STMicroelectronics

STSafe S300 Security Target Lite

Common Criteria for IT security evaluation

Rev. A
Jul 31st 2020

INDEX

1 References 3

2 ST reference and TOE reference 4

3 TOE overview 5

4 TOE description 6

5 Conformance claims 9

6 Security problem definition 11
6.1 Assets 11
6.2 Subjects 11
6.3 Threats 11
6.4 Organisational Security Policies 12

7 Security Objectives 13
7.1 Security Objectives for the TOE 13
7.2 Security Objectives for the Operational Environment 13
7.3 Security Objectives rationale 13

8 Security requirements 15
8.1 SFA/Weaver SFRs 15
8.2 Loader SFRs 17
8.3 Security Assurance requirements 19
8.4 Security Functional Requirements Rationale 19
8.5 Security Assurance Requirements Rationale 21

9 TOE Summary specification 25
9.1 User Authentication and Access control 25
9.2 Stored Data Protection 26

10 Revision history 27

1 References

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1 Revision 5. April 2017.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[JCRE305]	JCRE 3.0.5 Classic Java Card 3 Platform Runtime Environment Specification, Classic Edition, version 3.0.5
[JCVM305]	JCVM 3.0.5 Classic Java Card 3 Platform Virtual Machine Specification, Classic Edition, version 3.0.5
[JCAPI305]	JCAPI 3.0.5 Classic Java Card API, Classic Edition, version 3.0.5
[GP_I2CSPI]	GlobalPlatform I2C/SPI GlobalPlatform Technology APDU Transport over SPI / I2C Version 0.0.0.39
[STLite_ST33G1M2]	ST33G1M2 C01 – Security target for composition, Rev C01.3, October 2019
[ST_STSafeS300]	STSafe S300 Security target – rev F – July 31st 2020

2 ST reference and TOE reference

Present document	
Title:	STSafe S300 Lite - Security Target Lite
Assurance Level:	EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5
Company:	STMicroelectronics
CC Version:	3.1 R5 [CC1] [CC2] [CC3]
PP Conformance:	None
Version:	Rev. A Jul 31st 2020

ST Reference	
Title:	STSafe S300 - Security Target
Assurance Level:	EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5
Company:	STMicroelectronics
CC Version:	3.1 R5 [CC1] [CC2] [CC3]
PP Conformance:	None
Version:	Rev. F Jul 31st 2020

Table 1 ST Reference

TOE Reference	
TOE name and version	STSafe S300 v1.2.5
Operational Guidance	[AGD_OPE] Rev. D
Preparative Guidance	[AGD_PRE] Rev. C

Table 2 TOE Reference

This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.

3 TOE overview

STSafe S300 is a Secure element product that offers secure storage capability over the Weaver and SFA applications, intended to be used as a secure storage element by a mobile phone. The product offers also an additional functionality called “Firmware Upgrade OS” that allows Operational OS firmware update.

The TOE is a composition of a Java Card OS and the SFA and Weaver applications, with the ST33G1M2 IC platform (including Neslib and Storekeeper). Details of these TOE parts are provided in the following sections.

4 TOE description

Product overview

STSafe S300 is a Secure element product that offers secure storage capability over the Weaver and SFA applications, intended to be used as a secure storage element by a mobile phone.

The product is composed by two different Operating Systems (Oss):

1) Operational OS

The Operational OS offers secure storage capability and it is composed by several elements:

- The Weaver application
- The SFA Application

Supported communication protocols are SPI and I2C according to [GP_I2CSPI], both co-exist together and are selected in the product through a PIN modulation.

The product supports also a Java Card Virtual machine and GlobalPlatform functionalities. Card content management functionalities are disabled.

2) Firmware Upgrade OS

The product contains also an additional operating system, called “Firmware Upgrade OS” that is used to patch the operational OS firmware at OEM factory or on the field.

The “Firmware Upgrade OS” communicates over the SPI / I2C protocols according to [GP_I2CSPI].

Hardware description

The hardware is ST33G1M2, secure chip based on SC300 core [STLite_ST33G1M2]. The specific versions of the hardware parts are as follow:

Hardware identifier	ST33G1M2 (maskset K8H0A version F) Firmware revision A
Neslib version	v6.3.4
Storekeeper version	V1.0.9

Note that the NESlib version is present twice, once for the Operational OS and once for the Firmware Upgrade OS. The Storekeeper on the other side is present only in the Operational OS.

Physical / Communication Protocol

The device communicates over the SPI/I2C interface according to [GP_I2CSPI].

The SPI/I2C library, implementing the Physical / communication protocol, is present twice (once for the Operational OS and once for the Firmware Upgrade OS).

