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

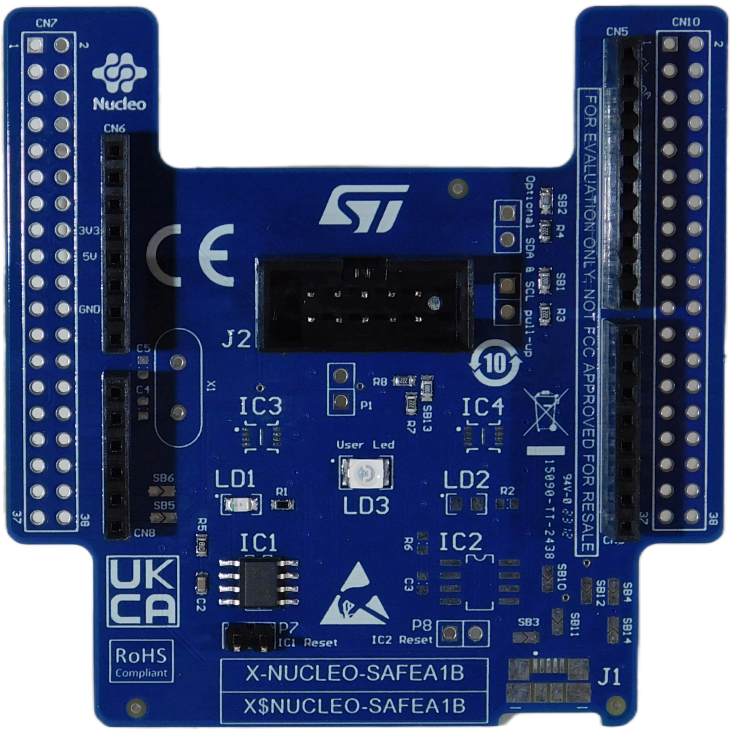
Introduction

The X-NUCLEO-SAFEA1B 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-SAFEA1B 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-SAFEA1B



1 Getting started

1.1 Hardware requirements

The X-NUCLEO-SAFEA1B expansion board can be connected to any STM32 Nucleo development board through the matching Arduino UNO R3 connector pins.

Note: Handle the X-NUCLEO-SAFEA1B with care and avoid bending or damaging the pins as the board has male/female pass-through connectors and ESD sensitive components.

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-SAFEA1B 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-SAFEA1B 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-SAFEA1B interfaces with the STM32 Nucleo microcontrollers via the I²C communication bus.

2.1 Jumpers and solder bridges

Table 1. X-NUCLEO-SAFEA1B 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-SAFEA1B 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-SAFEA1B 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-SAFEA1B expansion.

