STMicroelectronics

ST31R480 B01 with Random Number Generator software library Security Target for composition

Common Criteria for IT security evaluation

SMD_ST31R480_ST_23_004 Rev B01.4

December 2024

www.st.com

BLANK

ST31R480 B01 platform
Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: ST31R480 B01 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev B01.4, issued in December 2024.

3 Registration: registered at STMicroelectronics under number SMD_ST31R480_ST_23_004.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the **ST31R480 B01** Security Integrated Circuit (IC), designed on the **ST31 platform of STMicroelectronics**, with firmware version 3.0.6 and the random number generator software library RngLib version 2.0.2.

5 The precise reference of the Target of Evaluation (TOE) is given in *Section 1.4: TOE identification* and the security IC features are given in *Section 1.6: TOE description*.

6 A glossary of terms and abbreviations used in this document is given in *Appendix A: Glossary*.

Contents

List of tables

List of figures

1.3 Context

7 The Target of Evaluation (TOE) referred to in *Section 1.4: TOE identification*, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Connected Security Sub-group of STMicroelectronics (ST).

8 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL6 augmented by ALC_FLR.2 and ASE_TSS.2.

9 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE security ICs, and to summarise their chosen TSF services and assurance measures.

10 This ST claims to be an instantiation of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*" (PP) registered and certified under the reference *BSI-CC-PP-0084-2014* in the German IT Security Evaluation and Certification Scheme, ***with the following augmentations***:

- Addition #1: "Support of Cipher Schemes" from *AUG*
- Addition #4: "Area based Memory Access Control" from *AUG*
- Additions specific to this Security Target, some of which in compliance with *JIL-Post-Deliv-Load* and *ANSSI-CC-CER/F/06.002*.

The original text of this PP is typeset as indicated here, its augmentations from *AUG* as indicated here, and text originating in *JIL-Post-Deliv-Load* and *ANSSI-CC-CER/F/06.002* as indicated here, when they are reproduced in this document.

This ST instantiates the following packages from the above mentioned PP:

- Authentication of the Security IC
- Loader dedicated for usage in secured environment only
- Loader dedicated for usage by authorized users only.

11 Extensions introduced in this ST to the SFRs of the Protection Profile (PP) are exclusively drawn from the Common Criteria part 2 standard SFRs.

12 This ST makes various refinements to the above mentioned PP and *AUG*. They are all properly identified in the text typeset as ***indicated here*** or ~~here~~. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: ***BSI*** for *BSI-CC-PP-0084-2014*, ***AUG1*** for Addition #1 of *AUG*, ***AUG4*** for Addition #4 of *AUG*., and ***JIL*** for *JIL-Post-Deliv-Load* and *ANSSI-CC-CER/F/06.002*.

1.4 TOE identification

13 The Target of Evaluation (TOE) is the ST31R480 B01 platform.

14 "ST31R480 B01" completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 15: Guidance documentation*, and its development and production sites indicated in *Table 16: Sites list*.

15 B01 is the version of the evaluated platform. Any change in the TOE components, the guidance documentation and the list of sites leads to a new version of the evaluated platform, thus a new TOE.

Table 1. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	RngLib version
K4H0A	B	0x0299	3.0.6	2.0.2

1. Part of the product information.

16 The IC maskset name is the product hardware identification.
The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST software.

17 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: TOE components*, and the configuration elements as detailed in the Data Sheet, referenced in *Table 15: Guidance documentation*.

1.5 TOE overview

18 Designed for secure ID and banking applications, the TOE is a serial access microcontrollers that incorporate the most recent generation of Arm®[a] processors for embedded secure systems. Its SecurCore® SC000™ 32-bit RISC core is built on the Cortex® M0 core with additional security features to help to protect against advanced forms of attacks.

19 Different derivative devices may be configured depending on the customer needs:

- either by ST during the manufacturing or packaging process,
- or by the customer during the packaging, or composite product integration, or personnalisation process.

20 They all share the same hardware design and the same maskset (denoted by the Master identification number). The Master identification number is unique for all product configurations.

21 The configuration of the derivative devices can impact the I/O mode, and the available NVM size, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
I/O mode	Contact only, Dual mode, Contactless only
NVM size	320 or 480 Kbytes

22 All combinations of different features values are possible and covered by this certification. All possible configurations can vary under a unique IC, and without impact on security.

23 The Master identification number is unique for all product configurations.
Each derivative device has a specific Child product identification number, also part of the product information, and specified in the Datasheet and in the Firmware User Manual, referenced in *Table 15*.

a. 1Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

24 The rest of this document applies to all possible configurations of the TOE, except when a restriction is mentioned. For easier reading, the restrictions are typeset as indicated here.

25 In a few words, the ST31R480 B01 offers a unique combination of high performances and very powerful features for high level security:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- Hardware 3-key Triple DES accelerator,
- Hardware AES accelerator,
- ISO/IEC 13239 CRC calculation block,
- NExt Step CRYPTography accelerator (NESCRYPT).
- Random number generator software library (RngLib) compliant to statistical test metrics *NIST SP800-90B*, *NIST SP800-22* and *BSI-AIS20/AIS31* and online and total failure tests of *NIST SP800-90B* and *BSI-AIS20/AIS31*.

1.6 TOE description

1.6.1 TOE hardware description

26 The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks.

27 The AES (Advanced Encryption Standard *[3]*) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in Electronic CodeBook (ECB) or Cipher Block Chaining (CBC) modes.

28 The 3-key triple DES accelerator (EDES+) supports efficiently the Triple Data Encryption Standard (TDES *[2]*), enabling Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes and DES computation.
Note that a triple DES can be performed by a triple DES computation or by 3 single DES computations.

29 The NESCRYPT Fast coprocessor allows fast and secure implementation of the most popular public key cryptography algorithms with a high level of performance (*[4]*, *[6]*, *[8]*,*[9]*, *[10]*, *[11]*).

30 The TOE offers 12 Kbytes of User RAM and up to 480 Kbytes of secure User high-density Flash memory (NVM).The SC000 Memory Protection Unit (MPU) provides support for the definition of up to 16 different memory regions, enabling the user to define its own region organization with specific protection and access permissions. A Library Protection Unit (LPU) is available to isolate protected code (e.g. a library) from the rest of the code embedded in the device. The LPU may be reserved to ST, when a ST library requires its protection.

31 As randomness is a key stone in many applications, the ST31R480 B01 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 *[1]* and directly accessible through dedicated registers.

32 Three general-purpose timers are available as well as a watchdog timer.

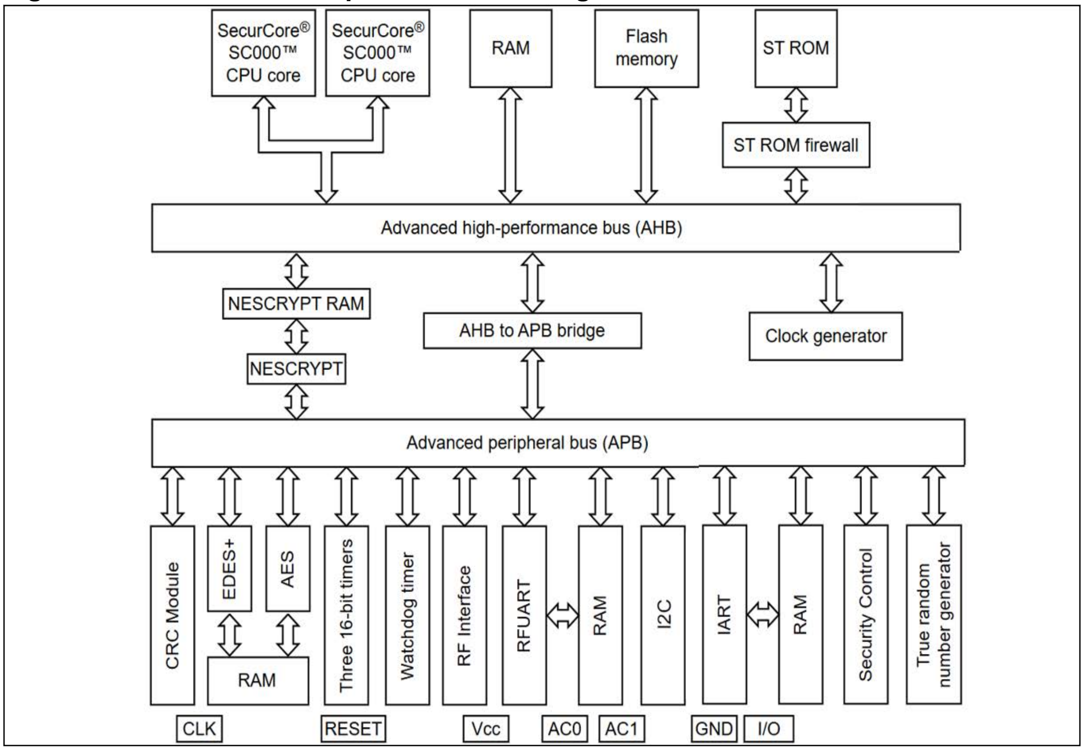
33 The TOE offers a contact serial communication interface fully compatible with the ISO/IEC 7816-3 standards, and a contactless interface including an RF Universal Asynchronous Receiver Transmitter (RF UART), enabling communication up to 848 kbps compatible with the ISO/IEC 14443 Type A and EMVCo™ standards.
These interfaces can be used simultaneously (dual mode), or the contact interface can be deactivated (see *Table 2: Derivative devices configuration possibilities*).

34 The TOE also provides an ISO/IEC13239 CRC calculation block which is **out of scope of this evaluation**.

35 The detailed features of this TOE are described in the Data Sheet and in the Cortex SC000 Technical Reference Manual, referenced in *Table 15*.

36 *Figure 1* provides an overview of the ST31R480 B01 platform.

Figure 1. ST31R480 B01 platform block diagram



1.6.2 TOE software description

37 The OST ROM contains a Dedicated Software which provides full test capabilities (operating system for test, called "OST"), not accessible by the Security IC Embedded Software (ES), after TOE delivery.

38 The System ROM and ST NVM of the TOE contain a Dedicated Software (Firmware) which provides:

- a Secure Flash Loader, enabling to securely and efficiently download the Security IC Embedded Software (ES) into the NVM. It also allows the evaluator to load software into the TOE for test purpose. The Secure Flash Loader is available in Admin configuration. The customer can choose to activate it in any phase of the product life-cycle under highly secured conditions, or to deactivate it definitely at a certain step.

- low-level functions called Flash Drivers, enabling the Security IC Embedded Software (ES) to modify and manage the NVM contents. The Flash Drivers are available in User configuration.
- a very reduced set of uncritical commands for basic diagnostic purpose (field return analysis), only reserved to STMicroelectronics.
- a set of highly protected commands for secure diagnostic purpose (advanced quality investigations), that can only be activated by the customer and be operated by STMicroelectronics on its own audited sites. This feature is protected by specific strong access control, completed by environmental measures which prevent access to customer assets. Furthermore, it can be permanently deactivated by the customer.

39 The TOE comprises a software library, located in User NVM, dedicated to random number generation (RngLib). The RngLib provides high-level routines that offer support for random number generation following recommendations from *NIST SP800-90B*, *NIST SP800-22* and *BSI-AIS20/AIS31* and associated evaluation. These are divided in the following categories:

- Library identification
- Service to get statistically tested random bits
- Retry mechanism
- Service to get raw bits from the noise source (reserved to certification purposes)
- Constants, macros, and types that facilitate the use of the library.

40 RngLib is embedded by the ES developer in his applicative code.

41 The Security IC Embedded Software (ES) is in User NVM.
Note: The ES is not part of the TOE and is out of scope of the evaluation.

1.6.3 TOE documentation

42 The user guidance documentation, part of the TOE, consists of:

- the *Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of flash memory - ST31R platform ST31R480 ST31R320 Datasheet - Preliminary document.*,
- the *ARM® SC000 Technical Reference Manual*,
- the *ARMv6-M Architecture Reference Manual*,
- the *ST31R platform firmware V3 - User manual*,
- the *Security guidance of the ST31R secure MCU platform - Application note*,
- the *Random number generation for ST31R - User manual*,
- the *Random number generator library RngLib 2.0.x - User manual*,
- the *RngLib 2.0.2 for ST31R platform - Release note*.

43 The complete list of guidance documents is detailed in *Table 15*.

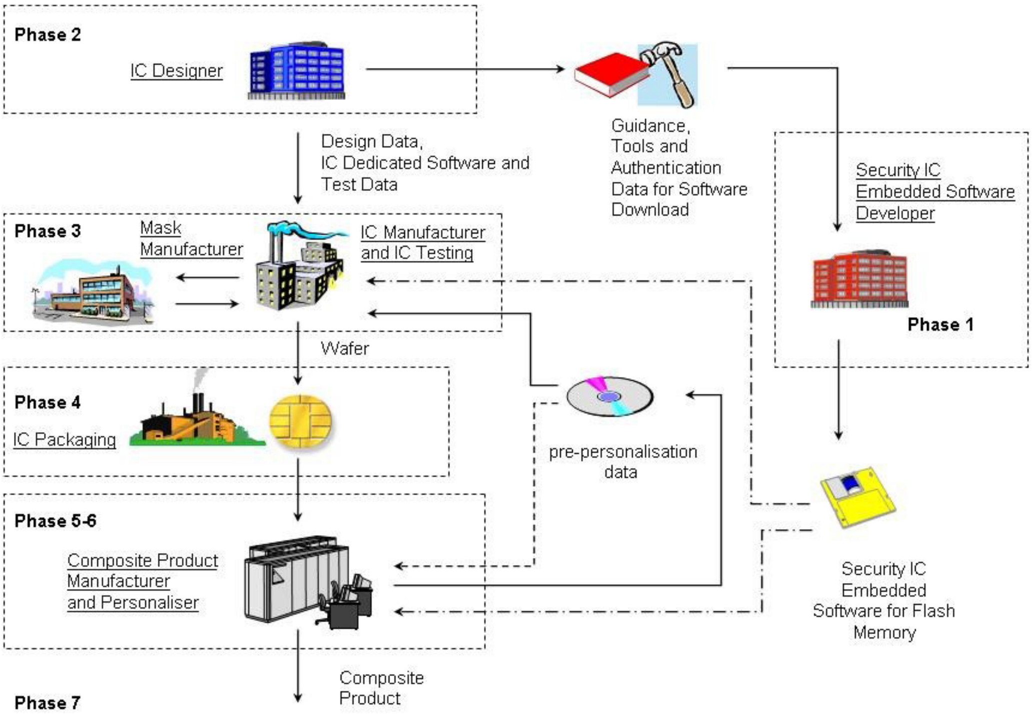
1.7 TOE life cycle

44 This Security Target is fully conform to the claimed PP. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer

to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 1.2.3.