Java Card

Java Card functionality is partially included in the TOE; more specifically, the product includes a fully functional Java Card Virtual Machine [JCVM305], a Java Card Runtime Environment [JCRE305] and Java Card API [JCAPI305] compliant to Java Card 3.0.5 specification.

As the product is closed with pre-loaded applications, only the required subset of Java Card functionalities is considered part of the TOE.

Secure Flash Application (SFA) and Weaver Application

The TOE provides two different applications for accessing two separate secure memories. The SFA is the default application; SFA application is operational only on logical channel 0, while Weaver application is operational only on logical channel 1.

.

TOE composition and identification

The TOE is the composition of a Java Card OS (including SFA and Weaver applications) over the Storekeeper library and the NESlib library, based on ST33G1M2 chip. The device has been certified Common Criteria together with the NESlib version.

As defined in [ADG_OPE], as the TOE is made by two Operating systems (Operational OS and Firmware Upgrade OS), the two Oss have independent GET DATA commands that return the two OS versions.

As the Operational OS uses the NESlib and the Storekeeper, the Operational OS GET DATA command returns also NESlib and Storekeeper versions.

As the Firmware Upgrade OS uses the NESlib, the Firmware Upgrade OS GET DATA command returns also NESlib version.

Both GET DATA commands allow also to identify the Hardware.

The Hardware and the NESlib that are part of the TOE are certified as follows:

Hardware identifier	ST33G1M2 (maskset K8H0A version F) Firmware revision A	ANSSI-CC-2020/22
Neslib version	v6.3.4	ANSSI-CC-2020/22
Store keeper version	V1.0.9	V1.0.7 certified ANSSI-CC-2017/73 During CC evaluation differences between v1.0.7 and v1.0.9 will be evaluated

The TOE certification applies to the following versions:

OS	V1.2.5
Weaver applet	V1.2.5

For further details, refer to [AGD_OPE].

5 TOE Delivery

The TOE will be delivered on the Secured Microcontroller STMicroelectronics ST33G1M2 with Cryptographic Library

The TOE will be delivered in the format “Wafer level chip scale package” (WLCSP), with OS and initial key preloaded.

User and Administrator guidance delivered in paper and (.pdf) format.

- STSafe S300 – Operational User Guidance [AGD_OPE]
- STSafe S300 – Preparative Procedure [AGD_PRE]

6 Conformance claims

The ST claims conformance to Common Criteria Version 3.1 revision 5 part 2 conformant [CC2] and part 3 conformant [CC3].

The ST does not claim conformance to any Protection Profile.

The TOE assurance level claim is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

7 Security problem definition

7.1 Assets

Assets	Description
Data stored in memory	All data stored in the SFA secure memory and the Weaver secure memory, accessible to valid authenticated users through the SFA and Weaver applications interfaces.
Authentication keys	Keys used to authenticate the user for accessing the SFA and Weaver functionality, as well as for performing a software loading operation.
Software image	The software image running on the TOE, which can be updated by a valid authenticated user through the software loader functionality.

Table 3 Assets

7.2 Subjects

Subjects	Description
SFA user	User accessing the SFA secure memory through the SFA application.
Weaver user	User accessing the Weaver secure memory through the Weaver application.
Loader user	User accessing the Loader functionality to perform a software loading operation.

Table 4 Subjects

7.3 Threats

Threats	Description
T.DATA_DISCLOSE	An attacker performs unauthorised disclosure of data stored in the SFA secure memory and Weaver secure memory, or the disclosure of the authentication keys, by means of software/hardware attacks.
T.DATA_MODIFY	An attacker performs unauthorised modification of the data stored in the SFA secure memory and Weaver secure memory, or the disclosure of the authentication keys, by means of software/hardware attacks.
T.LOADER_MISUSE	An attacker performs unauthorised use of the software

	loader functionality to upload a modified or malicious software version.

Table 5 Threats

7.4 Organisational Security Policies

Policies	Description
P.KEY_PERSO	The default SFA binding keys and the Loader keys are updated by the phone manufacturer during the manufacturing phase of the TOE. After the final keys are set, the TOE state is changed to the final usage phase.

Table 6 Organisational Security Policies

8 Security Objectives

8.1 Security Objectives for the TOE

Objectives	Description
OT.DATA_PROTECTION	The TOE shall protect the integrity of the data stored in the secure memory from software/hardware attacks, to ensure that the stored data can only be modified by a valid authenticated user through the defined TOE interfaces. This objective also includes the protection of the authentication keys.
OT.ACCESS_CONTROL	The TOE shall provide access control mechanisms to ensure only valid authenticated users can access the TOE functionality, i.e. SFA application, Weaver application and Loader functionality.

