How to use STM32 Nucleo expansion board based on the STSAFE-A110 secure element
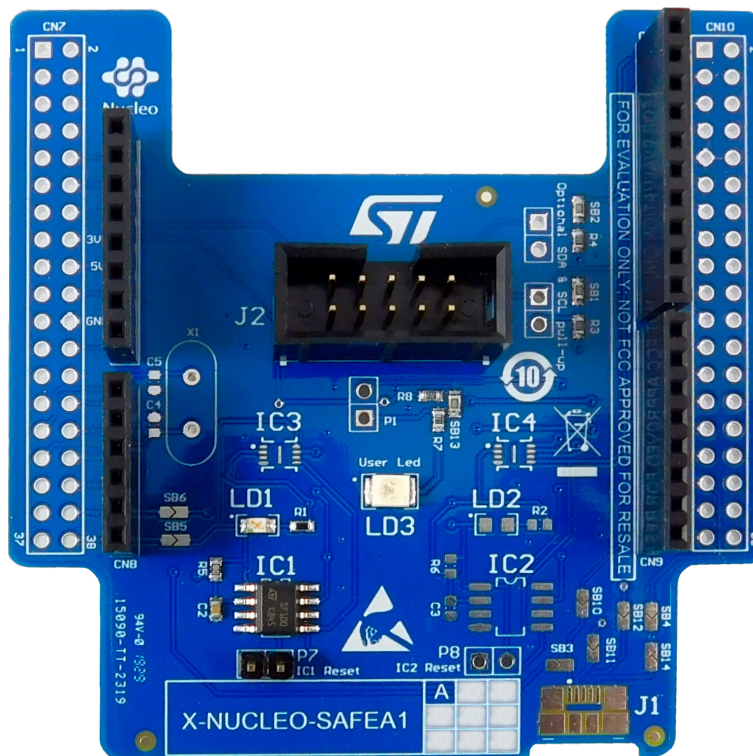
Introduction

The X-NUCLEO-SAFEA1A expansion board is based on the STSAFE-A110 secure element. It can be used with any STM32 Nucleo development board.

The on-board STSAFE-A110 is customized with a standard profile for evaluation and is compatible with the Arduino UNO R3 connector.

The X-NUCLEO-SAFEA1A expansion board is used with free X-CUBE-SAFEA1 or X-CUBE-SBSFU software packages containing sample code to demonstrate how to implement security applications.

Figure 1. X-NUCLEO-SAFEA1A expansion board

UM2670 - Rev 2 - June 2023
For further information contact your local STMicroelectronics sales office.

www.st.com

1 Getting started

1.1 Hardware requirements

The X-NUCLEO-SAFEA1A expansion board can be connected to any STM32 Nucleo development board through the matching Arduino UNO R3 connector pins.

Note: *Handle the X-NUCLEO-SAFEA1A with care and avoid bending or damaging the pins as the board has male/ female pass-through connectors and ESD sensitive components.*

───── **Related links** ─────

visit the Nucleo page on the ST website for further information

1.2 System requirements

To complete the system setup, you need:

- a PC running Windows version 7, 8 or 10
- a USB type A to mini-B USB cable to connect the STM32 Nucleo to the PC
- software package (X-CUBE-SAFEA1 or X-CUBE-SBSFU) installed on the user PC
- one of the compatible software development environments: IAR, Arm Keil, AC6, or Atolic

2 Hardware description

The X-NUCLEO-SAFEA1A expansion board has an embedded STSAFE-A110 secure element to allow you to evaluate its authentication and data management services connected to a local or remote host.

This STSAFE-A110 is factory personalized with a generic sample profile.

The main features of the X-NUCLEO-SAFEA1A expansion board are:

- On-board STSAFE-A110 customized with a standard evaluation profile
- HE10 extension connector to mount additional STSAFE devices
- Arduino UNO R3 connector
- Free drivers, middleware and software samples compatible with the STM32 ODE
- RoHS and WEEE compliant

The X-NUCLEO-SAFEA1A interfaces with the STM32 Nucleo microcontrollers via the I²C communication bus.

─── Related links ───

See application note AN5435 "STSAFE-A110 Generic sample profile description" available in the Resources section of the STSAFE-A110 product folder

2.1 Jumpers and solder bridges

Table 1. X-NUCLEO-SAFEA1A expansion board jumper and solder bridge functions

Jumper	Alternative soldering point	function
P1	SB13	Connects embedded LD3 green LED to STM32 Nucleo board
P4	SB1	Connects embedded 2.2kΩ pull-ups to I²C bus for SCL
P5	SB2	Connects embedded 2.2kΩ pull-ups to I²C bus for SDA
P7		Can be used to put STSAFE-A110 secure element in reset mode
	SB5	Can be used to drive the STSAFE-A110 reset pin via the STM32 MCU PC0 GPIO

2.2 Connector

X-NUCLEO-SAFEA1A Nucleo expansion board has an HE10 extension connector (J2) to mount an additional STSAFE-A1xx secure element.

