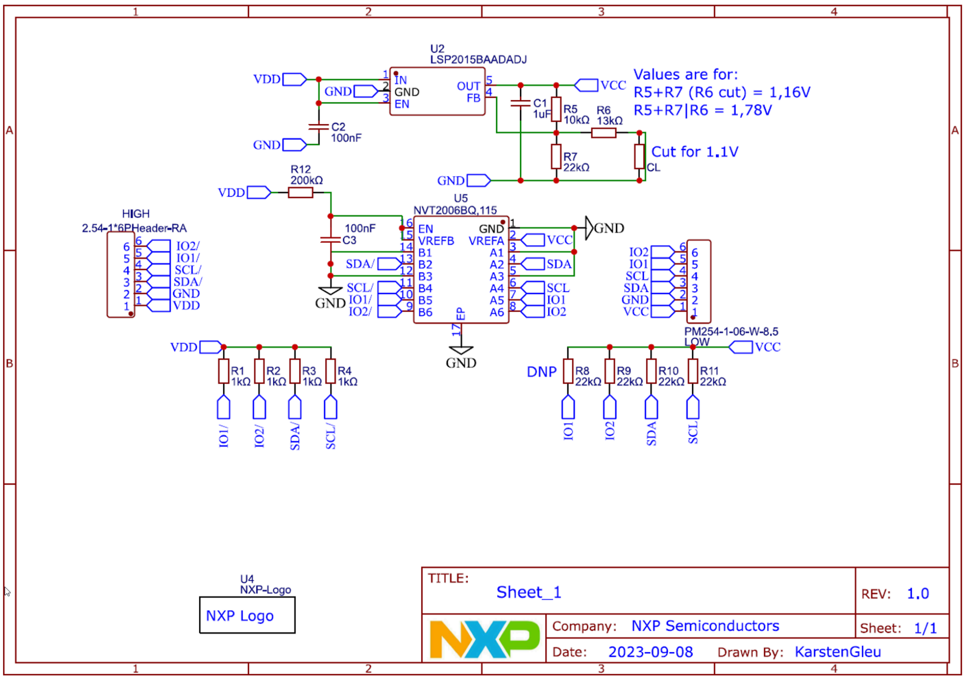


Figure 19. Level shifter board schematic

8 Revision history

Table 6. Revision history

Revision number	Date	Description
AN14238 v.1.0	15 January 2025	Initial version

Legal information

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.

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 https://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 document 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.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

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.

EdgeLock — is a trademark of NXP B.V.

Tables

Figures

Contents

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