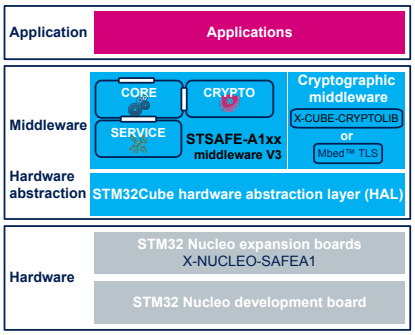
STSW-SAFEA1-MW

Data brief

STSAFE-A1xx middleware software



Product status link
STSW-SAFEA1-MW

Features

- Complete middleware library with a new redesigned architecture to improve robustness, security, reliability, scalability and maintainability
- CORE module to simplify integration in customer applications
- CRYPTO module to isolate all the cryptographic operations:
  - increased security level
  - reduced attack surface
- SERVICE module to enhance the hardware abstraction and the platform independence
- Memory optimization configuration to get the best from the available host MCU memory
- CRYPTO and SERVICE interfaces for easy customization at application level
- Compliance with the new STM32 BSP 2.6.1 for a better integration across all STMicroelectronics software packages
- Compliance with MISRA C 2012
- Easy portability across different MCU families, thanks to the STM32Cube
- Free, user-friendly license terms

Description

The STSAFE-A1xx middleware, called STSW-SAFEA1-MW, is a software component that provides a complete set of APIs to access the STSAFE-A100 or STSAFE-A110 device features from a host microcontroller.

The middleware is built on the STM32Cube software technology to ease portability across different STM32 microcontrollers.

It is also MCU-agnostic for additional portability across different MCUs.

The STSAFE-A100 and STSAFE-A110 are highly secure solutions. They act as secure elements to provide authentication and data management services to a local or remote host. They consist of a full turnkey solution with a secure operation system. They can be integrated in IoT devices, consumer electronics devices, consumables and accessories as well as smart-home, smart-city and industrial applications.

1 What is STM32Cube?

STMicroelectronics initiated the STM32Cube initiative to ease the developers' life by reducing the development effort, time and cost. The STM32Cube covers the STM32 portfolio.

STM32Cube Version 1.x includes:

- STM32CubeMX, a graphical software configuration tool that allows C initialization code to be generated using graphical wizards;
- A comprehensive embedded software platform, delivered per series (such as the STM32CubeF4 for the STM32F4 Series);
  - The STM32Cube *HAL*, an STM32 abstraction-layer embedded software, ensuring maximized portability across the STM32 portfolio;
  - A consistent set of middleware components such as *RTOS*, *USB*, *TCP/IP* and graphics;
  - All embedded software utilities coming with a full set of examples.

The STM32F4 Series, and STM32 devices in general, are Arm®-based devices.

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

2 How does this software complement the STM32Cube?

The proposed software is hardware-independent, but provides a SERVICE interface template based on the STM32Cube HAL, the hardware abstraction layer for the STM32 microcontroller. The SERVICE interface can be customized at application level to adapt the middleware to the supported MCUs and platforms. The package supports the new BSP 2.6.1 I/O bus drivers that can be easily ported to different platforms.

STSW-SAFEA1-MW provides a CRYPTO interface template for the Arm® Mbed™ TLS and the ST cryptographic library (X-CUBE-CRYPTOLIB). This interface thus allows the user application to select the cryptographic library and related features that the middleware needs (such as SHA or AES.).

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
28-Jan-2022	1	Initial release.

Glossary

AES Advanced encryption standard

API Application programming interface

BSP Board support package

HAL Hardware abstraction layer

I/O Input/output

IoT Internet of things

MCU Microcontroller unit

MISRA Motor Industry Software Reliability Association

MISRA C MISRA C is a software development language subset that was originally created to promote the use of the C programming language in safety-critical embedded applications within the motor industry.

RTOS Real-time operating system

Session A session starts upon one reset event and ends with the next reset event. Reset events are defined in all secure IC datasheets.

SHA Secure Hash algorithm

ST STMicroelectronics

TCP/IP Transmission control protocol/internet protocol

TLS Transport layer security

USB Universal serial bus