Table 7 TOE Security Objectives

8.2 Security Objectives for the Operational Environment

Objectives	Description
OE.KEY_PERSO	The operational environment shall ensure that when the TOE life cycle is in manufacturing state, and before it is set to release state, all the default keys in the TOE are updated with final usage phase keys, including the SFA binding keys and the software loading keys.

Table 8 Security Objectives for the operational environment

8.3 Security Objectives rationale

The following table shows how the security objectives for the TOE cover the threats.

Threats / Security Objectives	OT.DATA_PROTECTION	OT.ACCESS_CONTROL
T.DATA_DISCLOSE		X
T.DATA_MODIFY	X	
T.LOADER_MISUSE		X

Table 9 Mapping of threats to TOE security objectives

The threats **T.DATA_DISCLOSE** and **T.LOADER_MISUSE** are covered by the security objective OT.ACCESS_CONTROL, which ensures that all the TOE functionality (SFA application, Weaver application and Loader functionality) can only be accessed by valid authenticated users.

The threat **T.DATA_MODIFY** is covered by the security objective OT.DATA_PROTECTION, which ensures the integrity of the data stored in secure memory so it can only be modified through the TOE interfaces and by valid authenticated users.

The following table shows how the security objectives for the operational environment cover the OSP.

OSPs / Security Objectives	OE.KEY_PERSO
P.KEY_PERSO	X

Table 10 Mapping of OSP to security objectives of the environment

The OSP **P.KEY_PERSO** is covered by the environment security objective OE.KEY_PERSO, which enforces that the default TOE keys are updated by the phone manufacturer before the TOE is set to the final usage phase (URS).

9 Security requirements

Operations completed in this ST are shown in underline.

9.1 SFA/Weaver SFRs

FTP_ITC.1/SFA-Weaver Inter-TSF trusted channel	
Hierarchical to: No other components. Dependencies: No dependencies.	
FTP_ITC.1.1/SFA-Weaver	The TSF shall provide a communication channel between itself and the SFA user or the Weaver user that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SFA-Weaver	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/SFA-Weaver	The TSF shall initiate communication via the trusted channel for performing Read, Write or Erase operations through the SFA application or Weaver application.

FDP_ACC.1/SFA-Weaver Subset access control – SFA and Weaver	
Hierarchical to: No other components. Dependencies: FDP_ACF.1 Security attribute based access control.	
FDP_ACC.1.1/SFA-Weaver	The TSF shall enforce the SFA-Weaver SFP on (1) the subjects: SFA user, Weaver user, (2) the objects: data in SFA secure memory, data in Weaver secure memory (3) the operations: Read, Write and Erase

FDP_ACF.1/SFA-Weaver Security attribute based access control – SFA and Weaver
Hierarchical to: No other components. Dependencies: FMT_MSA.3 Static attribute initialization, FDP_ACC.1 Subset access control

FDP_ACF.1.1/SFA-Weaver	The TSF shall enforce the SFA-Weaver SFP to objects based on the following: (1) the subjects: SFA user, Weaver user with security attributes “Authenticated”, (2) the objects: the data in SFA secure memory with security attributes none, and the data in Weaver memory with security attributes none.
FDP_ACF.1.2/SFA-Weaver	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the SFA user with security attribute “Authenticated” set to “yes” can read, write or erase the data in the SFA secure memory through the SFA application. (2) the Weaver user with security attribute “Authenticated” set to “yes” can read, write or erase the data in the Weaver secure memory through the Weaver application.
FDP_ACF.1.3/SFA-Weaver	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SFA-Weaver	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: (1) the SFA user with security attribute “Authenticated” set to “no” cannot access the data in secure memory. (2) the Weaver user with security attribute “Authenticated” set to “no” cannot access the data in secure memory.

FDP_ETC.1 Export of user data without security attributes	
Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	
FDP_ETC.1.1	The TSF shall enforce the SFA-Weaver SFP when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data’s associated security attributes.

FDP_ITC.1 Import of user data without security attributes	
Hierarchical to: No other components. Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_MSA.3 Static attribute initialization	
FDP_ITC.1.1	The TSF shall enforce the SFA-Weaver SFP when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

FDP_SDI.2 Stored data integrity monitoring and action	
Hierarchical to: FDP_SDI.1 Stored data integrity monitoring Dependencies: No dependencies.	
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: SFA secure memory integrity status, Weaver secure memory integrity status.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data (2) inform the user about integrity error

9.2 Loader SFRs

FTP_ITC.1/Loader Inter-TSF trusted channel	
Hierarchical to: No other components. Dependencies: No dependencies.	
FTP_ITC.1.1/Loader	The TSF shall provide a communication channel between itself and the Loader user that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/Loader	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/Loader	The TSF shall initiate communication via the trusted channel for performing a software loading operation.