Note: *If you use the connector to accommodate new generation STSAFE-A devices, be sure that you insert jumper P7 to place the current STSAFE-A110 secure element soldered on the board in reset mode.*

3 STM32L4 series microcontroller software

The STM32 ODE software package X-CUBE-SAFEA1 provides demonstration source code for a NUCLEO-L476RG development board with X-NUCLEO-SAFEA1A expansion. The X-CUBE-SAFEA1 package includes drivers, middleware and several demonstration codes that implement the features of the STSAFE-A110 device through a host microcontroller. The demonstration codes use the STSAFE-A1xx middleware built on the STM32Cube software technology. They illustrate authentication, key pair generation, key establishment, local envelope wrapping and pairing features.

Another package, called X-CUBE-SBSFU, provides demonstration source code for Secure Boot and Secure Firmware Update solution. It updates of the STM32 microcontroller firmware with new features and addresses potential issues. The update process is a secure operation using the STSAFE-A110 to prevent unauthorized updates and access to confidential on-device data. It is available for the STM32L4 Series microcontrollers with examples provided for the B-L475E-IOT01A discovery kit with the X-NUCLEO-SAFEA1A expansion.

—— **Related links** ——————————————————————————————

STM32 ODE compatible software can be downloaded freely from the STSAFE-A110 product web folder in the Tools & Software section

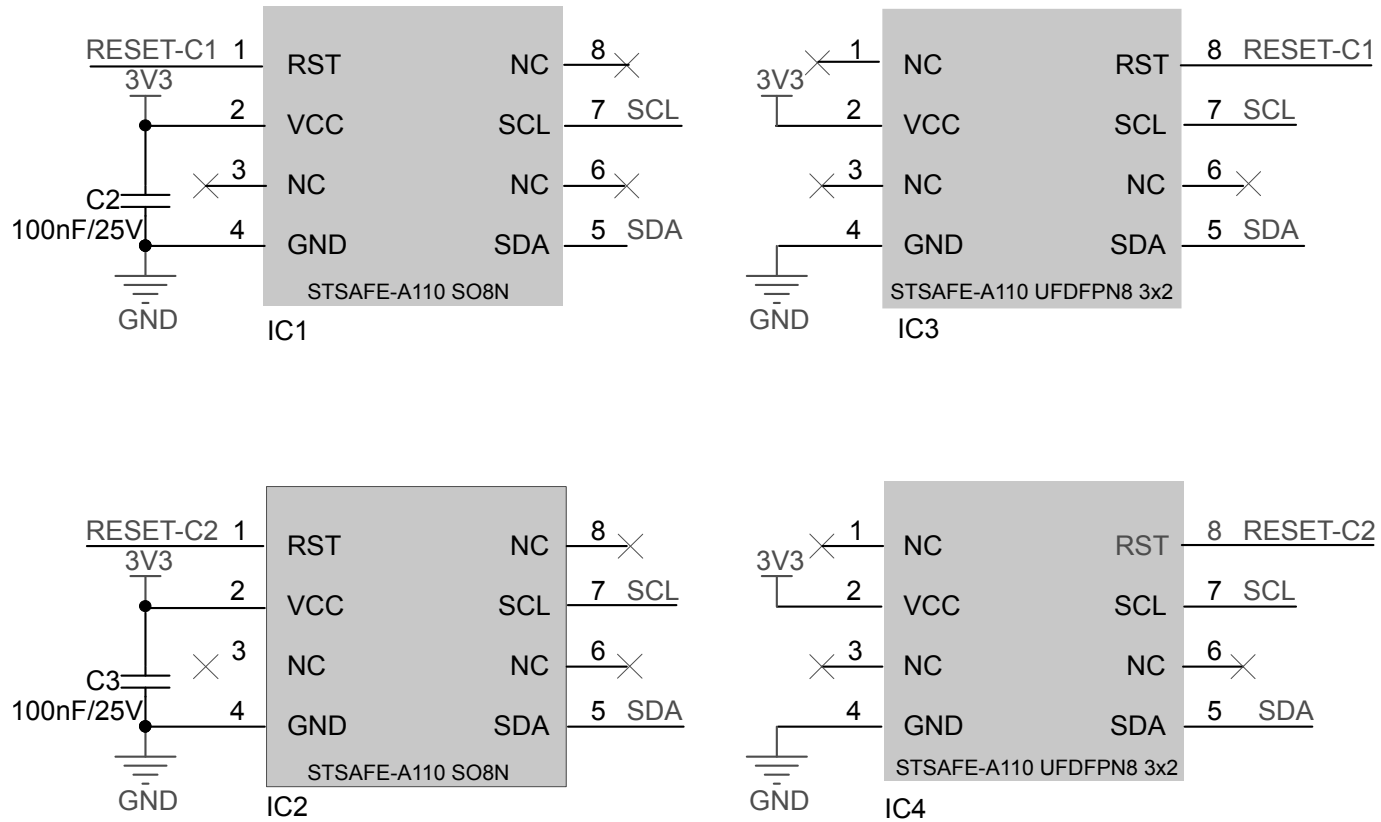Figure 2. **X-NUCLEO-SAFEA1 circuit schematic - STSAFE-A chips**

