STMicroelectronics

ST31G480 F01
including optional cryptographic library NESLIB
Security Target for composition

Common Criteria for IT security evaluation

SMD_ST31G480_ST_17_003 Rev F01.1

September 2023

www.st.com

BLANK

ST31G480 F01 platform Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: ST31G480 F01 including optional cryptographic library NesLib SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev F01.1, issued in September 2023.

3 Registration: registered at ST Microelectronics under number SMD_ST31G480_ST_17_003.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the **ST31G480 F01** Security Integrated Circuit (IC), designed on the **ST31 platform of STMicroelectronics**, with firmware version 2.1.0, and optional cryptographic library **NesLib 6.2.1**.

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 Subgroup of STMicroelectronics (ST).

8 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2 and AVA_VAN.5.

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.

The original text of this PP is typeset as indicated here, its augmentations from *AUG* as indicated here, when they are reproduced in this document.

This ST also instantiates the following package from the above mentioned PP:

- Loader dedicated for usage in secured environment 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***. 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* and ***AUG4*** for Addition #4 of *AUG*.

1.4 TOE identification

13 The Target of Evaluation (TOE) is the ST31G480 F01 platform.

14 “ST31G480 F01” completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 16: Guidance documentation*, and its development and production sites indicated in *Table 17: Sites list*.

15 F01 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	OST version	Optional NesLib crypto library version
K8L0B	H	00B8h	2.1.0	3.4	6.2.1

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 16: Guidance documentation*.

1.5 TOE overview

18 Designed for secure ID and banking applications, the TOE is a serial access microcontroller that incorporates the most recent generation of ARM® 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 personalisation 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, the available NVM size, the availability of Nescrypt as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
I/O mode	Contact only, Dual mode, Contactless only
NVM size	128, 192, 256, 320, 384, 448 or 480 Kbytes
Nescrypt	Active, Inactive
Capacitor	20pF, 68pF, 168pF

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 Data Sheet and in the Firmware User Manual, referenced in *Table 16*.

24 The rest of this document applies to all possible configurations of the TOE, with or without NesLib, except when a restriction is mentioned. For easier reading, the restrictions are typeset as indicated here.

25 In a few words, the ST31G480 F01 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 Security Enhanced DES accelerator,
- Hardware Security AES accelerator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- optional NExt Step CRYPTography accelerator (NESCRYPT),
- optional cryptographic library.

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. The AES (Advanced Encryption Standard *[6]*) 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.
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 triple DES computation.
If Nescrypt is active, the NESCRYPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance (*[7]*, *[9]*, *[12]*,*[13]*, *[14]*, *[15]*).

27 The TOE offers 12 Kbytes of User RAM and up to 480 Kbytes of secure User high-density Flash memory (NVM).

28 As randomness is a key stone in many applications, the ST31G480 F01 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 *[1]* and directly accessible thru dedicated registers.

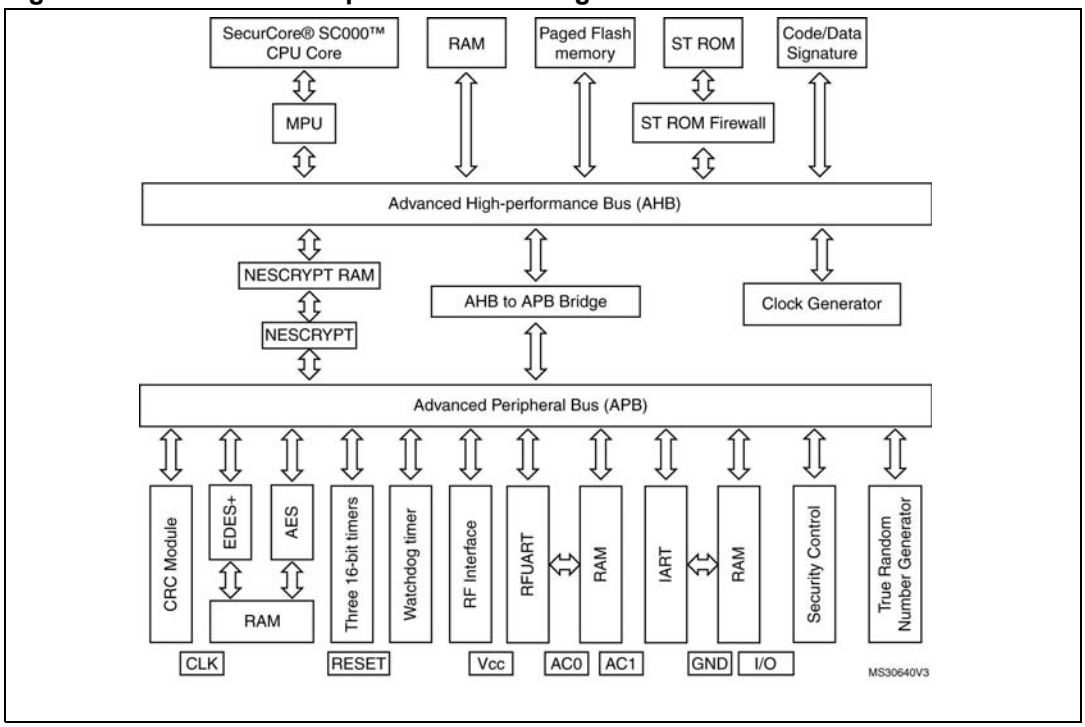
29 This device also includes the ARM® SecurCore® SC000™ memory protection unit (MPU), which enables the user to define its own region organization with specific protection and access permissions.