45 The composite product life cycle is decomposed into 7 phases. Each of these phases has the very same boundaries as those defined in the claimed Protection Profile.

Figure 2. Security IC Life-Cycle if Security IC Embedded Software is loaded by Security IC Dedicated Software into the programmable non-volatile Memory



46 The life cycle phases are summarized in *Table 3*.

47 The sites potentially involved in the TOE life cycle are listed in *Table 16*.

48 The limit of the evaluation corresponds to phases 1, 2, 3 and optionally 4, including the delivery and verification procedures of phase 1, and the TOE delivery either to the IC packaging manufacturer or to the composite product integrator; procedures corresponding to phases 5, 6 and 7 are outside the scope of this evaluation.

49 In the following, the term "Composite product manufacturing" is uniquely used to indicate phases 1, optionally 4, 5 and 6 all together.
This ST also uses the term "Composite product manufacturer" which includes all roles responsible of the TOE during phases 1, optionally 4, 5 and 6.

50 The TOE, except the RngLib, is delivered after Phase 3 in form of wafers or after Phase 4 in packaged form, depending on the customer's order.

51 The RngLib is delivered as part of Phase 1, as a software package part of the dedicated support software, downloaded by ST entitled employees, from a controlled centralized system, then sent encrypted to the customer. The RngLib is intended to be used in support to the development of secure embedded software in phase 1. So the ES developers embeds it and links it to his applicative code.

52 In the following, the term "TOE delivery" is uniquely used to indicate:

- after phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products,
- the RngLib part of the TOE is specifically delivered as part of phase 1 in form of a ciphered and signed binary file, so that the ES developer embeds it and links it to his applicative code.

53 The TOE is delivered in Admin (aka Issuer) or User configuration.

Table 3. Composite product life cycle phases

Phase	Name	Description
1	Security IC embedded software development	security IC embedded software development specification of IC pre-personalization requirements
2	IC development	IC design IC dedicated software development
3	IC manufacturing and testing	integration and photomask fabrication IC manufacturing IC testing IC pre-personalisation
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary
5	Security IC product finishing process	composite product finishing process composite product testing
6	Security IC personalisation	composite product personalisation composite product testing
7	Security IC end usage	composite product usage by its issuers and consumers

1.8 TOE environment

54 Considering the TOE, three types of environments are defined:

- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3 and optionally 4,
- Operational environment, including phase 1 and from phase 4 or 5 to phase 7.

1.8.1 TOE Development Environment (Phase 2)

55 To ensure security, the environment in which the development takes place is secured with controllable accesses having traceability. Furthermore, all authorised personnel involved

fully understand the importance and the strict implementation of defined security procedures.

56 The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

57 Design and development of the IC then follows, together with the dedicated and engineering software and tools development. The engineers use secure computer systems (preventing unauthorised access) to make their developments, simulations, verifications and generation of the TOE's databases. Sensitive documents, files and tools, databases on tapes, and printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

58 The development centres possibly involved in the development of the TOE are denoted by the activity “DEV” or “ES_DEV” in *Table 16*.

1.8.2 TOE production environment

59 As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all product at all stages of production.

Phase 3

60 Reticules and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. As reticules and photomasks are generated off-site, they are transported and worked on in a secure environment. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

61 The authorized sub-contractors potentially involved in the TOE mask manufacturing are denoted by the activity “MASK” in *Table 16*.

62 Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and pre-personalization of each TOE occurs to assure conformance with the device specification and to load the customer information.

63 The authorized front-end plant possibly involved in the manufacturing of the TOE are denoted by the activity “FE” in *Table 16*.

64 The authorized EWS plant potentially involved in the testing of the TOE are denoted by the activity “EWS” in *Table 16*.

65 Wafers are then scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner.

Phase 4

66 The good ICs are then packaged in phase 4, in a back-end plant. When testing, programming or deliveries are done offsite, ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

67 When the product is delivered after phase 4, the authorized back-end plants possibly involved in the packaging of the TOE are denoted by the activity “BE” in *Table 16*.

68 All sites denoted by the activity “WHS” or “WHSD” in *Table 16* can be involved for the logistics during phase 3 or 4.

1.8.3 TOE operational environment

69 A TOE operational environment is the environment of phases 1, optionally 4, then 5 to 7.

70 At phases 1, 4, 5 and 6, the TOE operational environment is a controlled environment.

71 End-user environments (phase 7): composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are pay-TV, banking cards, brand protection, portable communication SIM cards, health cards, transportation cards, access management, identity and passport cards. The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

2 Conformance claims (ASE_CCL, ASE_ECD)

2.1 Common Criteria conformance claims

72 The ST31R480 B01 platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

73 Furthermore it claims to be CC Part 2 (*CCMB-2017-04-002 R5*) extended and CC Part 3 (*CCMB-2017-04-003 R5*) conformant.

74 The extended Security Functional Requirements are those defined in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*):

- **FCS_RNG** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage,
- **FDP_SDC** Stored data confidentiality,
- **FIA_API** Authentication proof of identity.

The reader can find their certified definitions in the text of the "*BSI-CC-PP-0084-2014*" Protection Profile.

75 The assurance level for the ST31R480 B01 platform Security Target is ***EAL6*** augmented by ALC_FLR.2 and ASE_TSS.2.

2.2 PP Claims

2.2.1 PP Reference

76 The ST31R480 B01 platform Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

77 The following packages have been selected from the *BSI-CC-PP-0084-2014*:

- Package “Authentication of the Security IC”,
- Packages for Loader:
  – Package 1: Loader dedicated for usage in Secured Environment only,
  – Package 2: Loader dedicated for usage by authorized users only.

2.2.2 PP Additions

78 The main additions operated on the *BSI-CC-PP-0084-2014* are:

- Addition #4: “Area based Memory Access Control” from *AUG*,
- Addition #1: “Support of Cipher Schemes” from *AUG*,
- Specific additions for the Secure Flash Loader, to comply with *JIL-Post-Deliv-Load* and *ANSSI-CC-CER/F/06.002*,
- Specific additions for the Secure Diagnostic capability,
- Refinement of assurance requirements.

79 All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-CC-PP-0084-2014* being typeset as indicated here and ~~here~~. Text originating in *AUG* is typeset as indicated here. Text originating in *JIL-Post-Deliv-Load* and *ANSSI-CC-CER/F/06.002* is typeset as indicated here.

80 The security environment additions relative to the PP are summarized in *Table 4*.

81 The additional security objectives relative to the PP are summarized in *Table 5*.

82 A simplified presentation of the TOE Security Policy (TSP) is added.

83 The additional SFRs for the TOE relative to the PP are summarized in *Table 7*.

84 The additional SARs relative to the PP are summarized in *Table 9*.

2.2.3 PP Claims rationale

85 The differences between this Security Target security objectives and requirements and those of *BSI-CC-PP-0084-2014*, to which conformance is claimed, have been identified and justified in *Section 4* and in *Section 5*. They have been recalled in the previous section.

86 In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the *BSI-CC-PP-0084-2014*.

87 The security problem definition presented in *Section 3*, clearly shows the additions to the security problem statement of the PP.

88 The security objectives rationale presented in *Section 4.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-CC-PP-0084-2014*.

89 Similarly, the security requirements rationale presented in *Section 5.4* has been updated with respect to the Protection Profile.

90 All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness have been argued in the rationale sections of the present document.

3 Security problem definition (ASE_SPD)

91 This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assets to be protected, the threats, the organisational security policies and the assumptions.

92 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3. Only those originating in *AUG* or in *JIL-Post-Deliv-Load* / *ANSSI-CC-CER/F/06.002*, and the ones introduced in this Security Target, are detailed in the following sections.

93 A summary of all these security aspects and their respective conditions is provided in *Table 4*.

Table 4. Summary of security aspects

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
	BSI.T.Masquerade-TOE	Masquerade the TOE
	AUG4.T.Mem-Access	Memory Access Violation
	JIL.T.Open-Samples-Diffusion	Diffusion of open samples
	T.Confid-Applic-Code	Specific application code confidentiality
	T.Confid-Applic-Data	Specific application data confidentiality
	T.Integ-Applic-Code	Specific application code integrity
	T.Integ-Applic-Data	Specific application data integrity
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
	BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Resp-Appl	Treatment of User Data

3.1 Description of assets

94 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), the assets defined in section 3.1 of the Protection Profile are applied and the assets regarding threats are clarified in this Security Target.

95 The assets (related to standard functionality) to be protected are

- - the user data of the Composite TOE,
- - the Security IC Embedded Software, stored and in operation,
- - the security services provided by the TOE for the Security IC Embedded Software.

96 The user (consumer) of the TOE places value upon the assets related to high-level security concerns:

SC1 integrity of user data of the Composite TOE,

SC2 confidentiality of user data of the Composite TOE being stored in the TOE's protected memory areas,

SC3 correct operation of the security services provided by the TOE for the Security IC Embedded Software.

Note the Security IC Embedded Software is user data and shall be protected while being executed/processed and while being stored in the TOE's protected memories.

97 The Security IC may not distinguish between user data which is public knowledge or kept confidential. Therefore the security IC shall protect the user data of the Composite TOE in integrity and in confidentiality if stored in protected memory areas, unless the Security IC Embedded Software chooses to disclose or modify it.

98 In particular integrity of the Security IC Embedded Software means that it is correctly being executed which includes the correct operation of the TOE's functionality. Parts of the Security IC Embedded Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Security IC Embedded Software may need to be kept confidential since specific implementation details may assist an attacker.

99 Th***e*** Protection Profile requires the TOE to provide at least one security service: the generation of random numbers by means of a physical Random Number Generator. The annex 7 provides packages for typical additional security services. The Security Target may require additional security services as described in these packages or define TOE specific security services. It is essential that the TOE ensures the correct operation of all security services provided by the TOE for the Security IC Embedded Software.

100 According to th***e*** Protection Profile there is the following high-level security concern related to security service:

SC4 deficiency of random numbers.

101 To be able to protect these assets (SC1 to SC4) the TOE shall self-protect its TSF. Critical information about the TSF shall be protected by the development environment and the operational environment. Critical information may include:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks.

102 Such information and the ability to perform manipulations assist in threatening the above assets.

103 Note that there are many ways to manipulate or disclose the user data of the Composite TOE: (i) An attacker may manipulate the Security IC Embedded Software or the TOE. (ii) An attacker may cause malfunctions of the TOE or abuse Test Features provided by the TOE. Such attacks usually require design information of the TOE to be obtained. They pertain to all information about (i) the circuitry of the IC (hardware including the physical memories), (ii) the IC Dedicated Software with the parts IC Dedicated Test Software (if any) and IC Dedicated Support Software (if any), and (iii) the configuration data for the TSF. The knowledge of this information may enable or support attacks on the assets. Therefore the TOE Manufacturer must ensure that the development and production of the TOE (refer to Section 1.2.3) is secure so that no restricted, sensitive, critical or very critical information is unintentionally made available for attacks in the operational phase of the TOE (~~cf. [8] for details on assessment of knowledge of the TOE in the vulnerability analysis~~).

104 ***ST*** must apply protection to support the security of the TOE. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Security IC Embedded Software. This covers the Security IC Embedded Software itself if provided by the developer of the Security IC Embedded Software or any authentication data required to enable the download of software. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer. These aspects enforce the usage of the supporting documents and the refinements of SAR defined in th***e*** Protection Profile.

105 The information and material produced and/or processed by ***ST*** in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Initialisation Data and Pre-personalisation Data,
- Security IC Embedded Software, provided by the Security IC Embedded Software developer and implemented by the IC manufacturer,
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photomasks and products in any form

as long as they are generated, stored, or processed by ***ST***.

106 Application note:
The TOE providing a functionality for Security IC Embedded Software secure loading into NVM, the ES is considered as User Data being stored in the TOE’s memories at this step, and the Protection Profile corresponding packages are integrated, as well as the requirements from *JIL-Post-Deliv-Load*.

3.2 Threats

107 The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.
Only those originating in *AUG* and *ANSSI-CC-CER/F/06.002* are detailed in the following section.

BSI.T.Leak-Inherent	Inherent Information Leakage
BSI.T.Phys-Probing	Physical Probing
BSI.T.Malfunction	Malfunction due to Environmental Stress
BSI.T.Phys-Manipulation	Physical Manipulation
BSI.T.Leak-Forced	Forced Information Leakage
BSI.T.Abuse-Func	Abuse of Functionality
BSI.T.RND	Deficiency of Random Numbers
BSI.T.Masquerade-TOE	Masquerade the TOE
AUG4.T.Mem-Access	Memory Access Violation: Parts of the ***Security IC*** Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the ***Security IC*** Embedded Software. Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access. Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.
JIL.T.Open-Samples-Diffusion	Diffusion of open samples: An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code, …). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography, …). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC.

T.Confid-Applic-Code	Specific application code confidentiality: A specific application code may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the specific application executable code is stored. The attacker executes another application to disclose code belonging to the specific application.
T.Confid-Applic-Data	Specific application data confidentiality: A specific application data may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the specific application by another application. For example, the attacker executes an application that tries to read data belonging to the specific application.
T.Integ-Applic-Code	Specific application code integrity: A specific application code may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to memory area where the specific application executable code is stored and executed. The attacker executes another application that tries to alter (part of) the specific application code.
T.Integ-Applic-Data	Specific application data integrity: A specific application product data may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the specific application data by another application. The attacker executes an application that tries to alter (part of) the specific application data.

