Security Target for XCUBE SBSFU on STM32L476RG

Version 1.0, dated 2020-02-19

ST Microelectronics

1 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [SESIP] (in chapter “Security requirements and implementation”) and that a potential consumer can rely upon the product upholding if they fulfill the objectives for the environment (in chapter “Security Objectives for the operational environment”).

1.1 ST reference

See title page.

1.2 Platform reference

TOE name	*XCUBE SBSFU on STM32L476RG*
TOE version	*2.2.0*
TOE identification	*Microcontroller: 0x10076415 (DBGMCU_IDCODE mcu register value)* *SBSFU: e49d8458b477341c71573552c63ac21b22b969508deeaa69a4b14dc28a93f0a3*
TOE Type	*Root of Trust solution for IoT applications*

1.3 Included guidance documents

The following documents are included with the platform:

Reference	**Name**	**Version**
[CPG]	*XCUBE SBSFU on STM32L476R Certified Product Guidance*	*Ver. 0.3*
[AN5056]	*Application Note - Integration guide for the X-CUBE-SBSFU STM32Cube Expansion Package*	*Rev.4*
[AN5156]	*Application Note - Introduction to STM32 microcontrollers security*	*Rev.2*
[RM0351]	*Reference manual – STM3222L4x5 and STM32L4x6 advanced Arm-based 32-bit MCUs*	*Rev.6*
[UM2262]	*User Manual – Getting started with the X-CUBE-SBSFU STM32Cube Expansion Package*	*Rev.5*
[UM2285]	*User Manual – Development guidelines for STM32Cube Expansion Packages*	*Rev.1*
[UM1860]	*User Manual – Getting started with STM32CubeL4 for STM32L4 Series and STM32L4+ Series user manual*	*Rev.12*
[RM0351]	*Reference manual* *STM32L4x5 and STM32L4x6 advanced Arm®-based 32-bit MCUs*	Rev 6

1.4 Platform functional overview and description

The TOE consists of a Secure Boot (SB) and Secure Firmware Update (SFU) solution running on a STM32L476RG microcontroller, which is used as Root of Trust solution for IOT application.

The TOE is intended to be used by an integrator that deploys it into an IoT solution together with its own user application, providing assurance that the IoT application is securely booted and can be securely updated.

The main security features of the TOE are as follows:

- Secure Boot, ensuring authenticity and integrity of the user application.
- Secure Firmware Update with dual image support and three cryptographic schemes to protect the authenticity, integrity and confidentiality of the updates.
- Anti-rollback of user application, preventing an older than the actual version being installed in the platform.

The integrator can customize the SBSFU solution. The SBSFU solution is then protected and made immutable by using chip features once deployed.

The physical scope is delimited by the purple dotted line, as depicted in Figure 1, which comprises the SBSU application using services running in the Secure Enclave:

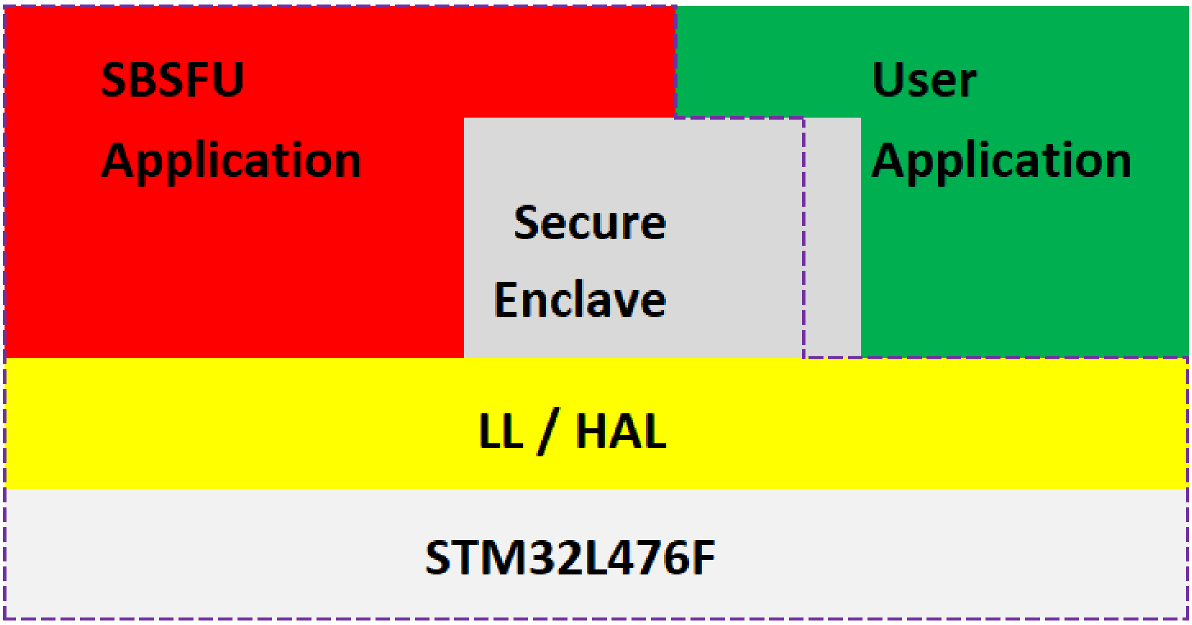

Figure 1 TOE scope

The SBSFU application uses a hardware execution firewall protected Secure Enclave to isolate the sensitive data and code from the user application. Note that part of the Secure Enclave, also known as Secure Engine, is out of the scope of the TOE, since it is the space that can be programmed for the User Application.

The cryptographic library used by the TOE to support the TOE functionality offers four different cryptographic schemes. Nevertheless, the applicable cryptographic schemes applicable to the TOE configuration are:

SECBOOT_CRYPTO_SCHEME value	Authentication	Confidentiality	Integrity
SECBOOT_ECCDSA_WITH_AES128_SHA256	ECDSA	AES128-CBC	SHA256
SECBOOT_AES128_GCM_AES128_GCM_AES128_GCM	AES GCM		

, since these are the ones that ensure integrity, authenticity and confidentiality of the user application installed on top of the SBSFU solution.

The source code of the SBSFU application is provided to the integrator with the exception of the crypto library, which is provided in compiled binary format. The integrator is also provided development support tools to create user applications and an example user application.

The integrator uses the security functionality provided by the TOE to develop a secure IoT solution. The developer provides a demo application that serves as a test application for the security functionalities.

1.4.1 Non-TOE Hardware, Software and Firmware

No non-TOE components are required by the XCUBE SBSFU solution.

2 Security Objectives for the operational environment

This section identifies and describes the security objectives that are to be addressed by the IT domain or by non-technical or procedural means along with references to the guidance documents that address such objectives.

SBSFU_SECRETS

The SBSFU secret keys used to protect the integrity, confidentiality and authenticity of the installed user application and the integrity, authenticity and the confidentiality of the user application firmware updates need to be preserved under custody of the user application developer.

, as described in §3.2.4 of [CPG] and Appendix D of [UM2262].

TRUSTED_INTEGRATOR

The integrator uses the security functionalities needed by the user application following the TOE guidance documentation. The integrator is trusted and does not attempt to thwart the TOE security functionalities nor bypass them. Specially the Secure Engine part accessible to the user –which is out of the scope of the TOE-, shall not be modified in a way that introduces a vulnerability in the TOE.

, as described in §3.2.4 of [CPG] and §6.2.4 of [UM2262].

KEY_DIVERSIFICATION

The integrator uses the AES GCM key provided by the TOE to derive unique keys for each device using the TOE, in order to use symmetric scheme to preserve confidentiality, integrity and authenticity of the assets.

, as described in §3.2.4 of [CPG].

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP1** as defined in [SESIP].

The requirements for this assurance level are met by the evidence supplied for certification, specified in section “SESIP1 sufficiency”.

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to give generate any needed update and distribute it, the developer has defined the following procedure:

To report a security vulnerability impacting a STM32 product or solution, you should contact STM32-CyberTeam through ***stm32-security@st.com***.

Your findings should include the following information:

- Full references of the product (full part number) or solution (software versions, tools versions, …)
- Detailed description of the vulnerability
- All instructions needed to reproduce the issue
- Impact of the reported vulnerability, including details of the exploit

Due to the sensitivity of vulnerability information, it is recommended to provide your findings through encrypted email using the below STM32-CyberTeam PGP/GPG Key.

Vulnerability management process

Security vulnerabilities related to STM products are managed by the STM32-CyberTeam through the following 4 stages process:

- Reporting: Any new issue being reported to the STM32-CyberTeam
- Evaluating: STM32 Cyber-Team will evaluate the potential vulnerability, by confirming the issue, analyze it and set a priority for resolving it.
- Solving: STM32 Cyber-Team will collaborate with division R&D to investigate a solution to mitigate or solve the issue. Depending on the component impacted (hardware, firmware, tools) the leadtime to bring that solution to the market may vary. At this stage, an internal ticket will be created and managed.

- Communicating: Once a solution is available (fix or mitigation), ST will manage communicating back. Depending on the nature of the vulnerability and the mitigation, an appropriate action will be communicated to ST customers. The disclosure may be public or could target a restricted list of customers.

Note that the SBSFU application cannot be updated. The reason is that the TOE is an efficient and small component and adding additional functionalities would increase the security threats and complexity.

