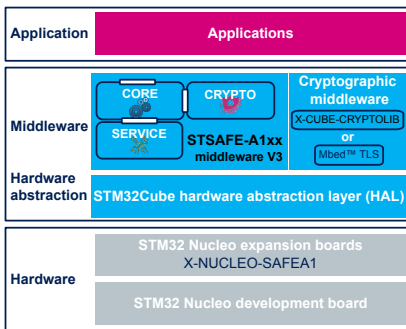


STSAFE-A110 software package



Features

- STSAFE-A110 middleware application programming interface
- Embedded sample demonstrations provided
- Support for **NUCLEO-L476RG** and **X-NUCLEO-SAFE1** boards
- STM32L4 Series HAL driver (STM32Cube)

Applications

- Elliptic-curve digital-signature algorithm (ECDSA) authentication (for instance of peripherals, IoT, USB Type-C devices or Qi wireless power transfer devices)
- Elliptic curve Diffie–Hellman (ECDH) secure-channel establishment with a remote host that includes transport layer security (TLS) handshake
- Signature verification service (secure boot and firmware upgrade)
- Usage monitoring with secure counters
- Pairing and secure channel with host application processor
- Wrapping and unwrapping of local envelopes
- On-chip key-pair generation

Description

The **X-CUBE-SAFE1** software package is a software component that provides driver, middleware and several demonstration codes, which use the **STSAFE-A110** device features from a host microcontroller.

These demonstration codes use the STSAFE-A1xx middleware built on the **STM32Cube** software technology. They illustrate the authentication, key pair generation, key establishment, local envelope wrapping and pairing features.

Product status link

[X-CUBE-SAFE1](#)



1 Software package description

The [X-CUBE-SAFE1](#) software package provides:

- complete middleware to build applications using the [STSAFE-A110](#), a highly secure solution that acts as a secure element, providing authentication and data management services to a local or remote host;
- sample demonstration codes, which can be integrated in Internet of things (IoT) devices, smart-home, smart-city and industrial applications, as well as consumer electronics devices, consumables and accessories:
 - ECDSA authentication (for instance of peripherals, IoT, USB Type-C devices or Qi wireless power transfer devices)
 - ECDH secure-channel establishment with a remote host that includes TLS handshake
 - Pairing and secure channel with host application processor
 - Wrapping and unwrapping of local envelopes
 - On-chip key-pair generation

Sample demonstration codes are available for the [X-NUCLEO-SAFE1](#) expansion board plugged on a [NUCLEO-L476RG](#) development board to ease portability across different STM32 microcontrollers, thanks to [STM32Cube](#).

In addition, the [X-NUCLEO-SAFE1](#) is MCU-agnostic for portability to other microcontrollers.

Note that all codes are free with user-friendly license terms.

Refer to the [STSAFE-A110](#) datasheet available on the [STSAFE-A110](#) internet page for additional information on the device.

Note that STM32 devices are based on Arm® cores.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.



2 Licence

X-CUBE-SAFE1 is delivered under STMicroelectronics' *STSAFE software package license agreement (SLA0087)*.

The table below shows the different license schemes delivered with the software components provided in this package.

Table 1. License schemes

Software components	Owner	License
STM32L4 Nucleo board support package (BSP)	STMicroelectronics	BSD-3-Clause ⁽¹⁾
Cortex [®] -M Cortex Microcontroller Software Interface Standard (CMSIS)	Arm [®]	BSD-3-Clause ⁽¹⁾
STM32L4 hardware abstraction layer (HAL)	STMicroelectronics	BSD-3-Clause ⁽¹⁾
XCUBE-SAFE1's application programming interface (API)	STMicroelectronics	SLA0088
X509 certificate parser for X CUBE CRYPTOLIB	STMicroelectronics	SLA0044
Arm [®] Mbed [™] transport layer security (TLS) ⁽²⁾	Arm	Apache 2.0
Demonstration codes	STMicroelectronics	SLA0044

1. *BSD stands for Berkeley Software Distribution.*

2. *Arm and Mbed are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.*

Revision history

Table 2. Document revision history

Date	Version	Changes
09-Dec-2019	1	Initial release.
13-Dec-2019	2	Added Section 2 Licence .

IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please 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.

© 2019 STMicroelectronics – All rights reserved