3.3 Organisational security policies

108 The TOE provides specific security functionality that can be used by the ***Security IC*** Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the ***Security IC*** application, against which threats the ***Security IC*** Embedded Software will use the specific security functionality.

109 ST applies the Protection policy during TOE Development and Production (*BSI.P.Process-TOE*) as specified below.

110 *BSI.P.Lim-Block-Loader* and *BSI.P.Ctrl-Loader* are dedicated to the Secure Flash Loader, and described in the *BSI-CC-PP-0084-2014* packages "Loader dedicated for usage in secured environment only" and "Loader dedicated for usage by authorized users only". *BSI.P.Ctrl-Loader* has been completed in accordance with *JIL-Post-Deliv-Load*.

111 ***ST*** applies the Additional Specific Security Functionality policy (*AUG1.P.Add-Functions*) as specified below.

BSI.P.Process-TOE Identification during TOE Development and Production:

An accurate identification ***is*** established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

BSI.P.Lim-Block-Loader Limiting and blocking the loader functionality:

The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader(1) in order to protect stored data from disclosure and manipulation.

1. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.

BSI.P.Ctrl-Loader Controlled usage to Loader Functionality:

Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation.

The activation of the loaded Additional ~~Code~~ ***user data*** is possible if:

– integrity and authenticity of the Additional ~~Code~~ ***user data*** have been successfully checked;

– the loaded ~~Additional Code~~ ***user data*** is targeted to the Initial TOE (Identification ~~Data~~ of the Additional ~~Code~~ ***user data*** and the Initial TOE will be used for this check).

Identification ~~Data~~ of the resulting Final TOE shall identify the Initial TOE and the ~~activated~~ Additional ~~Code~~ ***user data***. Identification Data shall be protected in integrity.

Note: Here, the term TOE denotes the TOE itself as well as the composite TOE which both may be maintained by loading of data.

AUG1.P.Add-Functions Additional Specific Security Functionality:

The TOE shall provide the following specific security functionality to the Security IC Embedded Software:

– Triple Data Encryption Standard (TDES),

– Advanced Encryption Standard (AES).

3.4 Assumptions

112 The following assumptions are described in the *BSI-CC-PP-0084-2014*, section 3.4.

BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
BSI.A.Resp-Appl	Treatment of User Data of the Composite TOE

4 Security objectives (ASE_OBJ)

113 The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation during development and production phases,
- provide random numbers,
- provide cryptographic support and access control functionality.

114 A summary of all security objectives is provided in *Table 5*.

115 Note that the origin of each objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *BSI-CC-PP-0084-2014*, sections 4.1 and 7.3. Only those which have been amended, those originating in *AUG*, those originating in *JIL-Post-Deliv-Load*, and the ones introduced in this Security Target, are detailed in the following sections.

Table 5. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
	BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader
	JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF
	JIL.O.Secure-Load-ACode	Secure loading of the Additional Code
	JIL.O.Secure-AC-Activation	Secure activation of the Additional Code
	JIL.O.TOE-Identification	Secure identification of the TOE
	O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image
	O.MemImage-Identification	Secure identification of the Memory Image
	BSI.O.Authentication	Authentication to external entities
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
	O.Firewall	Specific application firewall

Table 5. Summary of security objectives (continued)

	Label	Title
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader
	BSI.OE.Loader-Usage	Secure communication and usage of the Loader
	BSI.OE.TOE-Auth	External entities authenticating of the TOE
	OE.Composite-TOE-Id	Composite TOE identification
	OE.TOE-Id	TOE identification
	OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic
	OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic

4.1 Security objectives for the TOE

BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
BSI.O.Phys-Probing	Protection against Physical Probing
BSI.O.Malfunction	Protection against Malfunctions
BSI.O.Phys-Manipulation	Protection against Physical Manipulation
BSI.O.Leak-Forced	Protection against Forced Information Leakage
BSI.O.Abuse-Func	Protection against Abuse of Functionality
BSI.O.Identification	TOE Identification
BSI.O.RND	Random Numbers
BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader
BSI.O.Authentication	Authentication to external entities
JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF:

The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit, …) through the use of a dedicated code loaded on open samples.

JIL.O.Secure-Load-ACode	Secure loading of the Additional Code: The Loader of the ~~Initial~~ TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure. Note: Concretely, the TOE manages the Additional Code as a Memory Image.
JIL.O.Secure-AC-Activation	Secure activation of the Additional Code: Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.
JIL.O.TOE-Identification	Secure identification of the TOE: The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional TOE. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.
O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image: The Loader of the TOE shall check an evidence of authenticity and integrity of the loaded Memory Image. The Loader enforces that only the allowed version of the Additional Memory Image can be loaded after the Initial Memory Image. The Loader shall forbid the loading of an Additional Memory Image not intended to be assembled with the Initial Memory Image. Note: This objective is similar to JIL.O.Secure-Load-ACode, applied to user data (e.g. embedded software).

O.MemImage-Identification	Secure identification of the Memory Image: The Identification Data identifies the Initial Memory Image and Additional Memory Image. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. Storage of the Additional Memory Image and update of the Identification Data shall be performed at the same time in an Atomic way, otherwise (in case of interruption or incident which prevents this alignment), the Memory Image shall remain in its initial state or the TOE shall fail secure. The Identification Data of the Final Memory Image allows identifications of Initial Memory Image and Additional Memory Image. Note: This objective is similar to JIL.O.Secure-AC-Activation and JIL.O.TOE-Identification, applied to user data (e.g. embedded software).
AUG1.O.Add-Functions	Additional Specific Security Functionality: The TOE must provide the following specific security functionality to the ***Security IC*** Embedded Software: – Triple Data Encryption Standard (TDES), – Advanced Encryption Standard (AES).
AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control: The TOE must provide the ***Security IC*** Embedded Software with the capability to define ***dynamic memory segmentation and protection***. The TOE must then enforce ***the defined access rules*** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.
O.Firewall	Specific application firewall: The TOE shall ensure isolation of data and code between a specific application and the other applications. An application shall not read, write, compare any piece of data or code belonging to the specific application.

4.2 Security objectives for the environment

116 Security Objectives for the Security IC Embedded Software development environment (phase 1):

BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE

117 Clarification related to “Treatment of User Data of the Composite TOE (*BSI.OE.Resp-Appl*)”: By definition cipher or plain text data and cryptographic keys are User Data. The Security IC Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation. This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

118 Security Objectives for the operational Environment (phase 4 up to 7):

BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	Up to phase 6
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader: The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and, ***if desired,*** terminate irreversibly the Loader after intended usage of the Loader. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.	Up to phase 6
BSI.OE.Loader-Usage	Secure communication and usage of the Loader: The authorized user must support the trusted communication channel with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader. The authorized user must organize the maintenance transactions to ensure that the additional code (loaded as data) is able to operate as in the Final composite TOE. The authorized user must manage and associate unique Identification to the loaded data.	Up to phase 7
BSI.OE.TOE-Auth	External entities authenticating of the TOE The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.	Up to phase 7

OE.Composite-TOE-Id	Composite TOE identification: The composite manufacturer must maintain a unique identification of a composite TOE under maintenance.	Up to phase 7
OE.TOE-Id	TOE identification: The IC manufacturer must maintain a unique identification of the TOE under maintenance.	Up to phase 7
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic: If desired, the Composite Product Manufacturer will enable (or disable) irreversibly the Secure Diagnostic capability, thus enabling the IC manufacturer (or disabling everyone) to exercise the Secure Diagnostic capability.	Up to phase 7
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic: The IC manufacturer must support the trusted communication channel with the TOE by fulfilling the access conditions required by the Secure Diagnostic. The IC manufacturer must manage the Secure Diagnostic transactions so that they cannot be used to disclose critical user data of the Composite TOE, manipulate critical user data of the Composite TOE, manipulate Security IC Embedded Software or bypass, deactivate, change or explore security features or security services of the TOE	Up to phase 7

4.3 Security objectives rationale

119 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* Protection Profile, together with those in *AUG*, and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 3* are addressed by the security objectives stated in this chapter.

120 Thus, it is necessary to show that:

- security environment aspects from *AUG* and from this ST, are addressed by security objectives stated in this chapter,
- security objectives from *AUG* and from this ST, are suitable (i.e. they address security environment aspects),
- security objectives from *AUG* and from this ST, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).

121 The selected augmentations from *AUG* introduce the following security environment aspects:

- TOE threat "Memory Access Violation, (*AUG4.T.Mem-Access*)",
- organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)".

122 The augmentation made in this ST introduces the following security environment aspect:

- TOE threats "Diffusion of open samples, (*JIL.T.Open-Samples-Diffusion*)", "Specific application code confidentiality, (*T.Confid-Applic-Code*)", " Specific application data confidentiality, (*T.Confid-Applic-Data*)", " Specific application code integrity, (*T.Integ-Applic-Code*)", "Specific application data integrity, (*T.Integ-Applic-Data*)".

123 The justification of the additional policies, additional threats, provided in the next subsections shows that they do not contradict to the rationale already given in the Protection Profile *BSI-CC-PP-0084-2014* for the assumptions, policies and threats defined there.

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	
BSI.P.Ctrl-Loader	*BSI.O.Ctrl-Auth-Loader* *JIL.O.Secure-Load-ACode* *JIL.O.Secure-AC-Activation* *JIL.O.TOE-Identification* *O.Secure-Load-AMemImage* *O.MemImage-Identification* *BSI.OE.Loader-Usage* *OE.TOE-Id* *OE.Composite-TOE-Id*	
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	

Table 6. Security Objectives versus Assumptions, Threats or Policies (continued)

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.T.Abuse-Func	*BSI.O.Abuse-Func* *OE.Enable-Disable-Secure-Diag* *OE.Secure-Diag-Usage*	
BSI.T.RND	*BSI.O.RND*	
BSI.T.Masquerade-TOE	*BSI.O.Authentication* *BSI.OE.TOE-Auth*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
JIL.T.Open-Samples-Diffusion	*JIL.O.Prot-TSF-Confidentiality* *BSI.O.Leak-Inherent* *BSI.O.Leak-Forced*	
T.Confid-Applic-Code	*O.Firewall*	
T.Confid-Applic-Data	*O.Firewall*	
T.Integ-Applic-Code	*O.Firewall*	
T.Integ-Applic-Data	*O.Firewall*	

4.3.1 TOE threat "Abuse of Functionality"

124 The justification related to the threat “Abuse of Functionality, (*BSI.T.Abuse-Func*)” is as follows:

125 The threat *BSI.T.Abuse-Func* is directly covered by the security objective *BSI.O.Abuse-Func*, supported by the security objectives for the operational environment *OE.Enable-Disable-Secure-Diag and OE.Secure-Diag-Usage* for the particular case of the Secure Diagnostic. Therefore *BSI.T.Abuse-Func* is covered by these three objectives.

4.3.2 TOE threat "Memory Access Violation"

126 The justification related to the threat “Memory Access Violation, (*AUG4.T.Mem-Access*)” is as follows:

127 According to *AUG4.O.Mem-Access* the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the ***Security IC*** Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to *AUG4.T.Mem-Access*). The threat *AUG4.T.Mem-Access* is therefore removed if the objective is met.

128 The added objective for the TOE *AUG4.O.Mem-Access* does not introduce any contradiction in the security objectives for the TOE.

4.3.3 TOE threat "Diffusion of open samples"

129 The justification related to the threat “Diffusion of open samples, (*JIL.T.Open-Samples-Diffusion*)” is as follows:

130 According to threat *JIL.T.Open-Samples-Diffusion*, the TOE shall provide protection against attacks using open samples of the TOE to characterize the behavior of the IC and its security functionalities. The objective *JIL.O.Prot-TSF-Confidentiality* requires protection against disclosure of confidential operations of the Security IC through the use of a dedicated code loaded on open samples. Additionally, *BSI.O.Leak-Inherent* and *BSI.O.Leak-Forced* ensures protection against disclosure of confidential data processed in the Security IC. Therefore *JIL.T.Open-Samples-Diffusion* is covered by these three objectives.

131 The added objective for the TOE *JIL.O.Prot-TSF-Confidentiality* does not introduce any contradiction in the security objectives for the TOE.

4.3.4 TOE threat "Specific application code confidentiality"

132 The justification related to the threat “Specific application code confidentiality, (*T.Confid-Applic-Code*)” is as follows:

133 Since *O.Firewall* requires that the TOE ensures isolation of code between a specific application and the other applications, the code of the specific application is protected against unauthorised disclosure, therefore *T.Confid-Applic-Code* is covered by *O.Firewall*.

134 The added objective for the TOE *O.Firewall* does not introduce any contradiction in the security objectives for the TOE.

4.3.5 TOE threat "Specific application data confidentiality"

135 The justification related to the threat “Specific application data confidentiality, (*T.Confid-Applic-Data*)” is as follows:

136 Since *O.Firewall* requires that the TOE ensures isolation of data between a specific application and the other applications, the data of the specific application is protected against unauthorised disclosure, therefore *T.Confid-Applic-Data* is covered by *O.Firewall*.

4.3.6 TOE threat "Specific application code integrity"

137 The justification related to the threat “Specific application code integrity, (*T.Integ-Applic-Code*)” is as follows:

138 The threat is related to the alteration of a specific application code by an attacker. *O.Firewall* requires that the TOE ensures isolation of code between the specific application and the other applications, thus protecting the code of the specific application against unauthorised modification. Therefore the threat is covered by *O.Firewall*.

4.3.7 TOE threat "Specific application data integrity"

139 The justification related to the threat “Specific application data integrity, (*T.Integ-Applic-Data*)” is as follows:

140 The threat is related to the alteration of a specific application data by an attacker. Since *O.Firewall* requires that the TOE ensures complete isolation of data between the specific application and the other applications, the data of the specific application is protected against unauthorised modification, therefore *T.Integ-Applic-Data* is covered by *O.Firewall*.