30 The TOE offers a contact serial communication interface fully compatible with the ISO/IEC 7816-3 standard, and a contactless interface including an RF Universal Asynchronous Receiver Transmitter (RF UART), enabling communication up to 848 Kbits/s compatible with the ISO/IEC 14443 Type A, B and B', PayPass™ and ISO/IEC 18092 passive mode standards.
These interfaces can be used simultaneously (dual mode), or the contact interface can be deactivated (see *Table 2: Derivative devices configuration possibilities*).

31 The detailed features of this TOE are described in the Data Sheet and in the Cortex SC000 Technical Reference Manual, referenced in *Table 16*.

32 *Figure 1* provides an overview of the ST31G480 F01 platform.

Figure 1. ST31G480 F01 platform block diagram



1.6.2 TOE software description

33 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.

34 The System ROM and ST NVM of the TOE contain a Dedicated Software which provides a very reduced set of commands for final test (operating system for final test, called "FTOS"), not intended for the Security IC Embedded Software (ES) usage, and not available in User configuration.

35 The System ROM and ST NVM of the TOE contain a Dedicated Support Software called 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 not available in User configuration.

36 The System ROM and ST NVM of the TOE contain a Dedicated Support Software, which provides 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 all through the product life-cycle.

37 The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is a cryptographic library called NesLib. NesLib is a cutting edge cryptographic library in terms of security and performance.

NesLib is embedded by the ES developer in his applicative code.
Note that the NesLib RSA, ECC and Diffie-Hellman functions can only be used if Nescrypt is active.

NesLib is a cryptographic toolbox supporting the most common standards and protocols:

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[14]*), and Diffie-Hellman *[24]*,
- an asymmetric key cryptographic support module that provides very efficient basic functions to build up protocols using Elliptic Curves Cryptography on prime fields GF(p) with elliptic curves in short Weierstrass form *[12]*, and provides support for ECDH key agreement *[22]* and ECDSA generation and verification *[5]*.
- a module for supporting elliptic curve cryptography on Edwards curve 25519, in particular ed25519 signature generation, verification and point decompression *[26]*.
- a cryptographic support module that provides hash functions (SHA-1[a], SHA-2 *[4]*), SHA-3, Keccak and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3 *[21]*,
- a symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard cryptographic algorithm (DES) *[2]*,
- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES) *[6]*,
- support for Deterministic Random Bit Generators *[19]*,
- prime number generation and RSA key pairs generation *[3]*.

38 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, except NesLib when it is embedded.

1.6.3 TOE documentation

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

- the product Data Sheet,
- the product family Security Guidance,
- the AIS31 user manuals,
- the ARM SC000 Technical Reference Manual,
- the Firmware user manual,
- the Flash loader installation guide,
- optionally the NesLib user manuals and security recommendations.

40 The complete list of guidance documents is detailed in *Table 16*.

a. Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

1.7 TOE life cycle

41 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.

42 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.

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

44 The sites potentially involved in the TOE life cycle are listed in *Table 17*.

45 The limit of the evaluation corresponds to phases 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 1, 5, 6 and 7 are outside the scope of this evaluation.

46 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.

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

48 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.

49 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

Table 3. Composite product life cycle phases (continued)

Phase	Name	Description
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

50 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)

51 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.

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

53 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).

54 The development centres possibly involved in the development of the TOE are denoted by the activity “ES-DEV” or “DEV” in *Table 17*.

55 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).

56 The authorized sub-contractors potentially involved in the TOE mask manufacturing are denoted by the activity “MASK” in *Table 17*.

1.8.2 TOE production environment

57 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

58 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 of each TOE occurs to assure conformance with the device specification.

59 The authorized front-end plant possibly involved in the manufacturing of the TOE are denoted by the activity “FE” in *Table 17*.

60 The authorized EWS plant potentially involved in the testing of the TOE are denoted by the activity “EWS” in *Table 17*.

61 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

62 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.

63 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 17*.

64 All sites denoted by the activity “WHS” or “WHSD” in *Table 17* can be involved for the logistics during phase 3 or 4.

1.8.3 TOE operational environment

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

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

67 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

68 The ST31G480 F01 platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

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

70 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.

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

71 The assurance level for the ST31G480 F01 platform Security Target is ***EAL5*** augmented by ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2 and AVA_VAN.5.

2.2 PP Claims

2.2.1 PP Reference

72 The ST31G480 F01 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.

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

- Loader dedicated for usage in secured environment only.

2.2.2 PP Additions

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

- Addition #1: “Support of Cipher Schemes” from *AUG*,
- Addition #4: “Area based Memory Access Control” from *AUG*,
- Specific additions for the Secure Flash Loader
- Refinement of assurance requirements.

74 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. Text originating in *AUG* is typeset as indicated here.

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

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

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

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

79 The additional SARs relative to the PP are summarized in *Table 10*.

2.2.3 PP Claims rationale

80 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.

81 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*.

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

83 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*.

84 Similarly, the security requirements rationale presented in *Section 5.4* has been updated with respect to the protection profile.

85 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)

86 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.

87 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*, and the ones introduced in this Security Target, are detailed in the following sections.

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

89
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
	AUG4.T.Mem-Access	Memory Access Violation
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
	P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
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

90 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.

91 The assets regarding the threats are:

- 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 and product in any form,
- the TOE correct operation,
- the Security IC Embedded Software, stored in the TOE's protected memories and in operation,
- the security services provided by the TOE for the Security IC Embedded Software,
- the cryptographic co-processors for Triple-DES and AES, the random number generator,
- the TSF Data.