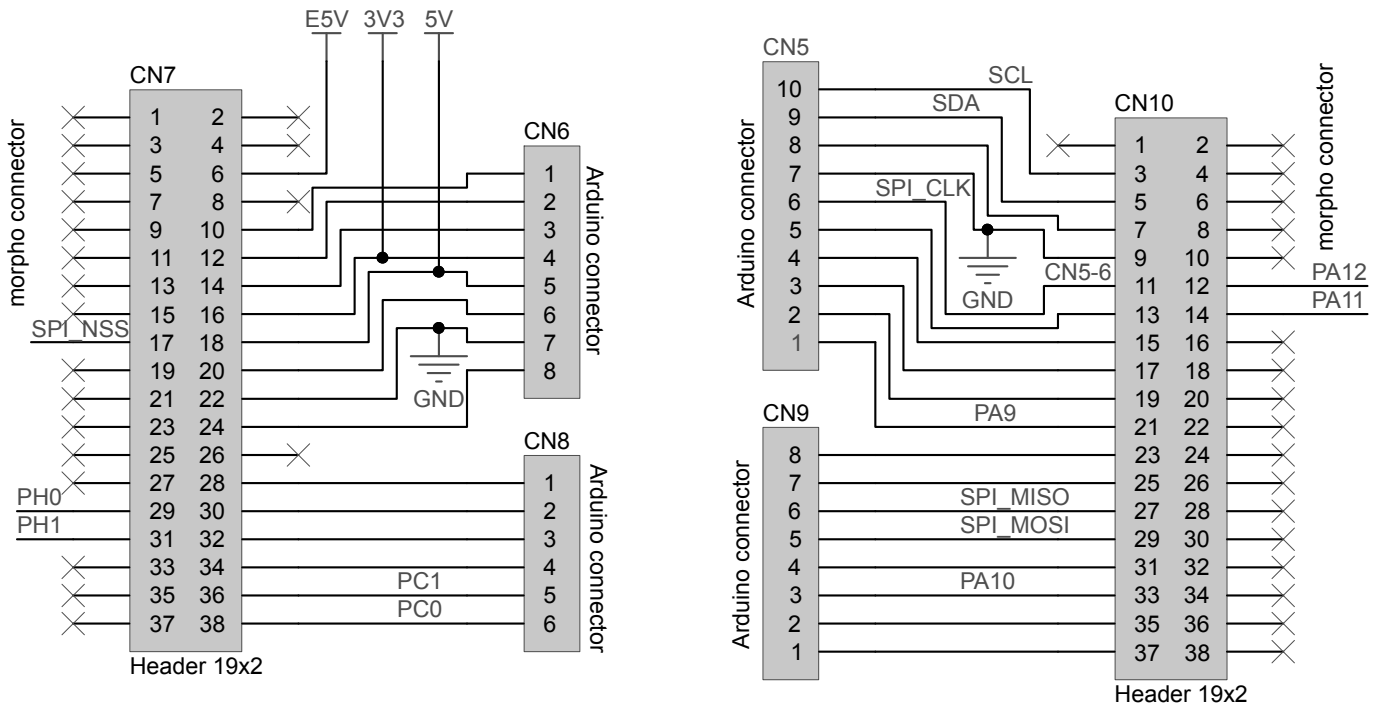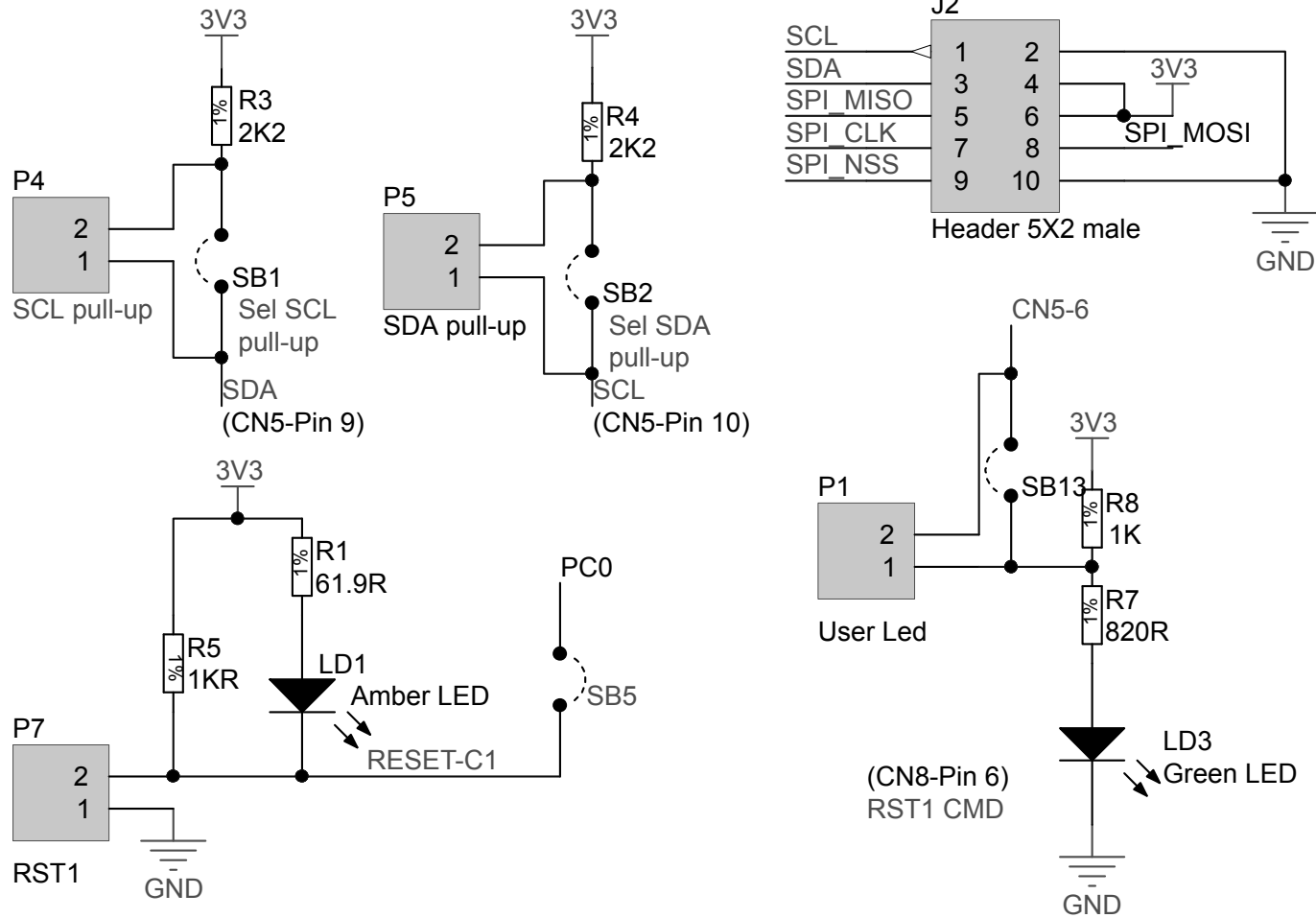**Figure 3. X-NUCLEO-SAFEA1 circuit schematic - Arduino and morpho connectors**