4.3.8 Organisational security policy "Controlled usage to Loader Functionality"

141 The justification related to the organisational security policy "Controlled usage to Loader Functionality, (*BSI.P.Ctrl-Loader*)" is as follows:

142 As stated in *BSI-CC-PP-0084-2014*, the organisational security policy “Controlled usage to Loader Functionality (*BSI.P.Ctrl-Loader*) is implemented by the security objective for the TOE “Access control and authenticity for the Loader (*BSI.O.Ctrl-Auth-Loader*)” and the security objective for the TOE environment “Secure communication and usage of the Loader (*BSI.OE.Loader-Usage*)”.
The security objectives “Secure loading of the Additional Code (*JIL.O.Secure-Load-ACode*)”, “Secure activation of the Additional Code (*JIL.O.Secure-AC-Activation*)”, and ”Secure identification of the TOE (*JIL.O.TOE-Identification*)” specified by *JIL-Post-Deliv-Load* additionally enforce this policy since they require authenticity, atomicity, identification of the loaded additional code, part of the TOE. ”Secure identification of the TOE (*JIL.O.TOE-Identification*)” is supported by the security objective for the TOE environment “TOE identification (*OE.TOE-Id*)”.
Similarly, the security objectives “Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)”, and “Secure identification of the Memory Image (*O.MemImage-Identification*)”, enforce this policy since they require authenticity, atomicity, identification of the loaded additional memory image for the user data (embedded software). ”Secure identification of Memory Image (*O.MemImage-Identification*)” is supported by the security objective for the TOE environment “Composite TOE identification (*OE.Composite-TOE-Id*)”.
Therefore the policy is covered by these nine objectives.

4.3.9 Organisational security policy "Additional Specific Security Functionality"

143 The justification related to the organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)" is as follows:

144 Since *AUG1.O.Add-Functions* requires the TOE to implement exactly the same specific security functionality as required by *AUG1.P.Add-Functions*, ***and in the very same conditions,*** the organisational security policy is covered by the objective.

145 Nevertheless the security objectives *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, , *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation* and *BSI.O.Leak-Forced* define how to implement the specific security functionality required by *AUG1.P.Add-Functions*. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from *AUG1.P.Add-Functions*.) Especially *BSI.O.Leak-Inherent* and *BSI.O.Leak-Forced* refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by *AUG1.P.Add-Functions*.

146 The added objective for the TOE *AUG1.O.Add-Functions* does not introduce any contradiction in the security objectives for the TOE.

5 Security requirements (ASE_REQ)

147 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 5.1*), a section on security assurance requirements (SARs) for the TOE (*Section 5.2*), a section on the refinements of these SARs (*Section 5.3*) as required by the "*BSI-CC-PP-0084-2014*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 5.4*).

5.1 Security functional requirements for the TOE

148 Security Functional Requirements (SFRs) from the "*BSI-CC-PP-0084-2014*" Protection Profile (PP) are drawn from *CCMB-2017-04-002 R5*, except the following SFRs, that are **extensions** to *CCMB-2017-04-002 R5*:

- **FCS_RNG** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage,
- **FDP_SDC** Stored data confidentiality,
- **FIA_API** Authentication proof of identity .

The reader can find their certified definitions in the text of the "*BSI-CC-PP-0084-2014*" Protection Profile.

149 All extensions to the SFRs of the "*BSI-CC-PP-0084-2014*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2017-04-002 R5*.

150 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2017-04-001 R5*. They are easily identified in the following text as they appear ***as indicated here***. Note that in order to improve readability, iterations are sometimes expressed within tables.

151 In order to ease the definition and the understanding of these security functional requirements, a simplified presentation of the TOE Security Policy (TSP) is given in the following section.

152 The selected security functional requirements for the TOE, their respective origin and type are summarized in *Table 7*.

Table 7. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-CC-PP-0084-2014*	*CCMB-2017-04-002 R5*
FPT_FLS.1	Failure with preservation of secure state			

Table 7. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality	*BSI-CC-PP-0084-2014*	Extended
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-CC-PP-0084-2014* Operated	
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing		
FDP_SDI.2	Stored data integrity monitoring and action			*CCMB-2017-04-002 R5*
FPT_PHP.3	Resistance to physical attack		*BSI-CC-PP-0084-2014*	
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1 / PTG.2	Random number generation - PTG.2	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	Extended
FCS_RNG.1 / PG	Random number generation			
FCS_RNG.1 / RngLib	Random number generation - RngLib			
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	*CCMB-2017-04-002 R5*
FDP_ACC.2 / Memories	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1 / Memories	Security attribute based access control		*AUG* #4 Operated	
FMT_MSA.3 / Memories	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Memories	Management of security attribute			
FMT_SMF.1 / Memories	Specification of management functions		Security Target Operated	
FIA_API.1	Authentication Proof of Identity	Masquerade	*BSI-CC-PP-0084-2014* Operated	Extended

Table 7. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality	*BSI-CC-PP-0084-2014* Operated	Extended
FMT_LIM.2 / Loader	Limited availability			
FTP_ITC.1 / Loader	Inter-TSF trusted channel - Loader	Loader violation		*CCMB-2017-04-002 R5*
FDP_UCT.1 / Loader	Basic data exchange confidentiality - Loader			
FDP_UIT.1 / Loader	Data exchange integrity - Loader			
FDP_ACC.1 / Loader	Subset access control - Loader			
FDP_ACF.1 / Loader	Security attribute based access control - Loader			
FMT_MSA.3 / Loader	Static attribute initialisation - Loader	Correct Loader operation	Security Target Operated	
FMT_MSA.1 / Loader	Management of security attribute - Loader			
FMT_SMR.1 / Loader	Security roles - Loader			
FIA_UID.1 / Loader	Timing of identification - Loader			
FIA_UAU.1 / Loader	Timing of authentication - Loader			
FMT_SMF.1 / Loader	Specification of management functions - Loader			
FPT_FLS.1 / Loader	Failure with preservation of secure state - Loader			
FAU_SAR.1 / Loader	Audit review - Loader	Lack of TOE identification		
FAU_SAS.1 / Loader	Audit storage - Loader			Extended

Table 7. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FTP_ITC.1 / Sdiag	Inter-TSF trusted channel - Secure Diagnostic	Abuse of Secure Diagnostic functionality	Security Target Operated	CCMB-2017-04-002 R5
FAU_SAR.1 / Sdiag	Audit review - Secure Diagnostic			
FMT_LIM.1 / Sdiag	Limited capabilities - Secure Diagnostic			Extended
FMT_LIM.2 / Sdiag	Limited availability - Secure Diagnostic			

5.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

153 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: ***exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).***

Failure with preservation of secure state (FPT_FLS.1)

154 The TSF shall preserve a secure state when the following types of failures occur: ***exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.***

155 Refinements:

The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

Regarding application note 14 of BSI-CC-PP-0084-2014, the secure state is reached by an immediate interrupt or by a reset, depending on the current context.

Regarding application note 15 of BSI-CC-PP-0084-2014, the TOE provides information on the operating conditions monitored during Security IC Embedded Software execution and after a warm reset. No audit requirement is however selected in this Security Target.

Limited capabilities (FMT_LIM.1) / Test

156 The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: ***Limited capability and availability Policy / Test***.

Limited availability (FMT_LIM.2) / Test

157 The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1) / Test" the following policy is enforced: ***Limited capability and availability Policy / Test***.

158 <u>*SFP_1: Limited capability and availability Policy / Test*</u>

Deploying Test Features after TOE Delivery does not allow User Data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Audit storage (FAU_SAS.1)

159 The TSF shall provide ***the test process before TOE Delivery*** with the capability to store the ***Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software*** in the ***NVM***.

Stored data confidentiality (FDP_SDC.1)

160 The TSF shall ensure the confidentiality of the information of the user data while it is stored in ***all the memory areas where it can be stored***.

Stored data integrity monitoring and action (FDP_SDI.2)

161 The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity errors*** on all objects, based on the following attributes: ***user data stored in all possible memory areas, depending on the integrity control attributes***.

162 Upon detection of a data integrity error, the TSF shall ***signal the error and react***.

Resistance to physical attack (FPT_PHP.3)

163 The TSF shall resist ***physical manipulation and physical probing,*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.

164 Refinement:

The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i)assuming that there might be an attack at any time and (ii)countermeasures are provided at any time.

Basic internal transfer protection (FDP_ITT.1)

165 The TSF shall enforce the ***Data Processing Policy*** to prevent the ***disclosure*** of user data when it is transmitted between physically-separated parts of the TOE.

Basic internal TSF data transfer protection (FPT_ITT.1)

166 The TSF shall protect TSF data from ***disclosure*** when it is transmitted between separate parts of the TOE.

167 Refinement:

The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1 below.

Subset information flow control (FDP_IFC.1)

168 The TSF shall enforce the ***Data Processing Policy*** on ***all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software***.

169 *SFP_2: Data Processing Policy*

User Data of the Composite TOE and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

Random number generation - PTG.2 (FCS_RNG.1 / PTG.2)

170 The TSF shall provide a ***physical*** random number generator that implements:

- ***(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.***
- ***(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.***
- ***(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.***
- ***(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.***
- ***(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.***

171 The TSF shall provide ***numbers of 32 bits words*** that meet

- ***(PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.***
- ***(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.***

Random number generation - PG (FCS_RNG.1 / PG)

172 The TSF shall provide a ***physical*** random number generator that implements:

- ***(PG.1) The rule RègleArchiGVA of*** ANSSI-PG-083 ***and the recommendation RecommandationArchiGVA of*** ANSSI-PG-083.
- ***(PG.2) Total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.***
- ***(PG.3) Online tests detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.***
-

173 The TSF shall provide ***numbers of 32-bit words*** that meet

- ***(PG.4) The rule RègleArchiGVA of*** *ANSSI-PG-083*
- ***(PG.5) Generated random numbers shall pass AIS31 statistical procedure tests (Test procedure A).***

174 Application note
The composite developer must implement a cryptographic post processing to comply with *ANSSI-PG-083* RègleArchiGDA and *SOG-IS ACM* note 49.

Random number generation - RngLib (FCS_RNG.1 / RngLib)

175 The TSF shall provide a ***physical*** random number generator that implements:

- ***(RngLib.1) The RngLib provides random numbers using the class PTG.2 from FCS_RNG.1 / PTG.2 as random source.***
- ***(RngLib.2) The RngLib provides random numbers from FCS_RNG.1 / PG as random source.***
- ***(RngLib.3) An online test compliant to*** *NIST SP800-90B* ***which detects non-tolerable statistical defects of 1024-bit raw random number sequence generated by the RNG, when it has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.***
- ***(RngLib.4) An online test compliant to*** *BSI-AIS20/AIS31* ***- PTG.2 class which detect non-tolerable statistical defects of 128-bit or 1024-bit raw random number sequence generated by the RNG, when it has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.***

176 The TSF shall provide random numbers that meets:

- ***(RngLib.5) Statistical tests suites from*** *NIST SP800-22* and or *NIST SP800-90B* and or *BSI-AIS20/AIS31*.

  Applicative note:
  The total failure test is a hardware mechanism which raises a flag that is later checked by the RngLib.
  The RngLib user can select as source for the random numbers to be tested either the FCS_RNG.1 / PTG.2 or the FCS_RNG.1 / PG security function.
  The RngLib user can select test procedure from *NIST SP800-90B* or the one of *BSI-AIS20/AIS31* or both.
  The RngLib user can select the online test procedure from *NIST SP800-90B* or the one of *BSI-AIS20/AIS31* or both.
  The ES developer can either use the RngLib for achieving the *NIST SP800-90B* and *BSI-AIS20/AIS31* requirements for total failure and online tests or implement it using the recommendations from *UM_ST31R_TRNG*.
  The conditioning requirements (according to *SOG-IS ACM*) are not implemented by the RngLib. In both cases *NIST SP800-90B* or *BSI-AIS20/AIS31* conditioning has to be implemented by the ES when required using the recommendations from *UM_ST31R_TRNG*.

5.1.2 Additional Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

177 The TSF shall perform ***the operations in*** *Table 8* in accordance with a specified cryptographic algorithm ***in*** *Table 8* and cryptographic key sizes ***of*** *Table 8* that meet the ***standards in*** *Table 8****.***

Table 8. FCS_COP.1 iterations (cryptographic operations)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
TDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Triple Data Encryption Standard	168 bits	*NIST SP 800-67* *NIST SP 800-38A*
AES	* encryption (cipher) * decryption (inverse cipher) - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS PUB 197*

5.1.3 Additional Security Functional Requirements for the memories protection

178 The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the memories protection.

Static attribute initialisation (FMT_MSA.3) / Memories

179 The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to provide ***minimally protective***[b] default values for security attributes that are used to enforce the SFP.

180 The TSF shall allow ***none*** to specify alternative initial values to override the default values when an object or information is created.

Application note:
The security attributes are the set of access rights currently defined. They are dynamically attached to the subjects and objects locations, i.e. each logical address.

b. See the Datasheet referenced in *Section 7* for actual values.

Management of security attributes (FMT_MSA.1) / Memories

181 The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***current set of access rights*** to ***software having the needed clearance.***

Complete access control (FDP_ACC.2) / Memories

182 The TSF shall enforce the ***Dynamic Memory Access Control Policy*** on ***all subjects (software), all objects (data including code stored in memories)*** and all operations among subjects and objects covered by the SFP.

183 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Security attribute based access control (FDP_ACF.1) / Memories

184 The TSF shall enforce the ***Dynamic Memory Access Control Policy*** to objects based on the following: ***software mode, the object location, the operation to be performed, and the current set of access rights.***

185 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the operation is allowed if and only if the software mode, the object location and the operation matches an entry in the current set of access rights.***

186 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***None***.

187 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- ***in User configuration, any access (read, write, execute) to the OST ROM is denied,***
- ***in User configuration, any write access to the ST NVM is denied.***

188 **Note**: It should be noted that this level of policy detail is not needed at the application level. The composite Security Target writer should describe the ES access control and information flow control policies instead. Within the ES High Level Design description, the chosen setting of IC security attributes would be shown to implement the described policies relying on the IC SFP presented here.

189 The following SFP ***Dynamic Memory Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / Memories":

190 *SFP_3: Dynamic Memory Access Control Policy*

The TSF must control read, write, execute accesses of software to data, based on the software mode and on the current set of access rights.