4 Schematic diagrams

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

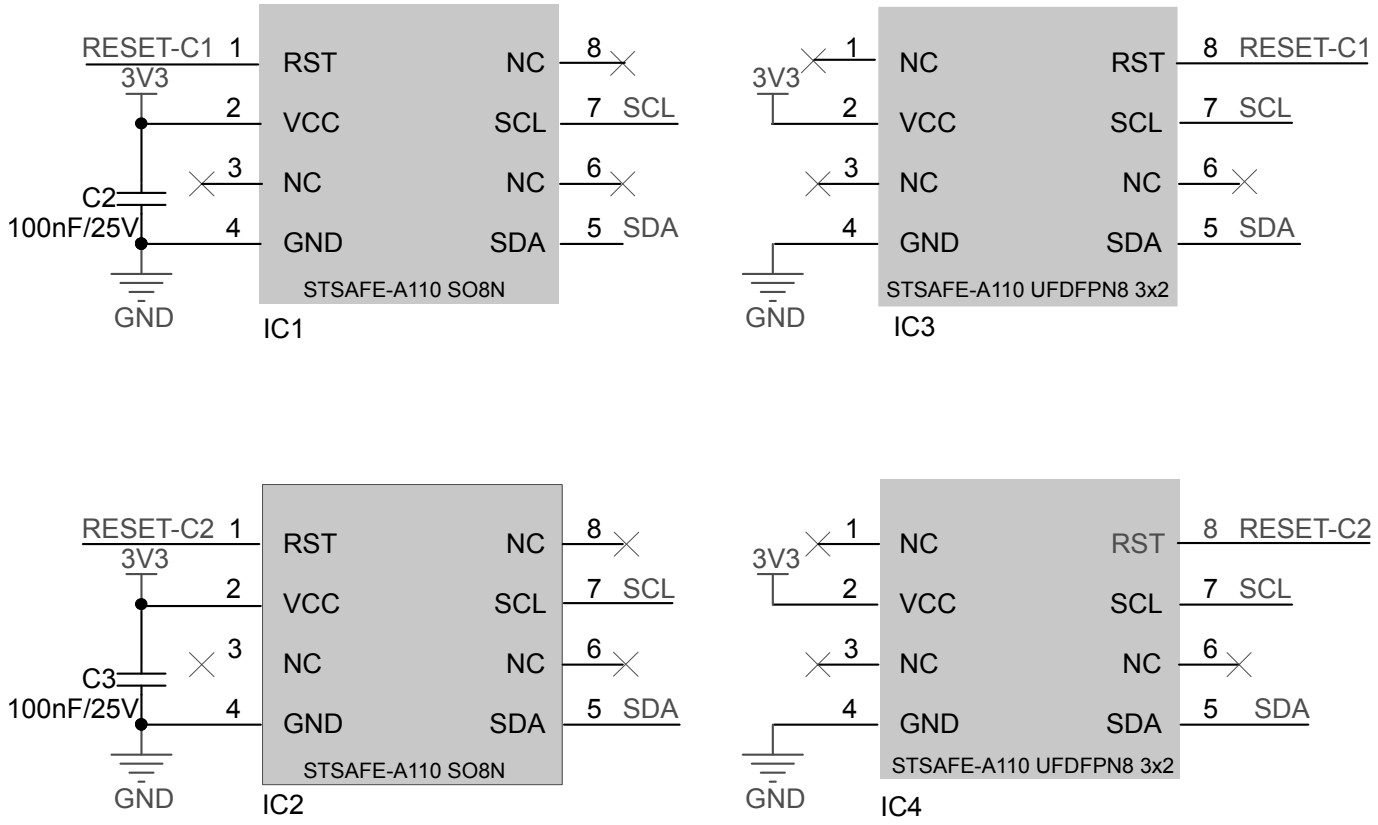