3.1.2 Vulnerability Survey (AVA_VAN.1)

An independent evaluation laboratory carried out a vulnerability analysis based on the traditional white-box approach defined in SESIP3 [SESISP] providing a substantial level of assurance. In addition, scalable attacks were also considered within the scope of the evaluation.

As a result, the certified TOE is considered resistant against the attacks based on the SESIP3 methodology [SESIP].

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Identification of platform type

The platform provides a unique identification of the platform type, including all its parts and their versions.

Rationale

The platform provides a unique identification of the microcontroller supporting the TOE, as described in §48.6.1 “MCU device ID code” of [RM0351].

The TOE unique identifier is provided in section 1.2: this is the SHA256 calculation of the complete ZIP SBSFU file delivered through st.com to customers.

This requirement is tested by the evaluation laboratory against ATE_IND.1 and AVA_VAN.3 in the scope of a SESIP3 evaluation, which exceeds the requirements for a SESIP1 evaluation claimed in this ST.

~~3.2.2 Secure update of platform~~

~~The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.~~

3.2.3 Secure install of application

The application can be installed in the field such that the integrity, authenticity and confidentiality of the application is maintained.

Rationale

The installation process is executed using the secure functions from the Secure Enclave, and authenticity, integrity and confidentiality of the process are ensured by using the mechanisms identified in section 1.4.

The installation process consists of writing the encrypted image and its header into slot #1 of the flash memory. The installation image authenticity is ensured by ECDSA or AES-GCM, integrity is ensured by SHA256 or AES-GCM and confidentiality is ensured by using AES-CBC or AES-GCM encryption.

This requirement is tested by the evaluation laboratory against ATE_IND.1 and AVA_VAN.3 in the scope of a SESIP3 evaluation, which exceeds the requirements for a SESIP1 evaluation claimed in this ST.

3.2.4 Secure update of application

The application can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the application is maintained.

Rationale

The update process consists of a dual image process using Slot #1 and Slot #0 as depicted in Figure 2.