Specification of management functions (FMT_SMF.1) / Memories

191 The TSF shall be capable of performing the following management functions: ***modification of the current set of access rights security attributes by software having the needed clearance, supporting the Dynamic Memory Access Control Policy.***

5.1.4 Additional Security Functional Requirements related to the loading and authentication capabilities

Authentication Proof of Identity (FIA_API.1)

192 The TSF shall provide a ***command based on a cryptographic mechanism*** to prove the identity of the TOE to an external entity.

Limited capabilities (FMT_LIM.1) / Loader

193 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: ***Loader Limited capability Policy.***

194 *SFP_4: Loader Limited capability Policy*

195 *Deploying Loader functionality after **delivery** does not allow stored user data to be disclosed or manipulated by unauthorized user.*

Limited availability (FMT_LIM.2) / Loader

196 The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: ***Loader Limited availability Policy.***

197 *SFP_5: Loader Limited availability Policy*

198 *The TSF prevents deploying the Loader functionality after **blocking of the loader**.*

199 **Note**: Blocking the loader is just an option.

Inter-TSF trusted channel (FTP_ITC.1) / Loader

200 The TSF shall provide a communication channel between itself and another trusted IT product 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.

201 The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

202 The TSF shall initiate communication via the trusted channel for ***Maintenance transaction***.

203 ***Refinement:***

In practice, the communication is not initiated by the TSF.

Basic data exchange confidentiality (FDP_UCT.1) / Loader

204 The TSF shall enforce the *Loader SFP* to receive user data in a manner protected from unauthorized disclosure.

Data exchange integrity (FDP_UIT.1) / Loader

205 The TSF shall enforce the *Loader SFP* to receive user data in a manner protected from modification, deletion, insertion errors.

206 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

Subset access control (FDP_ACC.1) / Loader

207 The TSF shall enforce the *Loader SFP* on:

- the subjects ***ST Loader, User Loader, and Delegated Loader,***
- the objects user data in ***User NVM and ST data in ST NVM,***
- the operation ***Maintenance transaction***.

Security attribute based access control (FDP_ACF.1) / Loader

208 The TSF shall enforce the *Loader SFP* to objects based on the following: ***all subjects, objects and attributes defined in the Loader SFP.***

209 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***if the user authenticated role is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.***

Note that the term “data” also addresses Additional Code, as this code is seen as data by the TSF.

210 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***none.***

211 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***none.***

212 The following SFP ***Loader SFP*** is defined for the requirements “Basic data exchange confidentiality (FDP_UCT.1) / Loader”, “Data exchange integrity (FDP_UIT.1) / Loader”, “Subset access control (FDP_ACC.1) / Loader”, "Security attribute based access control (FDP_ACF.1) / Loader", "Static attribute initialisation (FMT_MSA.3) / Loader", and "Management of security attributes (FMT_MSA.1) / Loader":

<u>213</u> *<u>SFP_6: Loader SFP</u>*

214 *The TSF must enforce that a maintenance transaction is performed if and only if* ***the user authenticated role is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.***

The TSF ruling is done according to a fixed access rights matrix, based on the subject, object and security attributes listed below.

The Security Function Policy (SFP) Loader SFP uses the following definitions:

- *the subjects are the ST Loader, the User Loader, and the Delegated Loader,*
- *the objects are ST NVM and User NVM,*
- *the operation is Maintenance transaction,*
- *the security attributes linked to the subjects are the remaining sessions, the number of consecutive authentication failures, the allowed memory areas, the logging capacity, the transaction identification.*

Note that subjects are authorized by cryptographic keys. These keys are considered as authentication data and not as security attributes.

Failure with preservation of secure state (FPT_FLS.1) / Loader

215 The TSF shall preserve a secure state when the following types of failures occur: ***the maintenance transaction is incomplete***.

Static attribute initialisation (FMT_MSA.3) / Loader

216 The TSF shall enforce the ***Loader SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

217 The TSF shall allow ***none*** to specify alternative initial values to override the default values when an object or information is created.

Management of security attributes (FMT_MSA.1) / Loader

218 The TSF shall enforce the ***Loader SFP*** to restrict the ability to ***modify*** the security attributes ***remaining sessions, transaction identification*** to ***the ST Loader or User Loader.***

Specification of management functions (FMT_SMF.1) / Loader

219 The TSF will be able to perform the following management functions: ***change the role authentication data, change the remaining sessions, block a role, under the Loader SFP.***

Security roles (FMT_SMR.1) / Loader

220 The TSF shall maintain the roles: ***ST Loader, User Loader, Delegated Loader, Secure Diagnostic, and Everybody***.

221 The TSF shall be able to associate users with roles.

Timing of identification (FIA_UID.1) / Loader

222 The TSF shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is identified.

223 The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

Timing of authentication (FIA_UAU.1) / Loader

224 The TSF shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is authenticated.

225 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

Audit storage (FAU_SAS.1) / Loader

226 The TSF shall provide ***the Loader*** with the capability to store the ***transaction identification of the loaded data*** in the ***NVM***.

227 ***Refinement:***

The TSF shall systematically store the transaction identification provided by the ST Loader or User Loader together with the loaded data.

Audit review (FAU_SAR.1) / Loader

228 The TSF shall provide ***Everybody*** with the capability to read the ***Product information and the Identification of the last completed maintenance transaction, if any,*** from the audit records.

229 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.5 Additional Security Functional Requirements related to the Secure Diagnostic capabilities

Limited capabilities (FMT_LIM.1) / Sdiag

230 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: ***Sdiag Limited Capability Policy.***

231 *SFP_7: Sdiag Limited Capability Policy*

232 *Deploying Secure Diagnostic capability does not allow stored user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*

Limited availability (FMT_LIM.2) / Sdiag

233 The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: ***Sdiag Limited Availability Policy.***

234 *SFP_8: Sdiag Limited Availability Policy*

235 *The TSF prevents deploying the Secure Diagnostic capability unless the Secure Diagnostic mode is explicitly enabled by the authorized user. When the Secure Diagnostic capability is deployed, the TSF allows performing only authorized and authentic diagnostic transactions.*

236 ***Refinement:***

By enabling the Secure Diagnostic capability, the Composite Product Manufacturer gives authority to the IC manufacturer to exercise the Secure Diagnostic capability known to abide by SFP_7.

Inter-TSF trusted channel (FTP_ITC.1) / Sdiag

237 The TSF shall provide a communication channel between itself and another trusted IT product 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.

238 The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

239 The TSF shall initiate communication via the trusted channel for ***Secure Diagnostic transaction***.

240 ***Refinement:***

In practice, the communication is initiated by the trusted IT product.

Audit review (FAU_SAR.1) / Sdiag

241 The TSF shall provide ***Everybody*** with the capability to read the ***Secure Diagnostic enable status,*** from the audit records.

242 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2 TOE security assurance requirements

243 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level ***6*** (EAL***6***) and augmented by taking the following components:

- ***ALC_FLR.2 and ASE_TSS.2.***

244 Regarding application note 22 of *BSI-CC-PP-0084-2014*, the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

245 The component ALC_FLR.2 is chosen as an augmentation in this ST because a solid flaw management is key for the continuous improvement of the security IC platforms, especially on markets which need highly resistant and long lasting products.

246 The component ASE_TSS.2 is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.

247 The set of security assurance requirements (SARs) is presented in *Table 9*, indicating the origin of the requirement.

Table 9. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL6/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL6
ADV_IMP.2	Complete mapping of the implementation representation of the TSF	EAL6
ADV_INT.3	Minimally complex internals	EAL6
ADV_SPM.1	Formal TOE security policy model	EAL6
ADV_TDS.5	Complete semiformal modular design	EAL6
AGD_OPE.1	Operational user guidance	EAL6/*BSI-CC-PP-0084-2014*
AGD_PRE.1	Preparative procedures	EAL6/*BSI-CC-PP-0084-2014*
ALC_CMC.5	Advanced support	EAL6
ALC_CMS.5	Development tools CM coverage	EAL6
ALC_DEL.1	Delivery procedures	EAL6/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	EAL6/*BSI-CC-PP-0084-2014*
ALC_FLR.2	Flaw reporting procedures	Security Target

Table 9. TOE security assurance requirements (continued)

Label	Title	Origin
ALC_LCD.1	Developer defined life-cycle model	EAL6/*BSI-CC-PP-0084-2014*
ALC_TAT.3	Compliance with implementation standards - all parts	EAL6
ASE_CCL.1	Conformance claims	EAL6/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL6/*BSI-CC-PP-0084-2014*
ASE_INT.1	ST introduction	EAL6/*BSI-CC-PP-0084-2014*
ASE_OBJ.2	Security objectives	EAL6/*BSI-CC-PP-0084-2014*
ASE_REQ.2	Derived security requirements	EAL6/*BSI-CC-PP-0084-2014*
ASE_SPD.1	Security problem definition	EAL6/*BSI-CC-PP-0084-2014*
ASE_TSS.2	TOE summary specification with architectural design summary	Security Target
ATE_COV.3	Rigorous analysis of coverage	EAL6
ATE_DPT.3	Testing: modular design	EAL6
ATE_FUN.2	Ordered functional testing	EAL6
ATE_IND.2	Independent testing - sample	EAL6/*BSI-CC-PP-0084-2014*
AVA_VAN.5	Advanced methodical vulnerability analysis	EAL6/*BSI-CC-PP-0084-2014*

5.3 Refinement of the security assurance requirements

248 As *BSI-CC-PP-0084-2014* defines refinements for selected SARs, these refinements are also claimed in this Security Target.

249 The main customizing is that the IC Dedicated Software is an operational part of the TOE after delivery, although it is mainly not available to the user.

250 Regarding application note 23 of *BSI-CC-PP-0084-2014*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

251 The text of the impacted refinements of *BSI-CC-PP-0084-2014* is reproduced in the next sections.

252 For reader's ease, an impact summary is provided in *Table 10*.

Table 10. Impact of EAL6 selection on *BSI-CC-PP-0084-2014* refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ALC_DEL	1	1	New refinement related to the Loader
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	5	None, refinement is still valid

Table 10. Impact of EAL6 selection on *BSI-CC-PP-0084-2014* refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, IC Dedicated Software is included
ADV_IMP	1	2	None, refinement is still valid
ADV_SPM	-	1	New refinement added (see below)
ATE_COV	2	3	IC Dedicated Software is included
AGD_OPE	1	1	None
AGD_PRE	1	1	New refinement related to the Loader
AVA_VAN	5	5	None

5.3.1 Refinement regarding delivery procedure (ALC_DEL)

253 According to *JIL-Post-Deliv-Load*:

254 For the delivery of the Initial TOE, Additional Code and Final TOE, all the guidance describing the delivery procedures shall be taken into account.

255 They must especially describe the protection measures of the proof associated to the Additional Codes and the protection measures of the cryptographic keys used to generate this proof. The measures described in the guidance will have to be audited.

5.3.2 Refinement regarding functional specification (ADV_FSP)

256 ~~Although the IC Dedicated Test Software is a part of the TOE, the test functions of the IC Dedicated Test Software are not described in the Functional Specification because the IC Dedicated Test Software is considered as a test tool delivered with the TOE but not providing security functions for the operational phase of the TOE.~~ ***The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are properly identified in the delivered documentation.***

257 The Functional Specification ***refers to datasheet to*** trace security features that do not provide any external interface but that contribute to fulfil the SFRs e.g. like physical protection. Thereby they are part of the complete instantiation of the SFRs.

258 The Functional Specification ***refers to design specifications to detail the*** mechanisms against physical attacks ***described*** in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those mechanisms where inspection of the layout is of relevance or tests beside the TSFI may be needed.

259 The Functional Specification ***refers to data sheet to*** specify operating conditions of the TOE. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.

260 All functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software (refer to the security functional requirement (FMT_LIM.2)) ***are part of the*** Functional Specification. Details will be given in the document for ADV_ARC~~, refer to~~

~~Section 6.2.1.5.~~ In addition, all these functions and mechanisms ***are*** subsequently ~~be~~ refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after TOE Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information ***is*** provided to allow tests and vulnerability assessment.

261 Since the selected higher-level assurance component requires a security functional specification presented in a “semi-formal style" (ADV_FSP.5.2C) the changes affect the style of description, the *BSI-CC-PP-0084-2014* refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

5.3.3 Refinement regarding security policy model (ADV_SPM)

262 The CC V3.1 explains how a security policy model contributes to the documentation of the security functionality of the TOE and requires the developer to indicate the policies that are formally modeled by means of the assignment designed in the part 3 assurance component ADV_SPM.1.

Formal TOE security policy model (ADV_SPM.1)

263 The developer ***provides*** a formal security policy model for ~~one of~~ the ***following*** Security Functional Policies~~, to be defined after analysis~~:

1. *SFP_1: Limited capability and availability Policy / Test*,
2. *SFP_4: Loader Limited capability Policy* ***and*** *SFP_5: Loader Limited availability Policy*
3. *SFP_7: Sdiag Limited Capability Policy* ***and*** *SFP_8: Sdiag Limited Availability Policy*
4. *SFP_3: Dynamic Memory Access Control Policy*.
5. *SFP_6: Loader SFP*.

264 For each policy covered by the formal security policy model, the model ~~shall~~ identif***ies*** the relevant portions of the statement of SFRs that make up that policy.

265 The developer shall provide a formal proof of correspondence between the model and any formal functional specification.

266 The developer ~~shall~~ provide***s*** a demonstration of correspondence between the model and the functional specification.

267 The functionalities modeled are all the SFRs except for the ones listed in *Table 11*.

Table 11. Not modeled SFRs

Label	Title	Explanation
FRU_FLT.2	Limited fault tolerance	Physical phenomenon that requires different modeling systems, nor formal system for mechanical reasoning.
FDP_SDC.1	Stored data confidentiality	Physical functions cannot be modeled in logic formal systems.
FPT_PHP.3	Resistance to physical attack	Physical functions cannot be modeled in logic formal systems, but the formal security policy model covers the reaction part.