92 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 security concerns are extended accordingly.

3.2 Threats

93 The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.

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

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.

3.3 Organisational security policies

94 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.

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

96 *BSI.P.Lim-Block-Loader* is dedicated to the Secure Flash Loader, and described in the *BSI-CC-PP-0084-2014* package "Loader dedicated for usage in secured environment only".

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

98 A new Organisational Security Policy (OSP) is defined here below:

99 P.Controlled-ES-Loading is related to the capability provided by the TOE to load Security IC Embedded Software into the NVM after TOE delivery, in a controlled manner, during composite product manufacturing. The use of this capability is optional, and depends on the customer's production organization.

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 in order to protect stored data from disclosure and manipulation.
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)(1), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded, – ***Secure Hashing (SHA-1***(2)***, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded, – Rivest-Shamir-Adleman (RSA), if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, – ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded. 1. Note that triple DES with two keys is no longer recommended as encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength. 2. Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.
P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE shall provide the capability to import the Security IC Embedded Software into the NVM, in a controlled manner, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. This capability is not available in User configuration.

3.4 Assumptions

100 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)

101 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.

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

103 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 originating in *AUG*, and the one 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
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
	O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
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

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
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)**,** **– *Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded**,** **– *Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded**,** – Rivest-Shamir-Adleman (RSA)**,** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, – ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded.
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.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE must provide the capability to load the Security IC Embedded Software into the NVM, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. The TOE must restrict the access to these features. The TOE must provide control means to check the integrity of the loaded user data. This capability is not available in User configuration.

4.2 Security objectives for the environment

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

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

105 Security Objectives for the operational Environment (phase 4 up to 6):

BSI.OE.Process-Sec-IC Protection during composite product manufacturing

BSI.OE.Lim-Block-Loader Limitation of capability and blocking the Loader

4.3 Security objectives rationale

106 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.

107 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).

108 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*)".

109 The augmentation made in this ST introduces the following security environment aspects:

- organisational security policies "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)".

110 The justification of the additional policies 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.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	Phase 5-6 optional Phase 4

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
P.Controlled-ES-Loading	*O.Controlled-ES-Loading*	Phase 4-6
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*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func*	
BSI.T.RND	*BSI.O.RND*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	

4.3.1 TOE threat "Memory Access Violation"

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

112 According to *AUG4.O.Mem-Access* the TOE must enforce the ***dynamic memory segmentation and protection*** 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.

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

4.3.2 Organisational security policy "Additional Specific Security Functionality"

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

115 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.

116 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*.

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

4.3.3 Organisational security policy "Controlled loading of the Security IC Embedded Software"

118 The justification related to the organisational security policy "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)" is as follows:

119 Since *O.Controlled-ES-Loading* requires the TOE to implement exactly the same specific security functionality as required by *P.Controlled-ES-Loading*, and in the very same conditions, the organisational security policy is covered by the objective.

120 The added objective for the TOE *O.Controlled-ES-Loading* does not introduce any contradiction in the security objectives.

5 Security requirements (ASE_REQ)

121 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

122 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.

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

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

124 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.

125 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.

126 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			
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality	*BSI-CC-PP-0084-2014* Operated	
FMT_LIM.2 / Loader	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification		
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	Random number generation	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	*CCMB-2017-04-002 R5*
FCS_CKM.1 (if NesLib is embedded only)	Cryptographic key generation		Security Target Operated	
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	

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

Label	Title	Addressing	Origin	Type
FDP_ITC.1 / Loader	Import of user data without security attributes	User data loading access violation	Security Target Operated	CCMB-2017-04-002 R5
FDP_ACC.1 / Loader	Subset access control			
FDP_ACF.1 / Loader	Security attribute based access control			
FMT_MSA.3 / Loader	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Loader	Management of security attribute			
FMT_SMR.1 / Loader	Security roles	Abuse of Admin functionality		
FIA_UID.1 / Loader	Timing of identification			
FMT_SMF.1 / Loader	Specification of management functions			

5.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

127 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)

128 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.***

129 ***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

130 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

131 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***.

132 *SFP_1: Limited capability and availability Policy / Test*

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)

133 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)

134 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)

135 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***.

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

Resistance to physical attack (FPT_PHP.3)

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

138 ***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)

139 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)

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

141 ***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)

142 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***.

143 *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 (FCS_RNG.1)

144 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.***

145 The TSF shall provide ***octets of bits*** 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.***

5.1.2 Additional Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

146 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. The list of operations depends on the presence of cryptographic accelerators or NesLib, as indicated in Table 8 (Restrict).

Table 8. FCS_COP.1 iterations (cryptographic operations)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
None	TDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Triple Data Encryption Standard (TDES)(1)	168 bits	*NIST SP 800-67* *NIST SP 800-38A*
None	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*
Only if NesLib		* Message authentication Code computation (CMAC) * Authenticated encryption/decryption in Galois Counter Mode (GCM) * Authenticated encryption/decryption in Counter with CBC-MAC (CCM)			*NIST SP 800-38B* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38C*
Only if NesLib and Nescrypt	RSA	* RSA public key operation * RSA private key operation without the Chinese Remainder Theorem * RSA private key operation with the Chinese Remainder Theorem * EMSA PSS and PKCS1 signature scheme coding * RSA Key Encapsulation Method (KEM)	Rivest, Shamir & Adleman's	from 829 bits to 4096 bits	*PKCS #1 V2.1*