Figure 3. X-NUCLEO-SAFEA1 circuit schematic - Arduino and morpho connectors

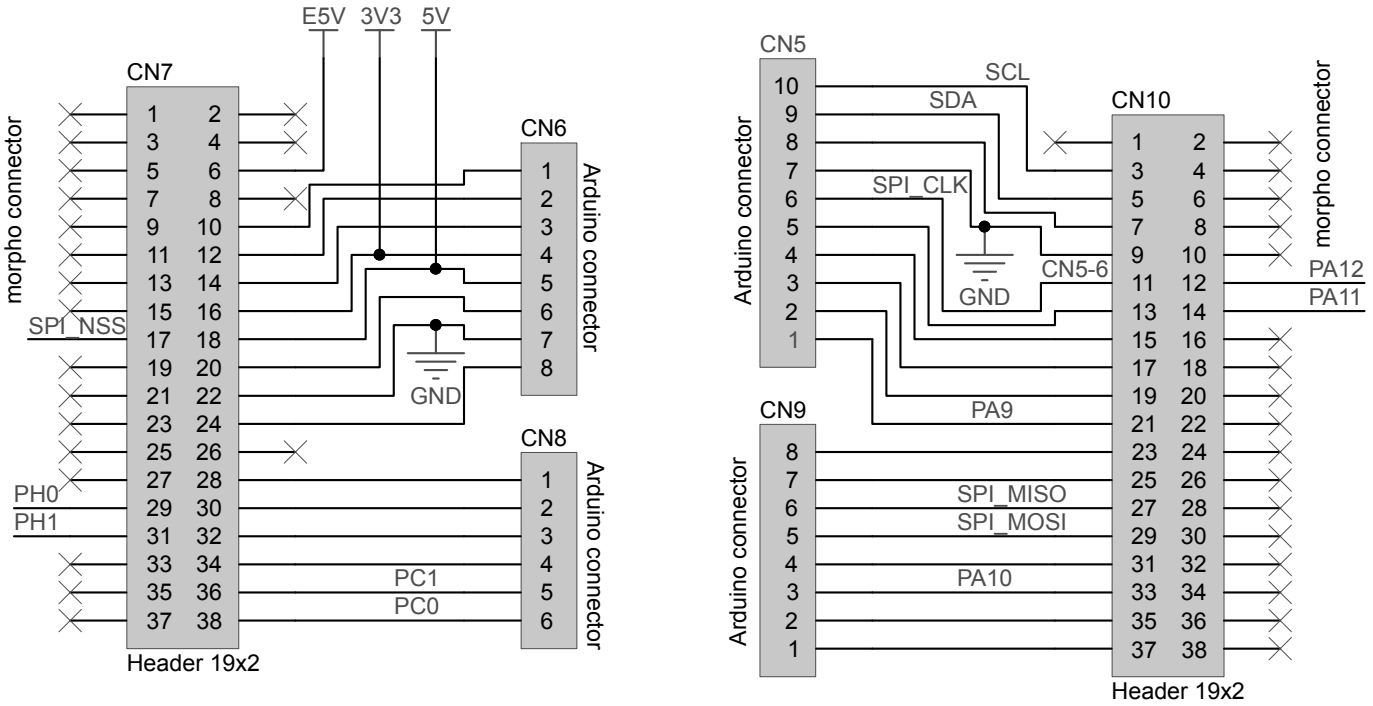
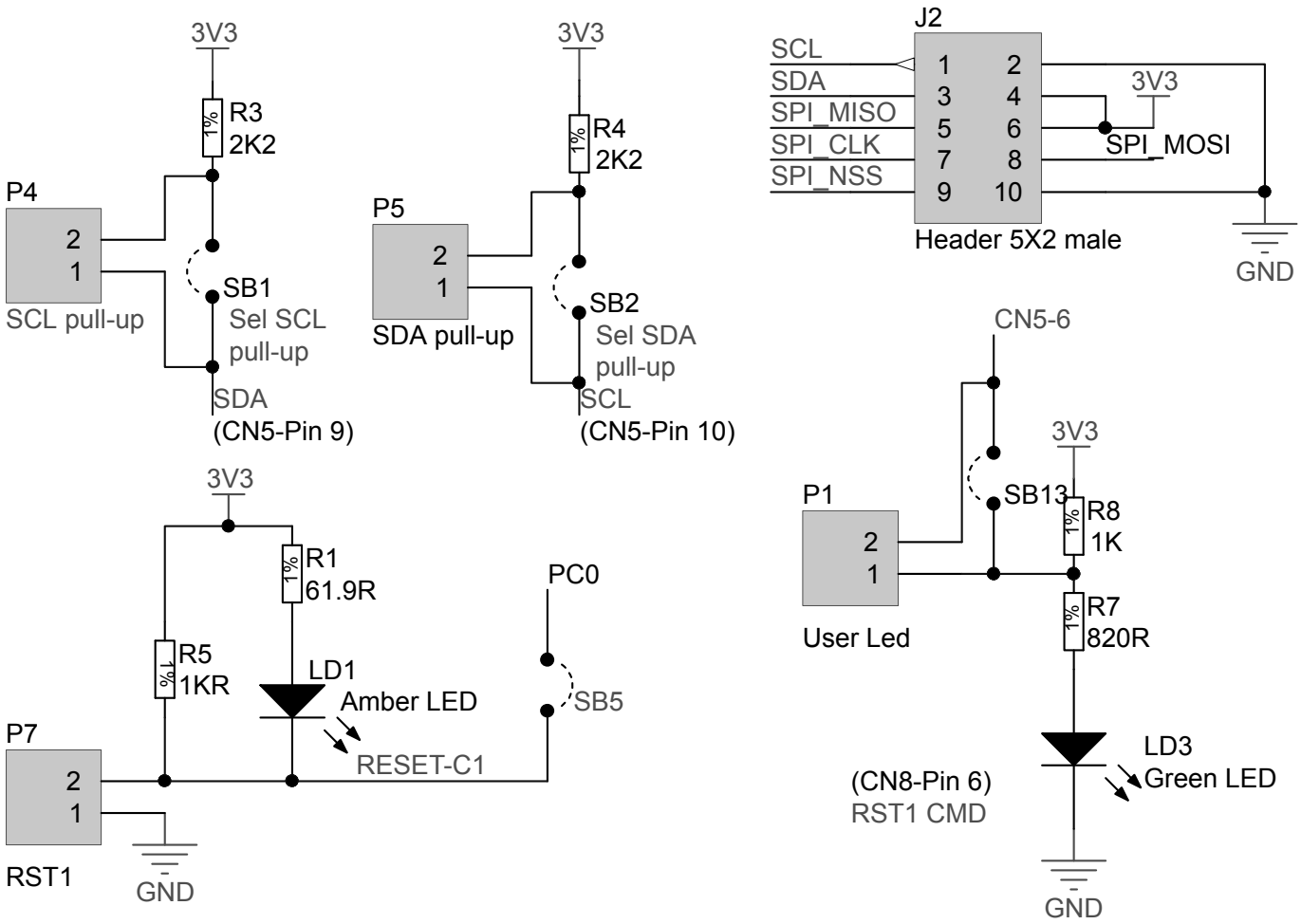