Table 11. Not modeled SFRs

Label	Title	Explanation
FDP_ITT.1	Basic internal transfer protection	Disclosure phenomenon that requires different modeling systems, information flow reasoning would only catch the logical part, but there is more to it.
FPT_ITT.1	Basic internal TSF data transfer protection	
FDP_IFC.1	Subset information flow control	Same rationale as FDP_ITT.1 and FPT_ITT.1. This is *SFP_2: Data Processing Policy*, the only SFP not covered by the formal security policy model.
FCS_RNG.1	Random number generation	Dedicated mathematical models are provided; traditionally not in the formal security policy model scope.
FCS_COP.1	Cryptographic operation	Dedicated analysis are performed; traditionally not in the formal security policy model scope.

5.3.4 Refinement regarding test coverage (ATE_COV)

268 The TOE ***is*** tested under different operating conditions within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that “Fault tolerance (FRU_FLT.2)” ***is*** proven for the complete TSF. The tests ~~must~~ also cover functions which may be affected by “ageing” (such as ~~EEPROM~~ ***NVM*** writing).

269 The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT_PHP.3) cannot be tested in a straightforward way. Instead ***STMicroelectronics provides*** evidence that the TOE actually has the particular physical characteristics (especially layout design principles). This ***is*** done by checking the layout (implementation or actual) in an appropriate way. The required evidence pertains to the existence of mechanisms against physical attacks (unless being obvious).

270 ~~The IC Dedicated Test Software is seen as a “test tool” being delivered as part of the TOE. However, the Test Features do not provide security functionality. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis.~~ ***The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are part of the Test Coverage Analysis.***

5.3.5 Refinement regarding preparative procedures (AGD_PRE)

271 According to *JIL-Post-Deliv-Load*:

272 Preparative user guidance are intended to be used by persons responsible for the following tasks:

- acceptance of the Initial TOE and of the Additional Code;
- installation of the TOE: download of the Additional Code onto the Initial TOE, activation of the Additional Code, checking of the resulting Identification Data.

5.4 Security Requirements rationale

5.4.1 Rationale for the Security Functional Requirements

273 Just as for the security objectives rationale of *Section 4.3*, the main line of this rationale is that the inclusion of all the security requirements of the *BSI-CC-PP-0084-2014* Protection Profile, together with those in *AUG*, and with those introduced in this Security Target, guarantees that all the security objectives identified in *Section 4* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Inherent	*Basic internal transfer protection FDP_ITT.1* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.Phys-Probing	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*
BSI.O.Malfunction	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.Phys-Manipulation	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* *Limited capabilities - Secure Diagnostic FMT_LIM.1 / Sdiag* *Limited availability - Secure Diagnostic FMT_LIM.2 / Sdiag* *Inter-TSF trusted channel - Secure Diagnostic FTP_ITC.1 / Sdiag* *Audit review - Secure Diagnostic FAU_SAR.1 / Sdiag* plus those for *BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FDP_SDI.2*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.O.Identification	*Audit storage FAU_SAS.1*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.RND	*Random number generation - PTG.2 FCS_RNG.1 / PTG.2* *Random number generation* - *FCS_RNG.1 / PG* *Random number generation - RngLib FCS_RNG.1 / RngLib* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDI.2*, *FDP_SDC.1*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.OE.Resp-Appl	Not applicable
BSI.OE.Process-Sec-IC	Not applicable
BSI.OE.Lim-Block-Loader	Not applicable
BSI.OE.Loader-Usage	Not applicable
BSI.OE.TOE-Auth	Not applicable
OE.Enable-Disable-Secure-Diag	Not applicable
OE.Secure-Diag-Usage	Not applicable
BSI.O.Authentication	*Authentication Proof of Identity FIA_API.1*
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*
BSI.O.Ctrl-Auth-Loader	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
JIL.O.Prot-TSF-Confidentiality	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*
JIL.O.Secure-Load-ACode	"*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader* "*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader* "*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader* "*Subset access control - Loader*" *FDP_ACC.1 / Loader* "*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader* "*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader* "*Management of security attribute - Loader*" *FMT_MSA.1 / Loader* "*Specification of management functions - Loader*" *FMT_SMF.1 / Loader* "*Security roles - Loader*" *FMT_SMR.1 / Loader* "*Timing of identification - Loader*" *FIA_UID.1 / Loader* "*Timing of authentication - Loader*" *FIA_UAU.1 / Loader* "*Audit storage - Loader*" *FAU_SAS.1 / Loader*
JIL.O.Secure-AC-Activation	"*Failure with preservation of secure state - Loader*" *FPT_FLS.1 / Loader*
JIL.O.TOE-Identification	"*Audit storage - Loader*" *FAU_SAS.1 / Loader* "*Audit review - Loader*" *FAU_SAR.1 / Loader* "*Stored data integrity monitoring and action*" *FDP_SDI.2*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
O.Secure-Load-AMemImage	“*Inter-TSF trusted channel - Loader*” *FTP_ITC.1 / Loader* “*Basic data exchange confidentiality - Loader*” *FDP_UCT.1 / Loader* “*Data exchange integrity - Loader*” *FDP_UIT.1 / Loader* “*Subset access control - Loader*” *FDP_ACC.1 / Loader* “*Security attribute based access control - Loader*” *FDP_ACF.1 / Loader* “*Static attribute initialisation - Loader*” *FMT_MSA.3 / Loader* “*Management of security attribute - Loader*” *FMT_MSA.1 / Loader* “*Specification of management functions - Loader*” *FMT_SMF.1 / Loader* “*Security roles - Loader*” *FMT_SMR.1 / Loader* “*Timing of identification - Loader*” *FIA_UID.1 / Loader* “*Timing of authentication - Loader*” *FIA_UAU.1 / Loader* “*Audit storage - Loader*” *FAU_SAS.1 / Loader*
O.MemImage-Identification	“*Failure with preservation of secure state - Loader*” *FPT_FLS.1 / Loader* “*Audit storage - Loader*” *FAU_SAS.1 / Loader* “*Audit review - Loader*” *FAU_SAR.1 / Loader* “*Stored data integrity monitoring and action*” *FDP_SDI.2*
OE.Composite-TOE-Id	Not applicable
OE.TOE-Id	Not applicable
AUG1.O.Add-Functions	*Cryptographic operation FCS_COP.1*
AUG4.O.Mem-Access	*Complete access control FDP_ACC.2 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories* *Management of security attribute FMT_MSA.1 / Memories* *Specification of management functions FMT_SMF.1 / Memories*
O.Firewall	“*Complete access control*” *FDP_ACC.2 / Memories* “*Security attribute based access control*” *FDP_ACF.1 / Memories* “*Static attribute initialisation*” *FMT_MSA.3 / Memories* “*Management of security attribute*” *FMT_MSA.1 / Memories* “*Specification of management functions*” *FMT_SMF.1 / Memories*

274 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 7* and *Table 12*, it can be verified that the justifications provided by the *BSI-CC-PP-0084-2014* Protection Profile and *AUG* can just be carried forward to their union.

275 From *Table 5*, it is straightforward to identify additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem-Access*) tracing back to *AUG*, additional objectives (*JIL.O.Prot-TSF-Confidentiality*, *JIL.O.Secure-Load-ACode*, *JIL.O.Secure-AC-Activation* and *JIL.O.TOE-Identification*) tracing back to *JIL-Post-Deliv-Load* / *ANSSI-CC-CER/F/06.002*, and additional objectives (*O.Secure-Load-AMemImage*, *O.MemImage-*

Identification, O.Firewall) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

276 Furthermore, a careful observation of the requirements listed in *Table 7* and *Table 12* shows that:

- there are security requirements introduced from *AUG* (*FCS_COP.1*, *FDP_ACC.2 / Memories*, *FDP_ACF.1 / Memories*, *FMT_MSA.3 / Memories* and *FMT_MSA.1 / Memories*),
- there are additional security requirements introduced by this Security Target (*FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMF.1 / Loader*, *FMT_SMR.1 / Loader*, *FIA_UID.1 / Loader*, *FIA_UAU.1 / Loader*, *FPT_FLS.1 / Loader*, *FAU_SAS.1 / Loader*, *FAU_SAR.1 / Loader*, *FMT_SMF.1 / Memories*, *FTP_ITC.1 / Sdiag, FAU_SAR.1 / Sdiag, FMT_LIM.1 / Sdiag, FMT_LIM.2 / Sdiag, FCS_RNG.1 / RngLib,* and various assurance requirements of EAL6+).

277 Though it remains to show that:

- security objectives from this Security Target, from *JIL-Post-Deliv-Load* / *ANSSI-CC-CER/F/06.002* and from *AUG* are addressed by security requirements stated in this chapter,
- additional security requirements from this Security Target and from *AUG* are mutually supportive with the security requirements from the *BSI-CC-PP-0084-2014* Protection Profile, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

278 The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in *BSI-CC-PP-0084-2014*, they form an internally consistent whole, is provided in the next subsections.

5.4.2 Additional security objectives are suitably addressed

Security objective "Dynamic Area based Memory Access Control (*AUG4.O.Mem-Access*)"

279 The justification related to the security objective "***Dynamic*** Area based Memory Access Control (*AUG4.O.Mem-Access*)" is as follows:

280 The security functional requirements "*Complete access control (FDP_ACC.2) / Memories*" ***and "****Security attribute based access control (FDP_ACF.1) / Memories****"***, with the related Security Function Policy (SFP) "***Dynamic Memory Access Control Policy***" exactly require to implement a ***Dynamic*** area based memory access control as demanded by *AUG4.O.Mem-Access*. Therefore, *FDP_ACC.2 / Memories* ***and*** *FDP_ACF.1 / Memories* with ***their*** SFP ***are*** suitable to meet the security objective.

281 The security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Memories*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) ***as further detailed in the security functional requirement "****Management of security attributes (FMT_MSA.1) / Memories****"***. These management functions ensure that the required access control can be realised using the functions provided by the TOE.

Security objective “Additional Specific Security Functionality (*AUG1.O.Add-Functions*)”

282 The justification related to the security objective “Additional Specific Security Functionality (*AUG1.O.Add-Functions*)” is as follows:

283 The security functional requirements “*Cryptographic operation (FCS_COP.1)*” exactly requires those functions to be implemented that are demanded by *AUG1.O.Add-Functions.* Therefore, *FCS_COP.1* is suitable to meet the security objective.

Security objective “Protection against Abuse of Functionality (*BSI.O.Abuse-Func*)”

284 This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by "*Limited availability (FMT_LIM.2) / Test*" ***and*** "*Limited availability (FMT_LIM.2) / Sdiag*", and the second one by "*Limited capabilities (FMT_LIM.1) / Test*" ***and*** "*Limited capabilities (FMT_LIM.1) / Sdiag*". Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, ***these*** security functional requirements together are suitable to meet the objective.

285 Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective. The relevant ***Security Functional requirements*** are also listed in *Table 12*.

Security objective “Random Numbers (*BSI.O.RND*)”

286 *FCS_RNG.1 / PTG.2*, *FCS_RNG.1 / PG* and *FCS_RNG.1 / RngLib* requires the TOE to provide random numbers of good quality. To specify the exact metric is left to the individual Security Target for a specific TOE.

287 Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator. Random numbers are often used by the Security IC Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorised disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the TOE.

Security objective “Access control and authenticity for the Loader (*BSI.O.Ctrl-Auth-Loader*)”

288 The justification related to the security objective “Access control and authenticity for the Loader (*BSI.O.Ctrl-Auth-Loader*)” is as follows:

289 The ***security functional requirement*** "*Subset access control (FDP_ACC.1) / Loader*" defines the subjects, objects and operations of the Loader SFP enforced by the SFR *FTP_ITC.1 / Loader*, *FDP_UCT.1 / Loader*, *FDP_UIT.1 / Loader* and *FDP_ACF.1 / Loader*. The ***security functional requirement*** "*Inter-TSF trusted channel (FTP_ITC.1) / Loader*" requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.

The ***security functional requirement*** "*Basic data exchange confidentiality (FDP_UCT.1) / Loader*" requires the TSF to receive data protected from unauthorized disclosure.
The ***security functional requirement*** "*Data exchange integrity (FDP_UIT.1) / Loader*" requires the TSF to verify the integrity ***and the rightfulness*** of the received data.
The ***security functional requirement*** "*Security attribute based access control (FDP_ACF.1) / Loader*" requires the TSF to implement access control for the Loader functionality.
Therefore, *FTP_ITC.1 / Loader*, *FDP_UCT.1 / Loader*, *FDP_UIT.1 / Loader*, *FDP_ACC.1 / Loader* and *FDP_ACF.1 / Loader* with their SFP are suitable to meet the security objective.

290 Complementary, the security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Loader*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) / Loader*"
The security functional requirements "*Security roles (FMT_SMR.1) / Loader*", "*Timing of identification (FIA_UID.1) / Loader*" and "*Timing of authentication (FIA_UAU.1) / Loader*" specify the roles that the TSF recognises and the actions authorized before their identification.
The security functional requirement "*Specification of management functions (FMT_SMF.1) / Loader*" provides additional controlled facility for adapting the loader behaviour to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realized using the functions provided by the TOE.

Security objectives "Protection of the confidentiality of the TSF (*JIL.O.Prot-TSF-Confidentiality*)", "Secure loading of the Additional Code (*JIL.O.Secure-Load-ACode*)" and "Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)"

291 The justification related to the security objectives **"**Protection of the confidentiality of the TSF (*JIL.O.Prot-TSF-Confidentiality*)", "Secure loading of the Additional Code (*JIL.O.Secure-Load-ACode*)" and "Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)" is as follows:

292 The security functional requirement "*Subset access control (FDP_ACC.1) / Loader*" defines the subjects, objects and operations of the Loader SFP enforced by the SFR FTP_ITC.1, FDP_UCT.1, FDP_UIT.1 and FDP_ACF.1/Loader.
The security functional requirement "*Inter-TSF trusted channel (FTP_ITC.1) / Loader*" requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.
The security functional requirement "*Basic data exchange confidentiality (FDP_UCT.1) / Loader*" requires the TSF to receive data protected from unauthorized disclosure.
The security functional requirement "*Data exchange integrity (FDP_UIT.1) / Loader*" requires the TSF to verify the integrity of the received data.
The security functional requirement "*Security attribute based access control (FDP_ACF.1) / Loader*" requires the TSF to implement access control for the Loader functionality.
The security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Loader*" requires that the TOE provides default values for security attributes.
The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) / Loader*".
The security functional requirements "*Security roles (FMT_SMR.1) / Loader*", "*Timing of identification (FIA_UID.1) / Loader*" and "*Timing of authentication (FIA_UAU.1) / Loader*"

specify the roles that the TSF recognises and the actions authorized before their identification.
The security functional requirement "*Specification of management functions (FMT_SMF.1) / Loader*" provides additional controlled facility for adapting the loader behaviour to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realised using the functions provided by the TOE.
The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires to store the identification data needed to enforce that only the allowed version of the Additional Memory Image can be loaded on the Initial TOE.