Table 8. FCS_COP.1 iterations (cryptographic operations) (continued)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Only if NesLib and Nescrypt	ECC on Weierstrass curves	* private scalar multiplication * prepare Jacobian * public scalar multiplication * point validity check * convert Jacobian to affine coordinates * general point addition * point expansion * point compression	Elliptic Curves Cryptography on GF(p) on curves in Weierstrass form	up to 640 bits	*IEEE 1363-2000*, *chapter 7* *IEEE 1363a-2004*
		* Diffie-Hellman (ECDH) key agreement computation			*NIST SP 800-56A*
		* digital signature algorithm (ECDSA) generation and verification			*FIPS PUB 186-4* *ANSI X9.62*, *section 7*
Only if NesLib and Nescrypt	ECC on Edwards curves	* ed25519 generation * ed25519 verification * ed25519 point decompression	Elliptic Curves Cryptography on GF(p) on curves in Edwards form, with curve 25519	256 bits	*EdDSA rfc* *EDDSA* *EDDSA2*
Only if NesLib	SHA	* SHA-1(2) * SHA-224 * SHA-256 * SHA-384 * SHA-512 * Protected SHA-1(2) * Protected SHA-256 * Protected SHA-384 * Protected SHA-512	Secure Hash Algorithm	assignment pointless because algorithm has no key	*FIPS PUB 180-2*
		* HMAC using any of the above hash functions		up to 256 bits	*FIPS PUB 198-1*

Table 8. FCS_COP.1 iterations (cryptographic operations) (continued)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Only if NesLib	Keccak	* SHAKE128, * SHAKE256, * SHA3-224, * SHA3-256, * SHA3-384, * SHA3-512, * Keccak[r,1600-r], * protected SHAKE128, * protected SHAKE256, * protected SHA3-224, * protected SHA3-256, * protected SHA3-384, * protected SHA3-512, * Protected Keccak[r,1600-r]	Keccak	no key for plain functions, variable key length up to security level for protected functions (security level is last number in function names and 1600-c for Keccak)	*FIPS PUB 202*
Only if NesLib	Keccak-p	* Keccak-p[1600,n_r = 24], * Keccak-p[1600, n_r=12], * protected Keccak-p[1600,n_r = 24], * protected Keccak-p[1600, n_r=12]	Keccak-p	no key for plain functions, any key length up to 256 bits for protected functions	*FIPS PUB 202*
Only if NesLib and Nescrypt	Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	up to 3968 bits	*ANSI X9.42*
Only if NesLib	DRBG	* SHA-1(2) * SHA-224 * SHA-256 * SHA-384 * SHA-512	Hash-DRBG	None	*NIST SP 800-90* *FIPS PUB 180-2*
		*AES	CTR-DRBG	128, 192 and 256 bits	*NIST SP 800-90* *FIPS PUB 197*

1. Note that triple DES with two keys is no longer recommended as encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength.
2. Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

Cryptographic key generation (FCS_CKM.1)

147 If NesLib is embedded only, the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm***, in*** *Table 9****,*** and specified cryptographic key sizes ***of*** *Table 9* that meet the following ***standards in*** *Table 9****.***

Table 9. FCS_CKM.1 iterations (cryptographic key generation)

Iteration label	[assignment: cryptographic key generation algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Prime generation	prime generation and RSA prime generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions	prime sizes up to 2048 bits	*FIPS PUB 140-2* *FIPS PUB 186-4*
RSA key generation	RSA key pair generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions	from 829 bits to 4096 bits	*FIPS PUB 140-2* *ISO/IEC 9796-2* *PKCS #1 V2.1*

5.1.3 Additional Security Functional Requirements for the memories protection

148 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

149 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.

150 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.

Management of security attributes (FMT_MSA.1) / Memories

151 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 running in privileged mode.***

Complete access control (FDP_ACC.2) / Memories

152 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.

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

153 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

154 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.***

155 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.***

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

157 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, and in User configuration, any write access to the ST NVM is denied.***

158 **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.

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

160 *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

161 The TSF will be able of performing the following management functions: ***modification of the current set of access rights security attributes by software running in privileged mode, supporting the Dynamic Memory Access Control Policy.***

5.1.4 Additional Security Functional Requirements related to the possible availability of final test and loading capabilities in phases 4 to 6 of the TOE life-cycle

Limited capabilities (FMT_LIM.1) / Loader

162 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.***

163 *SFP_4: Loader Limited capability Policy*

164 *Deploying Loader functionality after blocking of the loader does not allow stored user data to be disclosed or manipulated by unauthorized user.*

Limited availability (FMT_LIM.2) / Loader

165 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***.

166 *SFP_5: Loader Limited availability Policy*

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

Import of user data without security attributes (FDP_ITC.1) / Loader

168 The TSF shall enforce the ***Loading Access Control Policy*** when importing user data, controlled under the SFP, from ouside of the TOE.