Figure 4. X-NUCLEO-SAFEA1 circuit schematic - LEDs and jumpers

5 Bill of materials

Table 2. X-NUCLEO-SAFEA1A bill of materials

Item	Q.ty	Reference	Part/Value	Description	Manufacturer	Order code
1	1	C2	0.1 µF 0603 [1608 Metric] 25 V ± 10 % SMD X7R	Multilayer ceramic capacitor	Multicomp	MC0603B104K250CT
2	0	C3	0.1 µF 0603 [1608 Metric] 25 V ± 10 %	Multilayer ceramic capacitor (not mounted)	Multicomp	MC0603B104K250CT
3	0	C4, C5	22 pF 0603 [1608 Metric] 50 V ± 5% C0G/NP0	Multilayer ceramic capacitors (not mounted)	Multicomp	MC0603N220J500CT
4	1	CN5	Vertical, 2.54 mm, 10 contacts, receptacle, ESQ series, through hole	Board-to-board connector	SAMTEC	ESQ-110-24-T-S
5	1	CN6	Vertical, 2.54 mm, 8 contacts, receptacle, ESQ series, through hole	Board-to-board connector	SAMTEC	ESQ-108-24-T-S
6	0	CN7	Vertical, 2.54 mm, 38 contacts, receptacle, ESQ series, through hole	Board-to-board connector (not mounted)	SAMTEC	ESQ-119-14-G-D
7	1	CN8	Vertical, 2.54 mm, 6 contacts, receptacle, ESQ series, through hole	Board-to-board connector	SAMTEC	ESQ-106-24-T-S
8	1	CN9	Vertical, 2.54 mm, 8 contacts, receptacle, ESQ series, through hole	Board-to-board connector	SAMTEC	ESQ-108-24-T-S
9	0	CN10	Vertical, 2.54 mm, 38 contacts, receptacle, ESQ series, through hole	Board-to-board connector (not mounted)	SAMTEC	ESQ-119-14-G-D
10	1	IC1	STSAFE-A110 SO8N	Authentication and brand protection secure solution	ST	STSAFA110DFSPL02
11	0	IC2	STSAFE-A110 SO8N	Authentication and brand protection secure solution (not mounted)	ST	STSAFA110DFSPL02
12	0	IC3, IC4	STSAFE-A110 DFN23	Authentication and brand protection secure solution (not mounted)	ST	STSAFA110DFSPL02

Item	Q.ty	Reference	Part/Value	Description	Manufacturer	Order code
13	1	LD1	SM0805AC, 6MCD, 607	Amber LED	Bivar Inc.	SM0805AC
14	0	LD2	SM0805AC, 6MCD, 607	Amber LED (not mounted)	Bivar Inc.	SM0805AC
15	1	LD3	1.8 V 2 mA 570 nm	Green LED	OSRAM	LGT67K-H2K1-24-Z
16	0	J1	Receptacle, 5 ways, surface mount, right angle	USB connector, shielded, Micro USB Type B, USB 2.0 (not mounted)	MOLEX	47346-0001
17	1	J2	2.54 mm, 10 contacts, header, 303 Series, through hole, 2 rows	Wire-to-board connector	3M	30310-6002HB
18	1	P7, P8	473, 80 way, 2 row, straight pin header	Connector	Stelvio Kontek	613080262822
19	1	R1	61.9 ohm 0603 [1608 Metric] 75 V 100 mW	Thick film resistor	MULTICOMP	MCWR06X61R9FTL
20	0	R2	680 ohm 0603 [1608 Metric] 50 V 100 mW	Thick film resistor (not mounted)	MULTICOMP	MCWR06X6800FTL
21	4	R3, R4, R7, R8	2.2 kohm 0603 [1608 Metric] 50 V 100 mW SMD	Chip resistors	MULTICOMP	MCWR06X2201FTL
22	1	R5	1 kohms 0603 [1608 Metric] ±1%	Resistor	MULTICOMP	MCMR06X1001FTL
23	0	R6	1 kohms 0603 [1608 Metric] ±1%	Resistor (not mounted)	MULTICOMP	MCMR06X1001FTL
24	3	SB1, SB2, SB13	0 ohm 0603 [1608 Metric] 75 V 100 mW	Chip resistor	Vishay	CRCW06030000Z0EA
25	0	SB3, SB10, SB11, SB12	0 ohm 0603 [1608 Metric] 75 V 100 mW	Chip resistor (not mounted)	Vishay	CRCW06030000Z0EA
26	0	X1	8 MHz, through hole, 11.5 mm x 5 mm, 10 ppm, 18 pF, 10 ppm, 9B Series	9B-8.000MEEJ-B - Crystal,	TXC Corp.	9B-8.000MEEJ-B

6 Board versions

Table 3. X-NUCLEO-SAFEA1A versions

CPN	Finished good	Schematic diagrams	Bill of materials
X-NUCLEO-SAFEA1A	X$NUCLEO-SAFEA1A [1]	X$NUCLEO-SAFEA1A schematic diagrams	X$NUCLEO-SAFEA1A bill of materials

1. This code identifies the X-NUCLEO-SAFEA1A evaluation board first version.

Revision history

Table 4. Document revision history

Date	Version	Changes
14-Jan-2020	1	Initial release.
29-Jun-2023	2	Added Section 6 Board versions. Minor text changes.

Contents

List of figures

List of tables

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.