FDP_UCT.1 Basic data exchange confidentiality	
Hierarchical to: No other components. Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	
FDP_UCT.1.1	The TSF shall enforce the Loader SFP to receive user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components. Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	
FDP_UIT.1.1	The TSF shall enforce the Loader SFP to receive user data in a manner protected from modification, deletion, insertion errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

FDP_ACC.1/Loader Subset access control – Loader	
Hierarchical to: No other components. Dependencies: FDP_ACF.1 Security attribute based access control.	
FDP_ACC.1.1/Loader	The TSF shall enforce the Loader SFP on (1) the subjects: Loader user, (2) the objects: software image data, (3) the operation: performing a software loading

FDP_ACF.1/Loader Security attribute based access control – Loader	
Hierarchical to: No other components. Dependencies: FMT_MSA.3 Static attribute initialization, FDP_ACC.1 Subset access control	
FDP_ACF.1.1/Loader	The TSF shall enforce the Loader SFP to objects based on the following: (1) the subjects: Loader user with security attributes "Authenticated", (2) the objects: software image data in memory with security attributes none.
FDP_ACF.1.2/Loader	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the Loader user with security attribute "Authenticated" set to "yes" can perform a software loading operation.
FDP_ACF.1.3/Loader	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: (1) the Loader user with security attribute "Authenticated" set to "no" cannot perform a software loading operation.

9.3 Security Assurance requirements

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.2 Sufficiency of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample.
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 11 Security Assurance requirements

9.4 Security Functional Requirements Rationale

The following table shows the mapping of TOE security functional requirements to the TOE security objectives:

SFR / TOE objectives	OT.DATA_PROTECTION	OT.ACCESS_CONTROL
FTP_ITC.1/SFA-Weaver		X
FDP_ACC.1/SFA-Weaver		X
FDP_ACF.1/SFA-Weaver		X
FDP_ETC.1		X
FDP_ITC.1		X
FDP_SDI.2	X	
FTP_ITC.1/Loader		X

FDP_UCT.1	X	X
FDP_UIT.1	X	X
FDP_ACC.1/Loader		X
FDP_ACF.1/Loader		X

Table 12 Mapping of SFR to TOE security objectives

The following table shows the coverage of the SFR dependencies:

SFR	Dependency	Satisfied by
FTP_ITC.1/SFA-Weaver	None.	n/a
FDP_ACC.1/SFA-Weaver	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/SFA-Weaver
FDP_ACF.1/SFA-Weaver	FMT_MSA.3 Static attribute initialization FDP_ACC.1 Subset access control	FMT_MSA.3 is not required because the security attributes used to enforce the SFA-Weaver SFP are fixed during manufacturing phase and no new objects under control of the SFA-Weaver SFP are created. FDP_ACC.1/SFA-Weaver
FDP_ETC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1/SFA-Weaver
FDP_ITC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/SFA-Weaver FMT_MSA.3 is not required because the security attributes used to enforce the SFA-Weaver SFP are fixed during manufacturing phase and no new objects under control of the SFA-Weaver SFP are created.
FDP_SDI.2	None.	n/a
FTP_ITC.1/Loader	None.	n/a

FDP_UCT.1	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FTP_ITC.1/Loader FDP_ACC.1/Loader
FDP_UIT.1	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FTP_ITC.1/Loader FDP_ACC.1/Loader
FDP_ACC.1/Loader	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Loader
FDP_ACF.1/Loader	FMT_MSA.3 Static attribute initialization FDP_ACC.1 Subset access control	FMT_MSA.3 is not required because the security attributes used to enforce the Loader SFP are fixed during manufacturing phase and no new objects under control of the Loader SFP are created. FDP_ACC.1/Loader

Table 13 SFR dependencies coverage

9.5 Security Assurance Requirements Rationale

The assurance level for this ST is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for the current TOE.

10 Statement of composition

This is a Statement of Compatibility between this Composite ST and the IC Platform ST of the hardware and associated crypto-library ST33G1M2 [STLite_ST33G1M2]. The following mappings regarding SFRs, objectives and assurance requirements demonstrate the compatibility between the Composite Security Target and the IC platform ST33G1M2 ST.

The following table lists the Integrated Circuit ST33G1M2 Platform Security Functionalities for the Composite TOE.