169 The TSF shall ignore any security attributes associated with the User data when imported from outside of the TOE.

170 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE:

- ***the integrity of the loaded user data is checked at the end of each loading session,***
- ***the loaded user data is received encrypted, internally decrypted, then stored into the NVM.***

Static attribute initialisation (FMT_MSA.3) / Loader

171 The TSF shall enforce the ***Loading Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

172 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

173 The TSF shall enforce the ***Loading Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***remaining loading sessions*** to ***the Loader Administrator.***

Subset access control (FDP_ACC.1) / Loader

174 The TSF shall enforce the ***Loading Access Control Policy*** on ***all subjects, object NVM and all commands***.

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

175 The TSF shall enforce the ***Loading Access Control Policy*** to objects based on the following: ***the TOE mode, the user authenticated role, the remaining loading sessions and the requested command, according to the fixed loader access rights.***

176 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the command is allowed if and only if the TOE mode, the user authenticated role, the remaining loading sessions and the requested command match an entry in the fixed loader access rights.***

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

178 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***in User mode, no loader command is deployed.***

179 The following SFP ***Loading Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / Loader":

180 *SFP_6: Loading Access Control Policy*

181 *The TSF must enforce that only authorised users are allowed to download User code and data into the User NVM or to set the product profile.*
The TSF must enforce that only authorised users are allowed to be administrator of the provided loader functionality.
The TSF controls access to the loader functionality based on the TOE mode, the user authenticated role, the remaining loading sessions and the requested command according to the fixed loader access rights.

Specification of management functions (FMT_SMF.1) / Loader

182 The TSF will be able of performing the following management functions: ***change the TOE mode, change the user role, change the remaining sessions.***

Security roles (FMT_SMR.1) / Loader

183 The TSF shall maintain the roles: ***Loader and Loader Administrator***.

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

Timing of identification (FIA_UID.1) / Loader

185 The TSF shall allow ***boot and authentication command*** on behalf of the user to be performed before the user is identified.

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

5.2 TOE security assurance requirements

187 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level ***5*** (EAL***5***) and augmented by taking the following components:

- ***ADV_IMP.2, ADV_TDS.5, ALC_CMC.5,*** ALC_DVS.2, ***ALC_FLR.1, ALC_TAT.3, ASE_TSS.2*** and AVA_VAN.5.

188 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.

189 The component ALC_FLR.1 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.

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

191 The set of security assurance requirements (SARs) is presented in *Table 10*, indicating the origin of the requirement.

Table 10. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.2	Complete mapping of the implementation representation of the TSF	Security Target
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.5	Complete semiformal modular design	Security Target
AGD_OPE.1	Operational user guidance	EAL5/*BSI-CC-PP-0084-2014*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMC.5	Advanced support	Security Target
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	*BSI-CC-PP-0084-2014*
ALC_FLR.1	Basic flaw remediation	Security Target
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.3	Compliance with implementation standards - all parts	Security Target
ASE_CCL.1	Conformance claims	EAL5/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_INT.1	ST introduction	EAL5/*BSI-CC-PP-0084-2014*
ASE_OBJ.2	Security objectives	EAL5/*BSI-CC-PP-0084-2014*
ASE_REQ.2	Derived security requirements	EAL5/*BSI-CC-PP-0084-2014*
ASE_SPD.1	Security problem definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_TSS.2	TOE summary specification	Security Target
ATE_COV.2	Analysis of coverage	EAL5/*BSI-CC-PP-0084-2014*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-CC-PP-0084-2014*
ATE_IND.2	Independent testing - sample	EAL5/*BSI-CC-PP-0084-2014*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-CC-PP-0084-2014*

5.3 Refinement of the security assurance requirements

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

193 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.

194 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.

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

196 For reader's ease, an impact summary is provided in *Table 11*.

Table 11. Impact of EAL5 selection on *BSI-CC-PP-0084-2014* refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ADO_DEL	1	1	None
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	5	None, refinement is still valid
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
ATE_COV	2	2	IC Dedicated Software is included
AGD_OPE	1	1	None
AGD_PRE	1	1	None
AVA_VAN	5	5	None

5.3.1 Refinement regarding functional specification (ADV_FSP)

197 ~~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.***

198 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.

199 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.

200 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.

201 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.

202 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.

5.3.2 Refinement regarding test coverage (ATE_COV)

203 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 writing).

204 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).

205 ~~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.***

5.4 Security Requirements rationale

5.4.1 Rationale for the Security Functional Requirements

206 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* 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*
BSI.O.RND	*Random number generation FCS_RNG.1* 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_IFC.1*, *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
AUG1.O.Add-Functions	*Cryptographic operation FCS_COP.1* *Cryptographic key generation FCS_CKM.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*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*
O.Controlled-ES-Loading	*Import of user data without security attributes FDP_ITC.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* *Management of security attribute FMT_MSA.1 / Loader* *Specification of management functions FMT_SMF.1 / Loader* *Security roles FMT_SMR.1 / Loader* *Timing of identification FIA_UID.1 / Loader*

207 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.

208 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*, and an additional objective (*O.Controlled-ES-Loading*) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

209 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 (*FCS_CKM.1*, *FDP_ITC.1 / Loader*, *FDP_ACC.1 / Loader*, *FDP_ACF.1 / Loader*, *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMF.1 / Loader*, *FMT_SMR.1 / Loader*, *FIA_UID.1 / Loader*, and *FMT_SMF.1 / Memories,* and various assurance requirements of EAL5+).

210 Though it remains to show that:

- security objectives from this Security Target 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.

211 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*)”

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

213 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.

214 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*)”

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

216 The security functional requirements “*Cryptographic operation (FCS_COP.1)*” ***and*** "*Cryptographic key generation (FCS_CKM.1)*" exactly require those functions to be implemented that are demanded by *AUG1.O.Add-Functions****.*** Therefore, *FCS_COP.1* is suitable to meet the security objective, ***together with*** *FCS_CKM.1*.