293 Therefore, *FTP_ITC.1 / Loader*, *FDP_UCT.1 / Loader*, *FDP_UIT.1 / Loader*, *FDP_ACC.1 / Loader*, *FDP_ACF.1 / Loader* together with *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMR.1 / Loader*, *FMT_SMF.1 / Loader*, *FIA_UID.1 / Loader*, *FIA_UAU.1 / Loader,* and *FAU_SAS.1 / Loader* are suitable to meet these security objectives.

Security objective "Secure activation of the Additional Code (*JIL.O.Secure-AC-Activation*)"

294 The justification related to the security objective "Secure activation of the Additional Code (*JIL.O.Secure-AC-Activation*)" is as follows:

295 The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by *JIL.O.Secure-AC-Activation*.

296 Therefore, *FPT_FLS.1 / Loader* is suitable to meet this security objective.

Security objective "Secure identification of the TOE (*JIL.O.TOE-Identification*)"

297 The justification related to the security objective "Secure identification of the TOE (*JIL.O.TOE-Identification*)" is as follows:

298 The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to store the Identification Data of the Memory Images.
The security functional requirement "*Stored data integrity monitoring and action (FDP_SDI.2)*" requires the TSF to detect the integrity errors of the stored data and react in case of detected errors.
The security functional requirement "*Audit review (FAU_SAR.1) / Loader*" allows any user to read this Identification Data.

299 Therefore, *FAU_SAS.1 / Loader*, and *FAU_SAR.1 / Loader* together with *FDP_SDI.2* are suitable to meet this security objective.

Security objective "Secure identification of the Memory Image (*O.MemImage-Identification*)"

300 The justification related to the security objective "Secure identification of the Memory Image (*O.MemImage-Identification*)" is as follows:

301 The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to store the Identification Data of the Memory Images.
The security functional requirement "*Stored data integrity monitoring and action (FDP_SDI.2)*" requires the TSF to detect the integrity errors of the stored user data and react in case of detected errors.
The security functional requirement "*Audit review (FAU_SAR.1) / Loader*" allows any user to read this Identification Data.
The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF

to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by *JIL.O.Secure-AC-Activation*.

302 Therefore, *FAU_SAS.1 / Loader*, *FAU_SAR.1 / Loader* together with *FDP_SDI.2* and *FPT_FLS.1 / Loader* are suitable to meet this security objective.

Security objective “Specific application firewall (*O.Firewall*)”

303 The justification related to the security objective “Specific application firewall (*O.Firewall*)” is as follows:

304 The security functional requirements "*Complete access control (FDP_ACC.2) / Memories*" and "*Security attribute based access control (FDP_ACF.1) / Memories*", supported by "*Static attribute initialisation (FMT_MSA.3) / Memories*", require that no application can read, write, compare any piece of data or code belonging to a specific application. This meets the security objective *O.Firewall*.

305 The security attributes addressed by the functional requirements “*Management of security attributes (FMT_MSA.1) / Memories*" and "*Specification of management functions (FMT_SMF.1) / Memories*" ensure that the required access control can be realised using the functions provided by the TOE.

5.4.3 Additional security requirements are consistent

"Cryptographic operation (*FCS_COP.1*)"

306 These security requirements have already been argued in *Section : Security objective “Additional Specific Security Functionality (AUG1.O.Add-Functions)”* above.

"Random number generation (*FCS_RNG.1 / RngLib*)"

307 These security requirements have already been argued in *Section : Security objective “Random Numbers (BSI.O.RND)”* above.

"Static attribute initialisation (*FMT_MSA.3 / Memories*),
Management of security attributes (*FMT_MSA.1 / Memories*),
Complete access control (*FDP_ACC.2 / Memories*),
Security attribute based access control (*FDP_ACF.1 / Memories*)"

308 These security requirements have already been argued in *Section : Security objective “Dynamic Area based Memory Access Control (AUG4.O.Mem-Access)”* and *Section : Security objective “Specific application firewall (O.Firewall)”* above.

"Static attribute initialisation (*FMT_MSA.3 / Loader*),
Management of security attributes (*FMT_MSA.1 / Loader*),
Specification of management function (*FMT_SMF.1 / Loader*),
Security roles (*FMT_SMR.1 / Loader*),
Timing of identification (*FIA_UID.1 / Loader*),
Timing of authentication (*FIA_UAU.1 / Loader*)"

309 These security requirements have already been argued in *Section : Security objective “Protection against Abuse of Functionality (BSI.O.Abuse-Func)”* and *Section : Security objectives “Protection of the confidentiality of the TSF (JIL.O.Prot-TSF-Confidentiality)”, “Secure loading of the Additional Code (JIL.O.Secure-Load-ACode)” and “Secure loading of the Additional Memory Image (O.Secure-Load-AMemImage)”* above.

"Audit storage (*FAU_SAS.1 / Loader*),
Audit review (*FAU_SAR.1 / Loader*)"

310 These security requirements have already been argued in *Section : Security objective “Secure identification of the TOE (JIL.O.TOE-Identification)”* and *Section : Security objective “Secure identification of the Memory Image (O.MemImage-Identification)”* above.

"Failure with preservation of secure state (*FPT_FLS.1 / Loader*)"

311 This security requirement has already been argued in *Section : Security objective “Secure activation of the Additional Code (JIL.O.Secure-AC-Activation)”* and *Section : Security objective “Secure identification of the Memory Image (O.MemImage-Identification)”* above.

"Inter-TSF trusted channel(*FTP_ITC.1 / Sdiag*),
Audit review (*FAU_SAR.1 / Sdiag*),
Limited capabilities (*FMT_LIM.1 / Sdiag*),
Limited availability (*FMT_LIM.2 / Sdiag*)

312 These security requirements have already been argued in *Section : Security objective “Protection against Abuse of Functionality (BSI.O.Abuse-Func)”* above.

5.4.4 Dependencies of Security Functional Requirements

313 All dependencies of Security Functional Requirements have been fulfilled in this Security Target except :

- those justified in the *BSI-CC-PP-0084-2014* Protection Profile security requirement rationale,
- those justifed in *AUG* security requirements rationale,
- the dependency of *FCS_COP.1* on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 (see discussion below),
- the dependency of *FCS_COP.1* on FCS_CKM.4 (see discussion below),
- the dependency of *FAU_SAR.1 / Loader* on FAU_GEN.1 (see discussion below),
- the dependency of *FAU_SAR.1 / Sdiag* on FAU_GEN.1 (see discussion below).

314 Details are provided in *Table 13* below.

Table 13. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-CC-PP-0084-2014*
FPT_FLS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Test	FMT_LIM.2 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Test	FMT_LIM.1 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Loader	FMT_LIM.2 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Loader	FMT_LIM.1 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Sdiag	FMT_LIM.2 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FMT_LIM.2 / Sdiag	FMT_LIM.1 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*
FAU_SAS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDC.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDI.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FPT_PHP.3	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes, by FDP_ACC.2 / Memories	Yes, *BSI-CC-PP-0084-2014*
FPT_ITT.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-CC-PP-0084-2014*	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PTG.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PG	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / RngLib	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.4	No, see discussion below	
FDP_ACC.2 / Memories	FDP_ACF.1 / Memories	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes, by FDP_ACC.2 / Memories	Yes, *AUG* ***#4***
	FMT_MSA.3 / Memories	Yes	
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	
FMT_MSA.1 / Memories	[FDP_ACC.1 / Memories or FDP_IFC.1]	Yes, by FDP_ACC.2 / Memories and FDP_IFC.1	Yes, *AUG* ***#4***
	FMT_SMF.1 / Memories	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	Yes, *AUG* ***#4***

Table 13. Dependencies of security functional requirements (continued)

Label	**Dependencies**	**Fulfilled by security requirements in this Security Target**	**Dependency already in *BSI-CC-PP-0084-2014* or in *AUG***
FMT_SMF.1 / Memories	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_API.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FTP_ITC.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_UCT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_UIT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002 R5*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FIA_UID.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_SMF.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

Table 13. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FPT_FLS.1 / Loader	None	No dependency	***No**, CCMB-2017-04-002 R5*
FAU_SAS.1 / Loader	None	No dependency	**Yes**, *BSI-CC-PP-0084-2014*
FAU_SAR.1 / Loader	FAU_GEN.1	No, by FAU_SAS.1 / Loader instead, see discussion below	***No**, CCMB-2017-04-002 R5*
FTP_ITC.1 / Sdiag	None	No dependency	***No**, CCMB-2017-04-002 R5*
FAU_SAR.1 / Sdiag	FAU_GEN.1	No, see discussion below	***No**, CCMB-2017-04-002 R5*

315 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" on "Import of user data without security attributes (FDP_ITC.1)" or "Import of user data with security attributes (FDP_ITC.2)" or "Cryptographic key generation (FCS_CKM.1)". In this particular TOE, the ES has all possibilities to implement its own creation function, in conformance with its security policy. Therefore, no specific SFR is defined in this ST.

316 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" on "Cryptographic key destruction (FCS_CKM.4)". In this particular TOE, there is no specific function for the destruction of the keys. The ES has all possibilities to implement its own destruction function, in conformance with its security policy. Therefore, FCS_CKM.4 is not defined in this ST.

317 Part 2 of the Common Criteria defines the dependency of "*Audit review (FAU_SAR.1) / Loader*" on "Audit data generation (FAU_GEN.1)". In this particular TOE, "*Audit storage (FAU_SAS.1) / Loader*" is used to ensure the storage of audit data, because FAU_GEN.1 is too comprehensive to be used in this context. Therefore this dependency is fulfilled by "*Audit storage (FAU_SAS.1) / Loader*" instead.

318 Part 2 of the Common Criteria defines the dependency of "*Audit review (FAU_SAR.1) / Sdiag*" on "Audit data generation (FAU_GEN.1)". In this particular TOE, there is no specific function for audit data generation, the data to be audited are just stored. Therefore, FAU_GEN.1 is not defined in this ST.

5.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL6 (*Table 9*)

319 Regarding application note 22 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL6 with augmentations because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

320 EAL6 represents a meaningful increase in assurance from EAL4 by requiring a formal security policy model, semiformal design descriptions, a more structured (and hence analyzable) architecture, extensive testing, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.

321 The component ALC_FLR.2 is chosen as an augmentation in this ST because a solid flaw management is key for the continuous improvement of the security IC platforms, especially on markets which need highly resistant and long lasting products.

322 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL6. Therefore, these components add additional assurance to EAL6, but the mutual support of the requirements and the internal consistency is still guaranteed.

323 Note that detailed and updated refinements for assurance requirements are given in *Section 5.3*.

Dependencies of assurance requirements

324 Dependencies of security assurance requirements are fulfilled by the EAL6 package selection.

325 The augmentation to this package identified in paragraph *243* does not introduce dependencies not already satisfied by the EAL6 package, and is considered as consistent augmentation:

- ALC_FLR.2 has no dependency.
- ASE_TSS.2 dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this ST.

6 TOE summary specification (ASE_TSS)

326 This section demonstrates how the TOE meets each Security Functional Requirement, which will be further detailed in the ADV_FSP documents.

6.1 Limited fault tolerance (FRU_FLT.2)

327 The TSF provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to random number generation, power supply, data flows and cryptographic operations, thus preventing risk of malfunction.

6.2 Failure with preservation of secure state (FPT_FLS.1)

328 The TSF provides preservation of secure state by detecting and managing the following events, resulting in an immediate interruption or reset:

- Die integrity violation detection,
- Errors on memories,
- Glitches,
- High voltage supply,
- CPU and MPU errors,
- Sequence control,
- etc..

329 The ES can generate a software reset.

6.3 Limited capabilities (FMT_LIM.1) / Test, Limited capabilities (FMT_LIM.1) / Sdiag, Limited capabilities (FMT_LIM.1) / Loader, Limited availability (FMT_LIM.2) / Test, Limited availability (FMT_LIM.2) / Sdiag & Limited availability (FMT_LIM.2) / Loader

330 The TOE is either in Test, Admin or User configuration.

331 The TOE may also be in Basic Diagnostic (aka Diagnostic), Secure Diagnostic volatile configuration.

332 The Test and Diagnostics configurations are reserved to ST.

333 The TSF ensures the switching and the control of TOE configuration, the corresponding access control and the control of the corresponding capabilities.The transition controls rely on several strong mechanisms including fuse, authentication and control registers. Part of the transitions are only possible in the STMicroelectronics audited environment.

334 The TSF reduces the available features depending on the TOE configuration.

335 The customer can choose to disable irreversibly the Loading capability.

336 The customer can choose to irreversibly enable or disable the Secure Diagnostic capability. Only if the customer enables it, for quality investigation purpose, ST can exercise the Secure Diagnostic capability with a secure protocol, in an audited environment.

6.4 Inter-TSF trusted channel (FTP_ITC.1) / Sdiag

337 In Secure Diagnostic volatile configuration, the System Firmware provides a secure channel to allow another IT product to operate a Secure Diagnostic transaction.

6.5 Audit review (FAU_SAR.1) / Sdiag

338 The System Firmware allows to read the Secure Diagnostic status (permanently disabled, permanently enabled, disabled but still configurable).

6.6 Stored data confidentiality (FDP_SDC.1)

339 The TSF ensures confidentiality of the User Data, thanks to the following features:

- Memories scrambling and encryption,
- Protection of NVM sectors,
- MPU,
- LPU.