IC Platform ST33G1M2 SFRs	Composite ST SFRs
FDP_SDC.1 FDP_SDI.2	FDP_ACC.1/SFA-Weaver FDP_SDI.2
FCS_RNG.1 FCS_COP.1 FAU_SAS.1	FTP_ITC.1/SFA-Weaver FTP_ITC.1/Loader FDP_ACC.1/SFA-Weaver FDP_ACC.1/Loader FDP_ETC.1 FDP_ITC.1 FDP_UIT.1 FDP_UCT.1
FDP_ACF.1/Memories FDP_ACC.2/Memories	FDP_ACC.1/SFA-Weaver FDP_ACC.1/Loader FDP_ACF.1/SFA-Weaver FDP_ACF.1/Loader

FRU_FLT.2 FPT_FLS.1 FMT_LIM.1/Test FMT_LIM.2/Test FMT_LIM.1/Loader FMT_LIM.2/Loader FPT_PHP.3 FDP_ITT.1 FPT_ITT.1 FDP_IFC.1 FDP_ACC.2/Memories FDP_ACF.1/Memories FMT_MSA.3/Memories FMT_MSA.1/Memories FMT_SMF.1/Memories FDP_ACC.1/Loader FDP_ACF.1/Loader FMT_MSA.3/Loader FMT_MSA.1/Loader FMT_SMR.1/Loader FIA_UID.1/Loader FMT_SMF.1/Loader FDP_ITC.1/Loader	The SFRs are considered as protection for the whole TOE, as they provide generic security mechanisms implicitly used by the TOE security functionalities
FCS_CKM.1 All MFPlus SFRs All DESFire SFRs All APPLI_FWL SFRs	IP_SFR: Not relevant / Not used

There is no conflict between security objectives of the Composite ST and the IC platform ST33G1M2 ST:

ST33G1M2 Objectives	Composite ST Objectives
BSI.O.Leak-Inherent BSI.O.Leak-Forced BSI.O.Phys-Probing BSI.O.Phys-Manipulation BSI.O.Abuse-Func BSI.O.Malfunction	OT.ACCESS_CONTROL OT.DATA_PROTECTION
BSI.O.Identification BSI.O.RND AUG1.O.Add-Functions BSI.O.Cap-Avail-Loader O.Controlled-ES-Loading AUG4.O.Mem Access	OT.ACCESS_CONTROL
	Additional Objectives
BSI.OE.Resp-Appl BSI.OE.Process-Sec-IC	OE.KEY_PERSO

11 TOE Summary specification

The TOE is made by two Operating systems, the Operational OS and the Firmware Upgrade OS.

For the Operational OS two specific secure memory applications are identified, SFA and Weaver, that can be used by distinct users (SFA user and Weaver user). TOE provides secure storage of SFA and Weaver memory objects and requires user authentication to access data in read and in write. In addition, data integrity is ensured of both secure storage content and of key material.

The Firmware Upgrade OS allows the patching of the Operational OS that can be performed only by a specific user (Loader user) that needs to be authenticated. TOE verifies patch integrity and compatibility with existing firmware before applying the patch.

11.1 User Authentication and Access control

For Weaver User, SFA User and Loader User, authentication is achieved through the establishment of the secure channel.
The secure channel can be established using 3 different key sets, each corresponding to the 3 different TOE users: SFA user, Weaver user and Loader user. The TOE enforces access control by verifying that specific actions are authorized by the proper credential. Establishment of the secure channel with either of the 3 key sets provides access to the SFA application, Weaver application and the Loader functionality for each corresponding user.

Operational OS security operations are authorized to SFA and Weaver Users, while Firmware Upgrade OS security operations are authorized to Loader User.

This functionality meets the SFR related to user authentication and access control:

Operational OS functionalities authentication and access control:

- FTP_ITC.1/SFA-Weaver
- FDP_ACC.1/SFA-Weaver
- FDP_ACF.1/SFA-Weaver
- FDP_ETC.1
- FDP_ITC.1
- FDP_UCT.1
- FDP_UIT.1

Firmware Upgrade OS functionalities authentication and access control:

- FTP_ITC.1/Loader
- FDP_UCT.1

- FDP_ACC.1/Loader
- FDP_ACF.1/Loader
- FDP_UIT.1

11.2 Stored Data Protection

The TOE provides secure storage based on flash memory being managed by tearing safe transfer and wear-levelling mechanisms.

This functionality meets the SFR related to integrity protection of stored data, keys and firmware images:

- FDP_SDI.2

12 Revision history

Version	Subject
A	Initial Release