Security objective “Controlled loading of the Security IC Embedded Software (*O.Controlled-ES-Loading*)”

217 The justification related to the security objective “Controlled loading of the Security IC Embedded Software (*O.Controlled-ES-Loading*)” is as follows:

218 The security functional requirements "*Import of user data without security attributes (FDP_ITC.1) / Loader*", "*Subset access control (FDP_ACC.1) / Loader*" and "*Security attribute based access control (FDP_ACF.1) / Loader*", with the related Security Function Policy (SFP) “Loading Access Control Policy” exactly require to implement a controlled loading of the Security IC Embedded Software as demanded by *O.Controlled-ES-Loading*. Therefore, *FDP_ITC.1 / Loader*, *FDP_ACC.1 / Loader* and *FDP_ACF.1 / Loader* with their SFP are suitable to meet the security objective.

219 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*" and "*Timing of identification (FIA_UID.1) / Loader*" specifies the roles that the TSF recognises and the actions authorised 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.

5.4.3 Additional security requirements are consistent

"Cryptographic operation (*FCS_COP.1*) & key generation (*FCS_CKM.1*)"

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

221 These security requirements have already been argued in *Section : Security objective "Dynamic Area based Memory Access Control (AUG4.O.Mem-Access)"* above.

**"Import of user data without security attribute (*FDP_ITC.1 / Loader*),
Static attribute initialisation (*FMT_MSA.3 / Loader*),
Management of security attributes (*FMT_MSA.1 / Loader*),
Subset access control (*FDP_ACC.1 / Loader*),
Security attribute based access control (*FDP_ACF.1 / Loader*),
Specification of management function (*FMT_SMF.1 / Loader*),
Security roles (*FMT_SMR.1 / Loader*),
Timing of identification(*FIA_UID.1 / Loader*)"**

222 These security requirements have already been argued in *Section : Security objective "Controlled loading of the Security IC Embedded Software (O.Controlled-ES-Loading)"* above.

5.4.4 Dependencies of Security Functional Requirements

223 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 requirements rationale,
- those justifed in *AUG* security requirements rationale,
- the dependency of *FCS_COP.1* and *FCS_CKM.1* on FCS_CKM.4 (see discussion below).

224 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*

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 / 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*
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	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	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FDP_ITC.1 and FCS_CKM.1, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.4	No, see discussion below	
FCS_CKM.1	[FDP_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.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***	

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_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***
FMT_SMF.1 / Memories	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FMT_ITC.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / Loader	Yes	
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*
FDP_SMF.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

225 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, both "*Cryptographic key generation (FCS_CKM.1)*" and "*Import of user data without security attributes (FDP_ITC.1) / Loader*" may be used for the purpose of creating cryptographic keys, but also, the ES has all possibilities to implement its own creation function, in conformance with its security policy.

226 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" and "*Cryptographic key generation (FCS_CKM.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.

5.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5 (*Table 10*)

227 Regarding application note 22 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 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.

228 EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.

229 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. All dependencies introduced by the requirements chosen for augmentation are fulfilled. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

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

Dependencies of assurance requirements

231 Dependencies of security assurance requirements are fulfilled by the EAL5 package selection.

232 The augmentation to this package identified in paragraph *187* do not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_FLR.1 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)

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

234 The complete TOE summary specification has been presented and evaluated in the *ST31G480 F01 including optional cryptographic library NESLIB Security Target*.

235 For confidentiality reasons, the TOE summary specification is not fully reproduced here.

6.1 Limited fault tolerance (FRU_FLT.2)

236 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)

237 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 errors,
- MPU errors,
- External clock incorrect frequency,
- Sequence control,
- etc..

238 The ES can generate a software reset.

6.3 Limited capabilities (FMT_LIM.1) / Test

239 The TSF ensures that only very limited test capabilities are available in User configuration, in accordance with SFP_1: Limited capability and availability Policy / Test.

6.4 Limited capabilities (FMT_LIM.1) / Loader

240 The TSF ensures that the Secure Flash Loader and the final test capabilities are unavailable in User configuration, in accordance with SFP_4: Loader Limited capability Policy.

6.5 Limited availability (FMT_LIM.2) / Test & (FMT_LIM.2) / Loader

241 The TOE is either in Test, Admin (aka Issuer) or User configuration.

242 The only authorised TOE configuration modifications are:

- Test to Admin configuration,
- Test to User configuration,
- Admin to User configuration.

243 The TSF ensures the switching and the control of TOE configuration.

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

6.6 Stored data confidentiality (FDP_SDC.1)

245 The TSF ensures confidentiality of the User Data in all the memories where it can be stored.

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

246 The TSF ensures stored data integrity, in all the possible memory areas, depending on the integrity control attributes.

6.8 Audit storage (FAU_SAS.1)

247 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)

248 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)

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

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment,
- etc..

6.11 Random number generation (FCS_RNG.1)

250 The TSF provides 8-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.

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

251 The TOE provides optionally an EDES+ accelerator that has the capability to perform 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*.

If NesLib is embedded, the cryptographic library NesLib instantiates the same standard DES cryptographic operations.

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

252 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,

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

254 If NesLib is embedded, the cryptographic library NesLib instantiates the same standard AES cryptographic operations, and additionally provides:

- message authentication Code computation (CMAC),
- authenticated encryption/decryption in Galois Counter Mode (GCM),
- authenticated encryption/decryption in Counter with CBC-MAC (CCM).

6.14 Cryptographic operation: RSA operation (FCS_COP.1) / RSA if NesLib

255 The cryptographic library NesLib provides to the ES developer the following RSA functions, all conformant to *PKCS #1 V2.1*:

- RSA public key cryptographic operation for modulus sizes from 829 bits to 4096 bits,
- RSA private key cryptographic operation with or without CRT for modulus sizes from 829 bits to 4096 bits,
- RSA signature formatting,
- RSA Key Encapsulation Method.