6.7 Stored data integrity monitoring and action (FDP_SDI.2)

340 The TSF ensures stored data integrity, thanks to the following features:

- Memories parity control,
- Protection of NVM sectors,
- MPU,
- LPU.

6.8 Audit storage (FAU_SAS.1)

341 In User configuration, the TOE provides commands to store data and/or pre-personalisation data and/or supplements of the ES in the NVM. These commands are only available to authorized processes, and only until phase 6.

6.9 Resistance to physical attack (FPT_PHP.3)

342 The TSF ensures resistance to physical tampering, thanks to the following features:

- The TOE implements a set of countermeasures that reduce the exploitability of physical probing.
- The TOE is physically protected by active shields that command an automatic reaction on die integrity violation detection.

6.10 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1)

343 The TSF prevents the disclosure of internal and user data thanks to:

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment,
- Leakage protection in libraries.

6.11 Random number generation (FCS_RNG.1)

6.11.1 FCS_RNG.1 / PTG.2

344 The TSF provides 32-bit true random numbers that can be qualified with the test metrics required by the *BSI-AIS20/AIS31* standard for a PTG.2 class device.

6.11.2 FCS_RNG.1 / PG

345 The TSF provides 32-bit true random numbers conforming to ANSSI requirements (French scheme) *ANSSI-PG-083,* SOG-IS requirements *SOG-IS ACM* and that can be qualified with the AIS31 statistical procedure tests (Test procedure A of *BSI-AIS20/AIS31*.

6.12 Random number generation (FCS_RNG.1 / RngLib)

346 The TOE provides a software library RngLib that can generate:

- 1024-bit true random numbers that can be qualified with the test metrics required by the *NIST SP800-90B* standard including total failure test and online test procedures.
- 128 bits true random numbers that can be qualified with the test metrics required by the *BSI-AIS20/AIS31* standard for a PTG.2 class device including total failure test and online test procedures.
- The conditioning operations are not performed by the RngLib and must be implemented by the RngLib user when required using the recommendations from *UM_ST31R_TRNG*.

6.13 Cryptographic operation: TDES operation (FCS_COP.1) / TDES

347 The TOE provides an EDES+ accelerator that has the capability to perform 3-key Triple DES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode conformant to *NIST SP 800-67* and *NIST SP 800-38A*.

6.14 Cryptographic operation: AES operation (FCS_COP.1) / AES

348 The AES accelerator provides the following standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to *FIPS PUB 197* with intrinsic counter-measures against attacks:

- cipher,
- inverse cipher,

349 The AES accelerator can operate in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode.

6.15 Static attribute initialisation (FMT_MSA.3) / Memories

350 The TOE enforces a default memory management policy when none other is programmed by the ES.

351 The customer can also use the LPU to protect segments where part of its code and data are stored.

6.16 Management of security attributes (FMT_MSA.1) / Memories & Specification of management functions (FMT_SMF.1) / Memories

352 The TOE provides a dynamic Memory Protection Unit (MPU), that can be configured by the ES.

353 The Library Protection Unit (LPU) offers complementary memory protections, that can be configured in Admin configuration, in case the LPU is not reserved to ST.

6.17 Complete access control (FDP_ACC.2) / Memories & Security attribute based access control (FDP_ACF.1) / Memories

354 The TOE enforces the dynamic memory management policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), a Library Protection Unit (LPU), and complementary protection mechanisms, programmed by the ES.

355 Overriding the MPU and LPU set of access rights, depending on the TOE configuration, the TOE enforces protections on specific parts of the memories.

6.18 Authentication Proof of Identity (FIA_API.1)

356 In Admin configuration, the System Firmware provides commands based on a cryptographic mechanism which allows another IT product to check that the TOE is a genuine TOE.

6.19 Inter-TSF trusted channel (FTP_ITC.1) / Loader, Basic data exchange confidentiality (FDP_UCT.1) / Loader, Data exchange integrity (FDP_UIT.1) / Loader & Audit storage (FAU_SAS.1) / Loader

357 In Admin configuration, the System Firmware provides a secure channel to allow another IT product to operate a maintenance transaction.

358 The ciphered data is automatically decrypted then stored in the requested memory.

359 A maintenance transaction can end only after a successful integrity check of the loaded data or an erase. The identification data associated with the memory update is automatically logged during the session,

6.20 Subset access control (FDP_ACC.1) / Loader & Security attribute based access control (FDP_ACF.1) / Loader

360 In Admin configuration, during a maintenance transaction, the System Firmware verifies if the Loader access conditions are satisfied and returns an error when this is not the case.

361 In particular, the additional memory update must be intended to be assembled with the memory update previously loaded.

6.21 Failure with preservation of secure state (FPT_FLS.1) / Loader

362 In Admin configuration, the System Firmware enforces that a maintenance transaction can only end when it is consistent or canceled by an erase.

6.22 Static attribute initialisation (FMT_MSA.3) / Loader

363 In Admin configuration, the System Firmware provides restrictive default values for the Flash Loader security attributes.

6.23 Management of security attributes (FMT_MSA.1) / Loader & Specification of management functions (FMT_SMF.1) / Loader

364 In Admin configuration, the System Firmware provides the capability for an authorized user to change part of the Flash Loader security attributes.

6.24 Security roles (FMT_SMR.1) / Loader

365 The System Firmware supports the assignment of roles to users through the assignment of different keys for the different roles. This allows to distinguish between the roles of ST Loader, User Loader, Delegated Loader, Secure Diagnostic, and Everybody.

6.25 Timing of identification (FIA_UID.1) / Loader & Timing of authentication (FIA_UAU.1) / Loader

366 The System Firmware identifies the user through the key selected for authentication. This is performed by verifying an encryption, thus preventing to unveil the key.

367 After this authentication, both parties share a session key.

368 A limited number of operations is allowed on behalf of the user before the user is identified and authenticated, such as boot, authentication and non-critical queries.

6.26 Audit review (FAU_SAR.1) / Loader

369 In Admin configuration, the System Firmware allows to read the product information and the identification data of all memory updates previously loaded on the TOE.

7 Identification

Table 14. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	RngLib version
K4H0A	B	0x0299	3.0.6	2.0.2

1. Part of the product information.

Table 15. Guidance documentation

Component description	Reference	Version
Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of flash memory - ST31R platform ST31R480 ST31R320 Datasheet - Preliminary document.	DS_ST31R	0.4
ARM® SC000 Technical Reference Manual	ARM DDI 0456	A
ARMv6-M Architecture Reference Manual	ARM DDI 0419	C
ST31R platform firmware V3 - User manual	UM_ST31R_FWv3	1
Security guidance of the ST31R secure MCU platform - Application note	AN_SECU_ST31R	1
Random number generation for ST31R - User manual	UM_ST31R_TRNG	1
Random number generator library RngLib 2.0.x - User manual	UM_RngLib_2.0	1
RngLib 2.0.2 for ST31R platform - Release note	RN_ST31R_RngLib_2.0.2	1

Table 16. Sites list

Site	Address	Activities(1)
AMTC / TOPPAN Dresden	Advanced Mask Technology Center Gmbh & Co KG Rahnitzer Allee 9, 01109 Dresden, Germany	MASK
CHIPBOND JY	Chipbond Technology Corporation No. 10, Prosperity 1 Road, Science Park, Hsinchu, Taiwan R.O.C	BE

Table 16. Sites list (continued)

Site	Address	Activities[1]
CHIPBOND LH	Chipbond Technology Corporation No. 3, Li Hsin 5 Road, Science Park, Hsinchu, Taiwan R.O.C	BE
DNP	Dai Nippon Printing Co., Ltd 2-2-1 Kami-Fukuoka, Fujimino-shi Saitama 356-8507 Japan	MASK
DPE	Dai Printing Europe Via C. Olivetti 2/A I-20041 Agrate Italy	MASK
Feiliks	Feili Logistics (Shenzhen) Co., Ltd. Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHSD
Pantos	LX Pantos Logistics (HK) Co Ltd. Unit 1001, 10/F, Mapletree Logistics Hub, 30 Tsing Yi Road, Tsing Yi, N.T. Hong Kong	WHSD
ST AMK1	STMicroelectronics 5A Serangoon North Avenue 5 554574 Singapore	DEV
ST AMK6	STMicroelectronics 18 Ang Mo Kio Industrial park 2 569505 Singapore	WHS WHSD
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers 20180 Bouskoura Maroc	BE WHSD
ST Calamba	STMicroelectronics 9 Mountain Drive, LISP II, Brgy La mesa, CALAMBA, Philippines 4027	BE WHSD
ST Catania	STMicroelectronics Str. Primosole, 50, 95121 Catania, Italy	DEV

Table 16. Sites list (continued)

Site	Address	Activities[1]
ST Crolles	STMicroelectronics 850 rue Jean Monnet 38926 Crolles France	DEV FE MASK
ST Gardanne	CMP George Charpak 880 Avenue de Mimet 13541 Gardanne France	BE
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	BE DEV ES_DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive 508938 Singapore	WHSD
ST Palermo	STMicroelectronics Via Tommaso Marcellini, 8L, 90129 Palermo, Italy	DEV
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark 35700 Rennes France	DEV ES_DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, Z.I. 13106 Rousset Cedex France	DEV ES_DEV EWS WHSD
ST Sophia	STMicroelectronics Sky Sophia, Bât B, 776 Rue Albert Caquot, 06410 Biot France	DEV

Table 16. Sites list (continued)

Site	Address	Activities[1]
STS Shenzhen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone Shenzhen P.R. China 518038	BE
STS Shenzhen Lab	STS Microelectronics 17 Taohua Road, Futian free trade zone, Shenzhen P.R. China 518038	BE
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh 319521 Singapore	EWS
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l’Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
TERADYNE	Teradyne 200 avenue Olivier Perroy, Les portes de Rousset - Bâtiment C 13970 ROUSSET- France	EWS
UTAC Indonesia		BE

1. BE = back-end and back-end manufacturing
DEV = hardware, firmware development,
ES_DEV= OS & Library development,
EWS = electrical wafer sort and/or pre-perso,
FE = front-end manufacturing,
MASK = mask manufacturing or mask preparation,
WHS = warehouse, no final delivery to customer,
WHSD = warehouse delivery, final delivery to customer,
IT = information technology.

8 References

Table 17. Common Criteria

Component description	Reference	Version
Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017	CCMB-2017-04-001 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2017-04-002 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017	CCMB-2017-04-003 R5	3.1 Rev 5

Table 18. Protection Profile

Component description	Reference	Version
Eurosmart - Security IC Platform Protection Profile with Augmentation Packages	BSI-CC-PP-0084-2014	1.0

Table 19. Other standards

Ref	Identifier	Description
[1]	BSI-AIS20/AIS31	A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler BSI, Version 2.0, 18-09-2011
[2]	NIST SP 800-67	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology
[3]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, updated May 2023
[4]	ISO/IEC 9796-2	ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002
[5]	NIST SP 800-38A	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, December 2001
[6]	ISO/IEC 14888	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[7]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[8]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000

Table 19. Other standards

Ref	Identifier	Description
[9]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[10]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[11]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[12]	NIST SP 800-90A	NIST Special Publication 800-90A, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), June 2015
[13]	JIL-Post-Deliv-Load	Security requirements for post-delivery code loading, JIL, Version 1.0, February 2016
[14]	ANSSI-CC-CER/F/06.002	PP0084: Interpretations, ANSSI, April 2016
[15]	NIST SP800-90B	NIST Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standards and Technology (NIST), January 2018
[16]	NIST SP800-22	NIST Special Publication 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications, National Institute of Standards and Technology (NIST), Revision 1a, April 2010
[17]	SOG-IS ACM	Agreed Cryptographic Mechanisms, SOG-IS Crypto Evaluation Scheme, Version 1.3, February 2023.
[18]	ANSSI-PG-083	Guide des mécanismes cryptographiques: Règles et recommendations concernant le choix et le dimensionnement des mécanismes cryptographiques. ANSSI, version 2.0.4, January 2020.

Appendix A Glossary

A.1 Terms

Authorised user

A user who may, in accordance with the TSP, perform an operation.

Composite product

Security IC product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation.

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

Electronic component(s) designed to perform processing and/or memory functions.

IC Dedicated Software

IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by ***ST***. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

IC Dedicated Test Software

That part of the IC Dedicated Software which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC developer

Institution (or its agent) responsible for the IC development.

IC manufacturer

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

IC packaging manufacturer

Institution (or its agent) responsible for the IC packaging and testing.

Initialisation data

Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data)

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations.

Packaged IC

Security IC embedded in a physical package such as micromodules, DIPs, SOICs or TQFPs.

Pre-personalization data

Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases. If "Package 2: Loader dedicated for usage by authorized users only" is used the Pre-personalisation Data may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.

Secret

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security IC

Composition of the TOE, the Security IC Embedded Software, User Data, and the package.

Security IC Embedded SoftWare (ES)

Software embedded in the Security IC and not developed by the IC designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3.

Security IC embedded software (ES) developer

Institution (or its agent) responsible for the security IC embedded software development and the specification of IC pre-personalization requirements, if any.

Security attribute

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Sensitive information

Any information identified as a security relevant element of the TOE such as:

– the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
– the security IC embedded software,
– the IC dedicated software,
– the IC specification, design, development tools and technology.

Smartcard

A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

Subject

An entity within the TSC that causes operations to be performed.

Test features

All features and functions (implemented by the IC Dedicated Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

TOE Delivery

The period when the TOE is delivered which is after Phase 3 ***or Phase 4 in this Security target***.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data

All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

A.2 Abbreviations

Table 20. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI).
BE	Back End manufacturing.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1. R5.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information.
DES	Data Encryption Standard.
DEV	Development.
DIP	Dual-In-Line Package.
DRBG	Deterministic Random Bit Generator.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
ES	Security IC Embedded Software.
EWS	Electrical Wafer Sort.
FE	Front End manufacturing.
FIPS	Federal Information Processing Standard.
I/O	Input / Output.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
LPU	Library Protection Unit.
MASK	Mask manufacturing.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.

Table 20. List of abbreviations (continued)

Term	Meaning
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or Security Target.
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.
WHS	Warehouse.