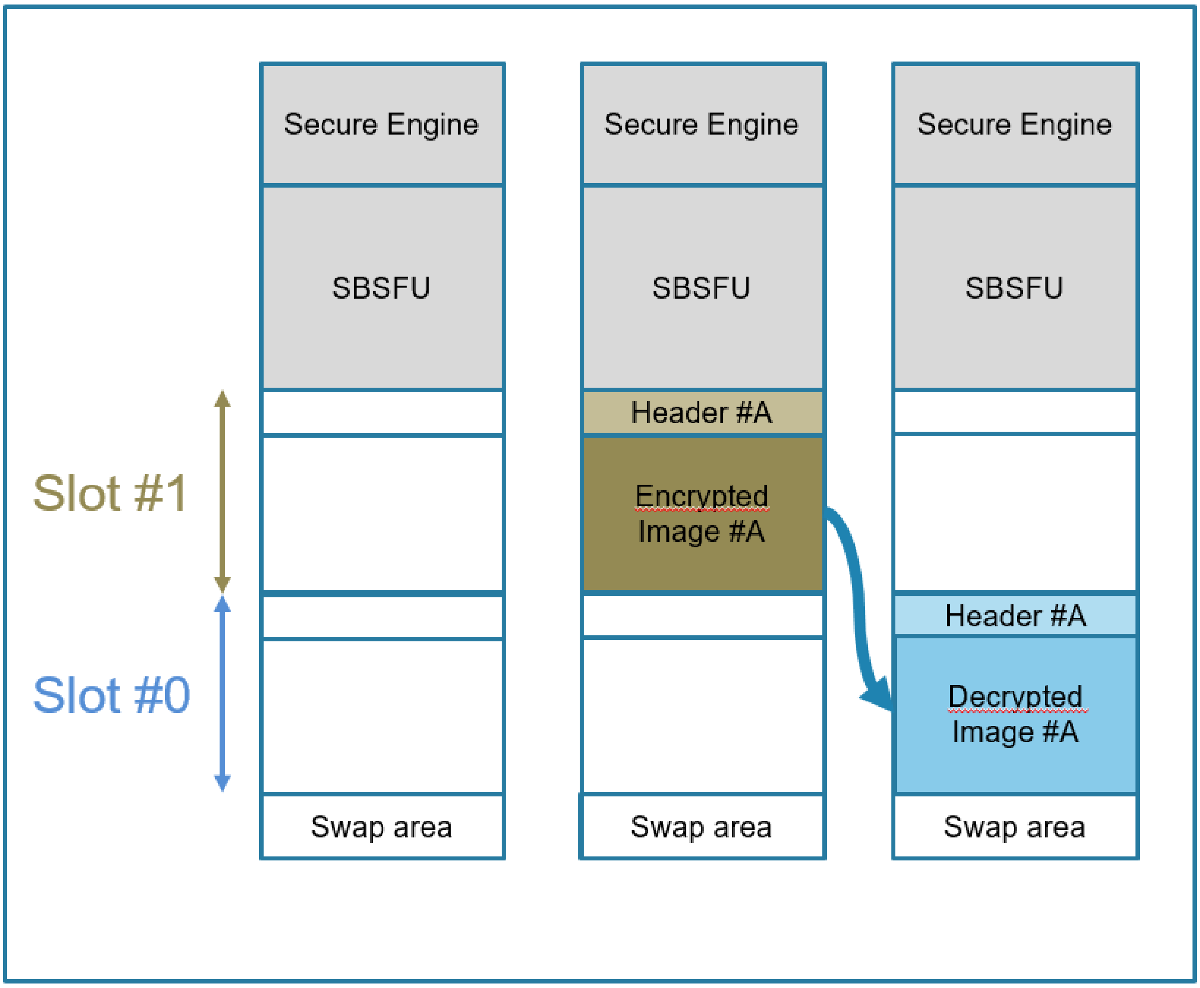

Figure 2 Application update process

The update process is executed using the secure functions from the Secure Enclave, and authenticity, integrity and confidentiality of the process are ensured by using the mechanisms identified in section 1.4.

The update process consists of writing the encrypted image and its header into slot #1 of the flash memory. The update candidate authenticity is ensured by ECDSA or AES-GCM, integrity is ensured by SHA256 or AES-GCM and confidentiality is ensured by using AES-CBC or AES-GCM encryption.

The SBSFU checks that the update candidate is not a previous firmware version by means of the anti-rollback mechanism.
This requirement is tested by the evaluation laboratory against ATE_IND.1 and AVA_VAN.3 in the scope of a SESIP3 evaluation, which exceeds the requirements for a SESIP1 evaluation claimed in this ST.

3.2.5 Software attacker resistance: isolation of platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

Rationale

The user application can by no means modify the part of the Secure Enclave used by the SBSFU as it is protected by the WRP function of the chip, hence the configuration of both the Secure Boot and the Secure Firmware Update components is kept unchanged. Each SE functionality is executed completely as enforced by the chip firewall and the SBSFU functions are logically locked once the TOE gives control to the user application.

This requirement is tested by the evaluation laboratory against ATE_IND.1 and AVA_VAN.3 in the scope of a SESIP3 evaluation, which exceeds the requirements for a SESIP1 evaluation claimed in this ST.

4 Mapping and sufficiency rationales

4.1 SESIP1 sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section "Introduction" and title page	The ST reference is in the Title, the TOE reference in the "Platform reference", the TOE overview and description in "Platform functional overview and description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the operational environment"	The objectives for the operational environment in "Security Objectives for the operational environment" refers to the guidance
	ASE_REQ.3 Listed Security requirements	Section "Security requirements and implementation"	All SFRs in the profile are taken from [SESIP][1]. "Identification of platform type" is included. "~~Secure update of platform~~" is included.
	ASE_TSS.1 TOE Summary Specification	Section "Security Functional Requirements"	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in Security Functional Requirements **Rationale**.

[1] The developer must not remove or substantially change the SFRs listed in the ST, and must indicate any additional SFRs explicitly. The evaluator must check this in accordance to the assurance activity.

ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section “Flaw Reporting Procedure (ALC_FLR.2)”	The flaw reporting and remediation procedure is described.
AVA: Vulnerability Assessment	AVA_VAN.1 Vulnerability survey	Section “Vulnerability Survey (AVA_VAN.1)”	The vulnerability survey and associated test results are described.

5 References

[ST Template] SESIP Security template v1.3

[SESIP] Security Evaluation Scheme for IoT Platforms, version 1.3

[JIL-AP] Application of Attack Potential to Smart Cards and Similar Devices, v3.0

6 Document History

Version	Date	Comment	Author
0.1	02/2019	Initial draft version for scheme discussion	Brightsight B.V.
0.2	03/09/2019	Draft for SESIP3	Brightsight B.V.
0.3	04/09/2019	Downgrade to SESIP1	Brightsight B.V.
0.4	10/09/2019	After ST update	ST/MCD
0.5	17/09/2019	Following BS/ST alignment	ST/MCD
0.6	19/09/2019	Evaluator’s feedback addressed	Brightsight B.V.
0.7	01/10/2019	Following BS/ST alignment	ST/MCD
0.8	08/01/2020	Release to Certifier	Brightsight B.V.
1.0	19/02/20	Official Release	Brightsight B.V.