6.15 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC if NesLib

256 The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Weierstrass form, all conformant to *IEEE 1363-2000* and *IEEE 1363a-2004*, including:

- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check,
- Jacobian conversion to affine coordinates,
- general point addition,
- point expansion and compression.

257 Additionally, the cryptographic library NesLib provides functions dedicated to the two most used elliptic curves cryptosystems:

- Elliptic Curve Diffie-Hellman (ECDH), as specified in *NIST SP 800-56A*,
- Elliptic Curve Digital Signature Algorithm (ECDSA) generation and verification, as stipulated in *FIPS PUB 186-4* and specified in *ANSI X9.62*, section 7.

258 The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Edwards form, with curve 25519, all conformant to *EdDSA rfc*, including:

- generation,
- verification,
- point decompression.

6.16 Cryptographic operation: SHA-1 & SHA-2 operation (FCS_COP.1) / SHA, if NesLib

259 The cryptographic library NesLib provides the SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*.

260 The cryptographic library NesLib provides the SHA-1, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*, and offering resistance against side channel and fault attacks.

261 Additionally, the cryptographic library NesLib offers support for the HMAC mode of use, as specified in *FIPS PUB 198-1*, to be used in conjunction with the protected versions of SHA-1, SHA-256, SHA-384, and SHA-512.

6.17 Cryptographic operation: Keccak & SHA-3 operation (FCS_COP.1) / Keccak, if NesLib

262 The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

263 The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

264 The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

265 The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

6.18 Cryptographic operation: Keccak-p operation (FCS_COP.1) / Keccak-p, if NesLib

266 The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202*:

- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].
- The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:
- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].

6.19 Cryptographic operation: Diffie-Hellman operation (FCS_COP.1) / Diffie-Hellman, if NesLib

267 The cryptographic library NesLib provides the Diffie-Hellman key establishment operation over GF(p) for size of modulus p up to 3968 bits, conformant to *ANSI X9.42*.

6.20 Cryptographic operation: DRBG operation (FCS_COP.1) / DRBG, if NesLib

268 The cryptographic library NesLib gives support for a DRBG generator, based on cryptographic algorithms specified in *NIST SP 800-90*.

269 The cryptographic library NesLib implements two of the DRBG specified in *NIST SP 800-90*:

- Hash-DRBG,
- CTR-DRBG.

6.21 Cryptographic key generation: Prime generation (FCS_CKM.1) / Prime_generation, if NesLib

270 The cryptographic library NesLib provides prime numbers generation for prime sizes up to 2048 bits conformant to *FIPS PUB 140-2* and *FIPS PUB 186-4*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

6.22 Cryptographic key generation: RSA key generation (FCS_CKM.1) / RSA_key_generation, if NesLib

271 The cryptographic library NesLib provides standard RSA public and private key computation for key sizes from 829 bits to 4096 bits conformant to *FIPS PUB 140-2, ISO/IEC 9796-2* and *PKCS #1 V2.1*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

6.23 Static attribute initialisation (FMT_MSA.3) / Memories

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

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

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

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

274 The TOE enforces the dynamic memory protection policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), programmed by the ES. Overriding the MPU set of access rights, the TOE enforces additional protections on specific parts of the memories.

6.26 Static attribute initialisation (FMT_MSA.3) / Loader

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

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

276 In Admin configuration, the System Firmware provides the capability to change part of the Flash Loader security attributes, only once in the product lifecycle.

6.28 Subset access control (FDP_ACC.1) / Loader, Security attribute based access control (FDP_ACF.1) / Loader, Security roles (FMT_SMR.1) / Loader & Timing of identification (FIA_UID.1) / Loader

277 In Admin configuration, the System Firmware grants access to the Flash Loader functions, only after presentation of the required valid passwords.

6.29 Import of user data without security attributes (FDP_ITC.1) / Loader

278 In Admin configuration, the System Firmware provides the capability of loading user data into the NVM, while ensuring confidentiality and integrity of the loaded data.

7 Identification

Table 14. ST31G480 F01 platform Security Target

Component description	Reference	Version
ST31G480 F01 including optional cryptographic library NESLIB Security Target	SMD_ST31G480_ST_17_001	F01.1

Table 15. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	OST version	Optional NesLib crypto library version
K8L0B	H	00B8h	2.1.0	3.4	6.2.1

1. Part of the product information.

Table 16. Guidance documentation

Component description	Reference	Version
ST31G platform - ST31G480 - Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of Flash memory - Datasheet	DS_ST31G480	4.0
ARM® Cortex SC000 Technical Reference Manual	ARM DDI 0456	A
ARMv6-M Architecture Reference Manual	ARM DDI 0419	C
ST31 Firmware User Manual	UM_ST31_FW	10
ST31G480 Flash memory loader installation guide - User manual	UM_31G_FL	2
NesLib 6.2 library - User manual	UM_NESLIB_6.2	3.0
ST31G, ST31H Secure MCU family - NesLib 6.2 security recommendations	AN_SECU_ST31G_H_NESLIB_6.2	11.0
NesLib 6.2.1 for ST31 Platforms - Release note	RN_ST31_NESLIB_6.2.1	10.0
ST31G and ST31H Secure MCU platforms Security Guidance	AN_SECU_ST31G_H	10.0
ST31G and ST31H - AIS31 Compliant Random Number - User Manual	UM_31G_31H_AIS31	1.0
ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note	AN_31G_31H_AIS31	1.0

