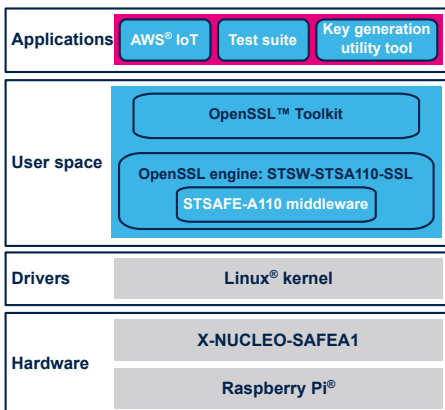


STSAFE-A110 *OpenSSL*[®] engine software package



Features

- Open access to the **STSAFE-A110's** authentication and security services on systems running *OpenSSL*[®]
- Compliant with the ENGINE cryptographic module support of *OpenSSL*.
- Connects to the user's Amazon Web Services[™] (AWS[™]) IoT account over a secure transport layer security (TLS) connection.
- Extends the *OpenSSL* toolkit's cryptographic features thanks to the use of the **STSAFE-A110** solution.
- Provides a test suite of 15 tests for:
 - Query functions to retrieve the product information
 - Envelop wrapping/unwrapping
 - Elliptic-curve digital-signature algorithm (ECDSA) signature/verification
 - Elliptic curve Diffie–Hellman (ECDH) generation of ephemeral keys
 - Reading certificates
 - Random number generation
 - Secure storage
- Provides a key generation utility tool that allows keys to be generated in the **STSAFE-A110** device.

Applications

- ECDSA authentication (for instance of peripherals, IoT or 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
- Cloud connectivity to Amazon[®]

Description

The **STSW-STSA110-SSL** software package can be used as an *OpenSSL*[®] engine (hardware support) or a C library for any Linux[®] application utilizing the **STSAFE-A110** hardware.

The **STSAFE-A110** is a highly secure solution that acts as a secure element providing authentication and secure data management services to a local or remote host. It consists of a full turnkey solution with a secure operating system running on the latest generation of secure microcontrollers.

Product status link

[STSW-STSA110-SSL](#)



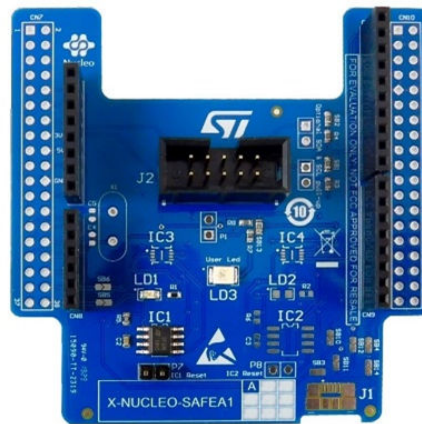
1 Setting up the hardware environment

This section describes the hardware components needed for developing a secure application.

1.1 STSAFE-A1xx expansion board

The hardware environment includes the STSAFE-A1xx expansion board (X-NUCLEO-SAFEA1). The figure below illustrates the board.

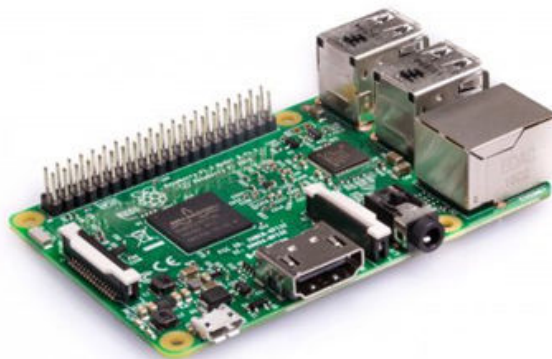
Figure 1. STSAFE-A1xx expansion board



1.2 Raspberry Pi® model board

A Raspberry Pi® model board is also required as part of the hardware environment. Information about Raspberry Pi (RPI) boards is available at: <https://www.raspberrypi.org/>. The figure below provides an illustration of this type of board.

Figure 2. Raspberry Pi board



2 License

STSW-STSA110-SSL is delivered under STMicroelectronics' *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
X-CUBE-SAFE ^{A1} application programming interface (API)	STMicroelectronics	SLA0088
Demonstration codes	STMicroelectronics	SLA0088
OpenSSL [®] API interface ⁽¹⁾⁽²⁾	The OpenSSL Project	OpenSSL License
API interface ⁽¹⁾	Eric Young (eay@cryptsoft.com)	Original SSLeay License
STSAFE securing a connection with AWS IoT example	Amazon.com	Amazon license

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<https://www.openssl.org/>).
2. OpenSSL is a registered trademark owned by the OpenSSL Software Foundation.

Revision history

Table 2. Document revision history

Date	Version	Changes
10-Dec-2020	1	Initial release.

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.

© 2020 STMicroelectronics – All rights reserved