Figure 4. **X-NUCLEO-SAFEA1 circuit schematic - LEDs and jumpers**



5 Bill of materials

Table 2. **X-NUCLEO-SAFEA1B 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	STSAFA110DFSPL03
11	0	IC2	STSAFE-A110 SO8N	Authentication and brand protection secure solution (not mounted)	ST	STSAFA110DFSPL03
12	0	IC3, IC4	STSAFE-A110 DFN23	Authentication and brand protection secure solution (not mounted)	ST	STSAFA110DFSPL03
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

Item	Q.ty	Reference	Part/Value	Description	Manufacturer	Order code
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-SAFEA1 versions**

CPN	Finished good	Schematic diagrams	Bill of materials
X-NUCLEO-SAFEA1B	X$NUCLEO-SAFEA1B (1)	X$NUCLEO-SAFEA1B schematic diagrams	X$NUCLEO-SAFEA1B bill of materials

1. *This code identifies the X-NUCLEO-SAFEA1B evaluation board first version.*

7 Regulatory compliance information

Notice for US Federal Communication Commission (FCC)

For evaluation only; not FCC approved for resale

FCC NOTICE - This kit is designed to allow:

(1) Product developers to evaluate electronic components, circuitry, or software associated with the kit to determine

whether to incorporate such items in a finished product and

(2) Software developers to write software applications for use with the end product.

This kit is not a finished product and when assembled may not be resold or otherwise marketed unless all required FCC equipment authorizations are first obtained. Operation is subject to the condition that this product not cause harmful interference to licensed radio stations and that this product accept harmful interference. Unless the assembled kit is designed to operate under part 15, part 18 or part 95 of this chapter, the operator of the kit must operate under the authority of an FCC license holder or must secure an experimental authorization under part 5 of this chapter 3.1.2.

Notice for Innovation, Science and Economic Development Canada (ISED)

For evaluation purposes only. This kit generates, uses, and can radiate radio frequency energy and has not been tested for compliance with the limits of computing devices pursuant to Industry Canada (IC) rules.

À des fins d'évaluation uniquement. Ce kit génère, utilise et peut émettre de l'énergie radiofréquence et n'a pas été testé pour sa conformité aux limites des appareils informatiques conformément aux règles d'Industrie Canada (IC).

Notice for the European Union

This device is in conformity with the essential requirements of the Directive 2014/30/EU (EMC) and of the Directive 2015/863/EU (RoHS).

Notice for the United Kingdom

This device is in compliance with the UK Electromagnetic Compatibility Regulations 2016 (UK S.I. 2016 No. 1091) and with the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (UK S.I. 2012 No. 3032).

Revision history

Table 4. **Document revision history**

Date	Revision	Changes
13-Jun-2023	1	Initial release.

Contents

List of figures

List of tables