Table 17. Sites list

Site	Address	Activities[1]
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, Z.I. 13106 Rousset Cedex France	DEV ES-DEV FE EWS WHSD MASK
ST AMK 1	STMicroelectronics 5A Serangoon North Avenue 5 554574 Singapore	DEV
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B 3d floor 1831 Diegem/Machelen Belgium	ES-DEV
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	DEV ES-DEV
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark 35700 Rennes France	DEV ES-DEV
ST Sophia	STMicroelectronics Sky Sophia, Bât B, 776 Rue Albert Caquot, 06410 Biot, France	DEV
ST Catania	STMicroelectronics Str. Primosole, 50, 95121 Catania, Italy	DEV
ST Palermo	STMicroelectronics Via Tommaso Marcellini, 8L, 90129 Palermo, Italy	DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV

Table 17. Sites list (continued)

Site	Address	Activities[1]
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
ST Gardanne	CMP Georges Charpak 880 Avenue de Mimet 13541 Gardanne France	BE
ST Crolles	STMicroelectronics 850 rue Jean Monnet 38926 Crolles France	DEV MASK
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh 319521 Singapore	EWS
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers 20180 Bouskoura Maroc	BE WHSD
ST Calamba	STMicroelectronics 9 Mountain Drive, LISP II, Brgy La mesa Calamba 4027 Philippines	BE WHSD
STS Shenzhen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone, Shenzhen, P.R. China 518038	BE
ST AMK 6	STMicroelectronics 18 Ang Mo Kio Industrial park 2 569505 Singapore	WHS
ST Loyang	STMicroelectronics 7 Loyang Drive 508938 Singapore	WHSD
AMKOR ATP1	AMKOR Technologies ATP1: Km 22 East Service Road, South Superhighway, Muntinlupa City 1771 Philippines	BE

Table 17. Sites list (continued)

Site	Address	Activities[1]
AMKOR ATP3/4	AMKOR Technologies ATP3/4: 119 North Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines	BE
SMARTFLEX	Smartflex Technologies 37A Tampines Street 92, 528886 Singapore	BE
CHIPBOND JY	Chipbond Technology Corporation No. 10, Prosperity 1 Road, Science Park Hsinchu, Taiwan R.O.C.	BE
CHIPBOND LH	Chipbond Technology Corporation No. 3, Li Hsin 5 Road, Science Park Hsinchu Taiwan R.O.C.	BE
UTAC Indonesia	PT UTAC Manufacturing Services Indonesia Jl Maligi I Lot A1-4, Kawasan Industri KIIC, Sukaluyu, Teluk Jambe Timur, Karawang 41361, Indonesia	BE
Feiliks	Feili Logistics (Shenzhen) CO., Ltd Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHSD
DNP	Dai Nippon printing Co ltd. 2-2-1 Kami-Fukuoka, Fujimino-shi, Saitama,356-8507, Japan	MASK
DPE	Dai Nippon Printing Europe Via C. Olivetti 2/A I-20041 Agrate Italy	MASK

1. Activities:
   ES-DEV = libraries development (Phase 1)
   DEV = development (Phase 2),
   MASK = mask preparation (Phase 2),
   IT = IT administration (Phase 2),
   FE = wafer manufacturing (Phase 3),
   EWS = electrical wafer sort (Phase 3),
   WHS = warehouse (Phases 3/4),
   WHSD = warehouse for delivery (Phases 3/4),
   BE = back-end manufacturing (Phase 4).

8 References

Table 18. 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 19. Protection Profile

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

Table 20. 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, revised January 2012, National Institute of Standards and Technology
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002
[4]	FIPS PUB 180-2	FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004
[5]	FIPS PUB 186-4	FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), July 2013
[6]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[7]	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

Table 20. Other standards

Ref	Identifier	Description
[8]	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, October 2010
[9]	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
[10]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[11]	MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
[12]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[13]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[14]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[15]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[16]	NIST SP 800-38B	NIST special publication 800-38B, Recommandation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), May 2005
[17]	NIST SP 800-38C	NIST special publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, National Institute of Standards and Technology (NIST), May 2004
[18]	NIST SP 800-38D	NIST special publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter mode (GCM) and GMAC, National Institute of Standards and Technology (NIST), November 2007
[19]	NIST SP 800-90	NIST Special Publication 800-90, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), March 2007

Table 20. Other standards

Ref	Identifier	Description
[20]	FIPS PUB 198-1	FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[21]	FIPS PUB 202	FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015
[22]	NIST SP 800-56A	NIST SP 800-90A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), May 2013
[23]	ANSI X9.31	ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), American National Standard for Financial Services, 1998
[24]	ANSI X9.42	ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, American National Standard for Financial Services, 2003 (R2013)
[25]	ANSI X9.62	ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard for Financial Services, 2005
[26]	EdDSA rfc	S. Josefsson and I. Liusvaara,, Edwards-curve Digital Signature Algorithm (EdDSA) draft-irtf-cfrg-eddsa-08, Network Working Group Internet-Draft, IETF, August 19, 2016, available from *https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-08*
[27]	EDDSA	Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "High-speed high-security signatures", *http://ed25519.cr.yp.to/ed25519-20110926.pdf* September 2011
[28]	EDDSA2	Bernstein, D., Josefsson, S., Lange, T., Schwabe, P., and B. Yang, "EdDSA for more curves", WWW *http://ed25519.cr.yp.to/eddsa-20150704.pdf* July 2015

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.

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 21. 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 21. 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.
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.